Chapter 3

Evaluation Theory for Characteristics of Cloud Identity Trust Framework

Eghbal Ghazizadeh and Brian Cusack

Additional information is available at the end of the chapter

http://dx.doi.org/10.5772/intechopen.76338

Abstract

Trust management is a prominent area of security in cloud computing because insufficient trust management hinders cloud growth. Trust management systems can help cloud users to make the best decision regarding the security, privacy, Quality of Protection (QoP), and Quality of Service (QoS). A Trust model acts as a security strength evaluator and ranking service for the cloud and cloud identity applications and services. It might be used as a benchmark to setup the cloud identity service security and to find the inadequacies and enhancements in cloud infrastructure. This chapter addresses the concerns of evaluating cloud trust management systems, data gathering, and synthesis of theory and data. The conclusion is that the relationship between cloud identity providers and Cloud identity users can greatly benefit from the evaluation and critical review of current trust models.

Keywords: cloud computing, cloud security, federated identity management system, cloud identity, trust frameworks

1. Introduction

Trust management had been established by Blaze, Feigenbaum and Lacy [1] to deal with security issues of centralized systems. The aim of their system was overcoming the inflexibility of a complex trust relationship, and centralized control of trust relationship. Trust management has been attractive by many researchers especially in the area of Peer to Peer, E-Commerce, Wireless Sensor Network, Grid Computing, and Cloud Computing [2]. There are several trust definitions but in this book chapter trust means the extent to which Cloud Identity users (CIdU) and Cloud Service Providers (CSP) are willing to depend on a CIdPs and Cloud Service

Customers (CSC) provisioning and de-provisioning their service and expect certain qualities that CIdPs promised to be met.

In the cloud computing, user and provider recommendation has been adopted as a trust [3]. The reason for widely using is to get the advantage of user and provider about the Trust Service Provider (TSP). Though, in the social psychology, it is well-known that the role of a service customer has a substantial influence on another customers' trust assessment. However, transitive recommendation and explicit recommendation are different forms of recommendation. Therefore, in the explicit recommendation, a consumer of the cloud clearly recommend a particular TSP, but, in the transitive recommendation, on the other hand, a cloud customer trusts a particular TSP because at least one of her trusted relations trusts the service. The reputation of the TSP is consequently related to the customer's feedback of TSP which highlight the importance of the trust. [5]. Moreover, as pointed in [6] reputation can have a direct or indirect influence on the trustworthiness of a TSP and CSP. Nevertheless, Unlike the recommendation, in reputation, cloud service consumers do not know the source of the trust feedback, because there are no trusted relations in reputation systems. eBay, Amazon, Aliexpress, and Epinions are some examples of online reputation-based systems and review systems where the consumer's opinions and reviews on specific products or services are expressed.

Therefore, the complexity and variety of the trust in the cloud area is one contemporary issue in which the research community has recently embarked. Manifesting itself as the descendant of several other trust framework such as user observation and computational frameworks inherits their limitations and advancements. Towards the end-goal of a thorough comprehension of the field of cloud identity trust framework, and a more rapid adoption from the scientific community, we propose in this chapter an ontology of trust framework which demonstrates a dissection of the trust frameworks into six main frameworks based on their characteristics and methods of data collection to help and improve user's knowledge based decision making. Moreover, evaluation theory leads this chapter to illustrates their interrelations as well as their inter-dependency on trust elements and attributes. The contribution of this chapter lies in being one of the first research and attempts to establish a dedicated ontology and taxonomy of the cloud identity trust framework with regards of the evaluation theory. Therefore, Better comprehension of the trust elements would enable and leads the CIdPs to design more trustworthy services and gateways for the CIdUs and facilitate the selection of the identity providers. In turn, this will assist the identity community to accelerate its contributions and insights into this evolving identity field.

2. Evaluation system architecture

Evaluation is a key analytical process in all intellectual, disciplines, and service providers [7]. Also, it is possible to apply different types of evaluation methods to provide knowledge of the complexity and ubiquity of the cloud service providers. This book chapter aim is to obtain a set of basic evaluation components based on the [8]. Moreover, this book chapter aims to propose a framework that can be used to develop a trusted computing with the purpose of improving the previous trust methods. In particular, evaluation system architecture method had been applied to review the trust establishment frameworks by means of the identification of the evaluation components and the analysis of their weaknesses and strengths. Therefore, this

book chapter seeks to highlight that related work of mentioned trust framework developed based on trust theoretical and practical foundation. In this section, evaluation theory [8] is considered as a theoretical foundation for developing cloud identity trust framework and its processes has been shown in **Figure 1**.

Comprehensive and reliable of the trust level evaluation in identity environment are two crucial reasons to use evaluation theory. Evaluation theory offers a formal and clear description of the concept of evaluation. Therefore, it proposes six components involved in an evaluation shown in **Figure 2** and will be adopted and discussed in the following sub-sections.

- Target: Trust between CIdPs and CIdUs
- Criteria: Trust elements of the Cloud Identity Providers (CIdP) and CSPs that are to be evaluated
- Yardstick or standard: the ideal trust framework against which the current trust framework is to be compared
- Data-gathering techniques: Critical or systematic literature review needed to obtain data to analyze each criterion
- Synthesis techniques: Generally this technique used to judge the target, obtaining the results of the evaluation with judging each particular element,
- Evaluation process: series of activities and tasks by means of which an evaluation is performed (out of scope for this book chapter)

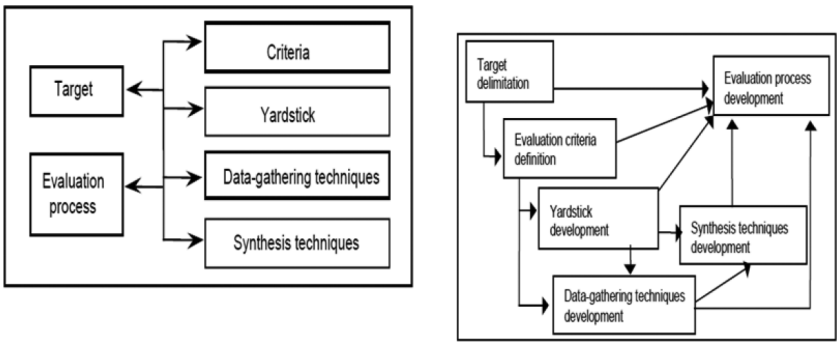

Figure 1. Components of an evaluation and their interrelations ([8], p. 6).

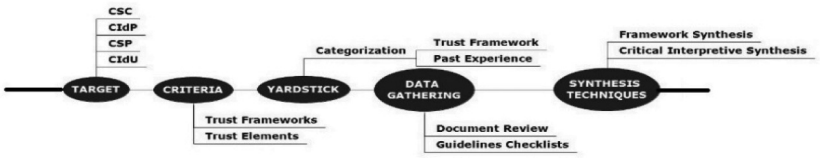

Figure 2. Cloud identity trust evaluation framework.

2.1. Target

The first activity as shown in **Figure 2** is identifying and ascertaining evaluation target. A target which means the object under evaluation provides knowledge about what the object is and presents a general description of the objective functions and domains. Therefore, in this book chapter level of trust for CIdPs has been selected to be the object under evaluation. It has been chosen because CSPs have not yet adopted an all-out cloud identity and they require identity federation in order to provide not only SSO but also agile and secure access controls between internal and external services. Besides, to enable communications among CIdPs, CIdUs, CSPs, they must be able to establish trust with one another and exchange identity information. Therefore, cloud identity trust framework has been developed to help CIdUs make a good decision based on the trust elements.

2.2. Evaluation criteria

Criteria definition is the second critical and essential step in developing a cloud identity trust framework. Having ascertained and delimited the target (CIdP), it is necessary to identify what characteristics (trust elements) of the target (CIdP) are important for evaluation purposes. These characteristics are referred to as evaluation criteria. Alabool and Mahmood [7] specified the importance to use as many criteria as possible to make better trust elements coverage under evaluation. These criteria also can pertain to diverse Sub-elements; while each sub-elements also can be broken down several elements. A critical literature review (overview of published materials) study has been conducted to answer two questions.

First, what is the current state of trust computing knowledge about these issues and problems (Looking for the taxonomy and methods of trust framework as shown in **Figure 2**)?

Second, what are the current trust computing in the theoretical or policy issues and debates related to trust, cloud computing, and cloud identity management systems (Looking for elements and cloud identity trust elements as shown in **Figure 2**)?

To answer the first question, there was a need for caching module to effectively communicate with CSCs. Attributes of a CSPs are used as evidence to make trust judgment on their service, and those attributes need to be distributed in a trustworthy way. In the following, attribute certification as an approach to deliver cloud attributes will be discussed. Hence, it had motivated to build a hybrid model for trust management in cloud identity computing environments. Current trends and existing approaches in the field of trust establishment need to be categorized in a precise way to identify and analyze the current cloud trust establishment method. In this regard, user observation, Auditing and Risk Assessment, Self-assessment Questionnaires, Benchmarking and Monitoring, Service Level Agreement (SLA) Based Trust framework, and Computational Trust Framework have been systematically categorized as a proposed trust models on the basis of their diverse attributes and techniques for calculating the trust score as a source of evidences and **Figure 3** shows the selected categories for this book chapter.

User observation: Users opinion, social network, and reputation based approaches are some of the user observation frameworks. The reputation of CSP is the aggregated opinion of CSCs

http://dx.doi.org/10.5772/intechopen.76338

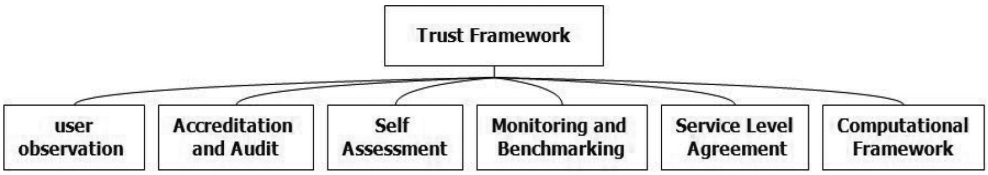

Figure 3. Taxonomy of trust frameworks.

towards that provider and the services whereas trust is between two entities. Usually, the high reputation indicates the high trust and customers who need to make trust judgment on a provider, may use the reputation to calculate or estimate the trust level of that provider. The result is a comprehensive score reflecting the overall opinion of the CSCs or a small number of scores on several major aspects of performance [9]. The social network based approach is an analog of how a person initially trusts an entity, unknown before in the real world. Moreover, when a cloud user has only limited direct experience with a cloud service, other users' opinions could be an important source of cloud attribute assessment.

Self-assessment: It is a free publicly accessible registry which allows CSPs and CIdPs to publish self-assessment of their security controls, in either a questionnaire or a matrix. It shows and determines how CIdPs and CSPs align with the security guidelines. However, the information offered is a cloud provider's self -assessment; cloud users may want assessments performed by some independent third-party professional organizations like CSA stare two and three [10].

Accreditation and audit: Generally, the trust elements and characteristics of CSPs need to be verified before use for decision CSCs' decision making. Therefore, it is expected assertions from third-party independent professional organizations. Trust solution provides cloud users a solution where the overall processes of cloud trust management can be delegated to third-party professionals. Though, similarly, the basis for cloud users to trust them needs to be established. Therefore, one possible solution is formal accreditation and audit to the trust mechanism problems. Auditing and risk assessment will be considered in this book chapter as a category of trust establishment and independent authority in the identity area. External audits, attestations, or certifications for the more general purpose have been used in practice.

Monitoring and benchmarking: It is needed to continuously measure and assess infrastructure or application behavior for performance, reliability, power usage, ability to meet SLAs and security to perform business analytics, for improving the operation of systems and applications, and for several other activities.

Service level agreement: In practice, one way to establish a trust for cloud providers is the fulfillment of SLAs. SLA validation and monitoring schemes are used to quantify what exactly a cloud provider is offering and which assurances are actually met [11]. Numerous works have been carried out to define SLA metrics in cloud computing. The SLA metrics selected in this study assess the cloud services from appropriate cloud providers and help this research to find the SLA gaps.

Computational framework: It is focusing on mathematically formal frameworks for measuring the level of trust, including modeling, languages, and algorithms for computing trust. It is integrated method of previous methods and new methods to eliminate trust elements, prioritize, formulate and disseminate level of providers' trust [12].

To answer for the second question, in this analysis step, this research seeks to draw upon key findings from related work on cloud computing, federated identity management, and trust computing, which aim to extend these trust elements through identifying characteristics and attributes of cloud and cloud identity providers. To do so, in this book chapter question number two has been split into two questions and struggles to answer these two questions which have been mention before.

Between cloud provider and cloud consumer, what are the Essential System Attributes (ESA) of trust establishment?

Between CIdPs and CIdUs, what are the Essential System Characteristics (ESC) of published trust establishment method?

Figure 4 illustrates the components of common trust framework which is based on the [13]. Based on this figure, as shown, indirect information like recommendations and direct observations are valuable for the any TSPs, CIdP, and CSPs. Moreover, the trust level is dynamic based on the provider interaction. Therefore, the trust level is based on the different factors such as but not limited monitoring, trust background and history, qualitative, and quantitative elements.

Therefore, the cloud customers will have the ability to select the services based on the ranking, real-time performance and. However, the key elements for the common trust frameworks based on the literature and previous research are:

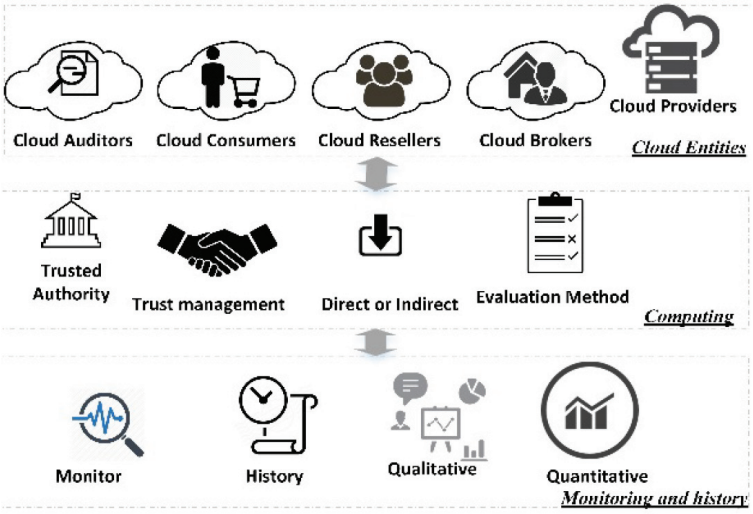

Figure 4. Service trust evaluation system architecture.

Cloud entities: This part responsible for communication with cloud customers and understanding their level of trust and application, and search and ranking of suitable trusted services using other components such as but not limited the direct or indirect trust, evaluation method, and trust management.

Monitoring and history information: this part searches for providers that can provide customers' requirements. Therefore, the direct and indirect trust will be monitoring during the time of service providing. In the meanwhile, these results will be saved in the trust level's database of the specific provider.

Computing service network structure and catalog: One of the main feature of cloud is transparency, which help the CSPs to advertise their features. Therefore, measurement of various service trust evaluation and the trust evaluation of service providers are two issues which arise based on this research and previous researches [12, 14, 15] which will be identified in this book chapter. A set of dimensions to study trust management issues where each layer of the framework has several dimensions have been identified in this section. These dimensions are identified by considering the highly dynamic, distributed, and non-transparent nature of cloud environments. Therefore, in this book chapter the dimension for the evaluation has been categorized in three separate areas which will be explained in the rest of this section.

2.2.1. Cloud entities

Cloud brokers, cloud resellers, cloud consumers, and cloud auditors are four primary entities in the cloud evaluation environment [16]. They each playing a different role and were identified by NIST [17]. However, in this sub-section, five cloud entities' trust evaluation issues will be explained and their trust relationship will be identified.

Credibility: It refers to the quality of the information or service that makes cloud entities trust the information or service [18, 19]. The credibility evaluation appears in several forms including the entity's credibility and the feedback credibility. For instance, lack of proper identity scheme, will cause easily leads to low accuracy of the trust level because trust management system suffers attacks such as Sybil attacks [20].

Privacy: The transparency feature of the CSPs and interactions with the Service Measurement Index (SMI), or Cloud Security Alliance Security, Trust & Assurance Registry (CSA STAR) suffers the privacy of the providers because it discloses the sensitive information of the entities. Indeed, cryptographic encryption techniques is essential when these providers interact with trust system management, but, the point is these techniques are inadequate in cloud environments due to its highly dynamic and distributed nature [21].

Personalization: It refers to the degree of autonomy in which the cloud entities adhere to the trust management rules. Both can have proper personalization in their feedback designs and executions. This means that cloud entities can select the trust process and the techniques they prefer. Personalization is applicable if the trust management system has fully autonomous collaboration, where each participant needs to interact via well-defined interfaces that allow participants to have control over their trust level and the flexibility to change their trust

processes without affecting each other. It is difficult to have a fully autonomous collaboration because of the complex translation features it requires [22].

Integration: It refers to the ability to integrate different trust management perspectives and techniques. Entities can give their security elements from different perspectives through different trust management techniques. Combining several trust management techniques can generally increase the accuracy of the trust results [23].

Security: It refers to the degree of dissemination protection that the entities and trust assessments has against malicious behaviors and attacks. The Cloud Trust Protocol (CTP) [24] is the mechanism by which some of the cloud entities ask for and receive information about the elements of transparency as applied to cloud service providers. The primary purpose of the CTP and the elements of transparency is to generate evidence-based confidence that everything that is claimed to be happening in the cloud is indeed happening as described.

2.2.2. Computing

A trust evaluation system should be able to evaluate and compute the trust relationships between CSPs and CSCs, which will significantly affect the level of trust. On the other hand, identifying trust computing methods and their perspectives, techniques, adaptability, security, and scalability are remained an important challenging issues in the trust management area [14, 25]. Therefore, in this sub-section the importance of these issues will be explained.

Perspective: Some trust management approaches focus on the CSP's perspective while others focus on the CSC's perspective. It is therefore crucial to determine the perspective supported by a trust assessment function. The more perspectives the trust management system supports, the more comprehensive the trust management system becomes [26].

Technique: It refers to the degree to which a technique can be adopted by the trust management system to manage and assess trust attributes. It is important to differentiate between the trust assessments functions that adopts a certain technique for trust management from the ones that adopt several trust management techniques together. Adopting several trust management techniques together can increase the accuracy of the trust results [9].

Adaptability: It refers to how quickly the trust assessment function can adapt to changes of the inquisitive cloud entities. Some trust assessment inquiries can follow certain customized criteria from the inquisitive parties (e.g., weighing the elements based on the user's expectation), while others may follow the general trust assessment metric. In addition, updating trust results may be used as another indicator of adaptability because of the highly dynamic nature of cloud environments where new cloud service providers and consumers can join while others might leave at any time [27].

Security: It refers to the degree of robustness of the trust assessment function against malicious behaviors and attacks. The computing function security level and the communication security level are two different security levels where attacks can occur. In the computing layer, there are several potential attacks against the trust assessment function including whitewashing, self-promoting, and slandering [28]. At the communication security level, there are several attacks

such as Man-in-the-Middle (MITM) attack and Denial-of-Service (DoS) attack or distributed Denial-of-Service (DDoS) attack [29].

Scalability: It is important that the cloud computing trust management system be scalable because it is highly dynamic and distributed nature of cloud environments. It refers to the ability of the trust computing system to grow in one or more characteristics. Trust models that follow a centralized architecture are more prone to several problems including scalability, availability, and security [30].

2.2.3. Monitoring and history

A trust evaluation system should be able to measure the truthfulness of entities based on the qualitative, quantitative, Semi-qualitative, entities' history, and monitoring methods [3, 14, 15, 18, 27]. Hence, a reliable trust management system depends on the response time, redundancy, and accuracy and capability of collecting and filtering the trust essential attributes and characteristics.

Response time: Lack of fast responding or delay to handle trust assessment inquiries by the trust framework leads inaccuracy of the distribute trust results, particularly when there is a significant number of CSPs and CSCs [31, 32].

Redundancy: As redundancy is one of the main attributes of cloud, consequently, the degree of the trust management redundancy is crucial to manage and assess the trust feedback. There are two redundancy approaches in cloud environment: First, assessment redundancy which occurs when multiple trust assessment inquiries are issued sequentially for the same cloud service. Second, data redundancy used to avoid scalability and monitoring issues. Redundancy causes resource waste and eventually affects the performance of the trust management system [33].

Accuracy: it refers to the degree of correctness of the monitoring, history, quantitative or qualitative results that can be determined through one or more accuracy attributes such as the unique identification of trust characteristics and using the proper techniques to disseminate the trust level. Poor identification of characteristics can lead to inaccurate trust results [9].

2.3. Evaluation yardstick

A yardstick can be defined as the ideal target which is trust identity management against which the real target is to compare. Yardstick [8] is a measure of standard used for comparison or to judge a certain target. For example, grouping evaluation criteria and then compare these criteria one by one with the yardstick is one of the most well-known approaches. In this study, criteria are categorized and evaluated depending on cloud trust framework and past experiences and knowledge.

2.3.1. Trust framework and past experience

Lack of the proper information and past experience of the CSPs leads the weak decision by the CSCs. Hence, many researchers [3, 27, 34–36] have conducted a research to compare and

evaluate the level of the services that user gain by the CSPs. For example, in a typical distributed environment [37], an agent (trustier) is acting in a domain where he needs to trust other agents or objects, whose ability and reliability are unknown. The trustier agent queries the trust system to gather more knowledge about the trustee agent and better ground its decision. However, a trust-based decision in a specific domain is a multi-stage process. But, the first step is the identification and selection of the appropriate input data. These data are in general, domain-specific, and identified through an analysis conducted over the application.

2.4. Data gathering techniques

"You can't control what you can't measure ([38], p. 1)". Measurement, assignation, and opinion are three main data-gathering techniques used in most evaluations in the IT environment. They are required to obtain data to analyze each evaluation criterion [8]. Measurement involves the use of the appropriate documents and guidelines to extract the criteria. For the assignation, documentation inspection has been assigned. Besides, observation techniques for getting subjective criteria data has been applied for opinion step. The primary goal of this part is to provide decision makers (CIdUs and CSCs) with information as complete as possible. In this book chapter, document review and numerous guidelines such as National Checklist Program for IT Products [39], Union Agency for Network and Information Security (ENISA) Auditing Framework for Trust Service Providers [40], and National Institute of Standards and Technology (NIST) Guidelines for Access Control System Evaluation Metrics [41] are the main data gathering techniques that used to collect data and information regard each criteria. Document reviews method of gathering data by reviewing documents that provide information about the characteristics, design, guidelines, requirements, and implementation process related to CIdPs and their responsibilities. While checklist refers to a series of commands and instructions for verifying that the product has been operated correctly [39]. This study used the proposed categorized frameworks as shown in **Figure 2** and proposed ESA which explained in general in 2.2 and will be explained in detail in the next part. The first trust elements (ESA) are developed to identify the essential cloud computing attributes according to cloud security, privacy, and trust attributes. The second trust elements (ESC) is designed to identify the essential cloud identity providers' characteristics regarding trust, security, and privacy.

The aim of ESC of Cloud Identity section is to highlight the major security, privacy, and trust issues in current existing cloud identity computing environments. The detailed analysis of the selected studies is based on their similarities in terms of the trust computing, cloud computing, and cloud identity.

2.5. Synthesis technique

Synthesis technique refers to a set of relative activities and stages to synthesize all information and data which are essential for each system criterion and elaborate in order to evaluate CIdP against [8]. In this book chapter, in order to synthesize the information obtained from documents review and guidelines a hybrid evaluation (cloud identity trust evaluation framework (**Figure 2**)) and ranking technique has been developed by integrated critical interpretive [42] and framework technique [43]. Therefore, better comprehension of the trust elements and

essential cloud identity provider trust characteristics (2.5.1) would enable the identity management systems to design more efficient system and applications for the CIdUs and CSCs and facilitate the adoption of this novel elements in their environments. In turn, this will assist the identity community to promote their contributions and insights into this evolving identity field.

2.5.1. Essential cloud identity provider trust characteristics

There can be several identity providers offering cloud-based identity services with similar functionalities (Habiba et al., [4]). CIdUs are interested to select identity providers not only based on the functional characteristics but also based on non-functional characteristics. This refers to how well CIdP behaves and what sort of capabilities the providers possess regarding non-functional attributes. In Cloud identity environments, according to (Habib et al., 2012) those attributes go beyond the non-functional QoS parameters, which are considered important for selecting trustworthy web service providers.

SLA is a common practice that identity providers consider in order to build a contractual relationship with a potential consumer. In the context of SLA, identity users trust an identity provider to provide compensation in the case of violation of specific clauses in the agreement. Therefore, in this section of research will attempt to identify the ESC of the cloud identity systems. These characteristics would help both CIdUs and CIdPs understand the importance of these features that are worth considering when selecting or implementing the CIDMS. Moreover, PKI is a widely used mature technology that employs trust mechanisms to support, key certification and validation, digital signature, attribute certification and validation. But the question is can researcher apply trust ideas used in PKI to establish trust mechanisms to the cloud? Huang and Nicol [9] identified and answered this question and mentioned that this raises questions that ask about the foundation of that trust, and how the trust is inferred or calculated. They suggested that the trust comes from recommendations along the chain of certificates by those certificate issuers, but the practice of digital certification and validation in real PKI systems suggests that the trust comes from compliance with certain certificate policies. However, certificate policies play a central role in PKI trust, therefore, PKI will be a policy-based trust.

The main goal of the ESC of CIdP is to highlight the major trust, privacy, and security issues in the existing cloud federated identity environments. The method and technique for this part can be summarized as: surveying the major trust, privacy, and security issues that lead threats in the existing cloud federated identity environments; and evaluating the methods which be addressed to minimize this potential trust, privacy, and security threats, and providing a high level of trust, security, and privacy. So, this section analyses the main attributes, which help in assessing the CIdPs operational trust.

2.5.1.1. Balancing

As nowadays is the era of data explosion and big data, especially in the cloud environment and indeed the amount of data storage increases quickly, trust framework should be dynamic and align with the latest technology of the balancing. So, load balancing is one of the main challenges which is required to distribute the dynamic workload across multiple nodes to

ensure that no single node is overwhelmed. However, by balancing and distributing the load between numerous resources, the performance of the services will be improving. Therefore, CSPs and CIdPs should be flexible, automated, and extensible by involving the latest standards and best practices. Meeting these criteria is essential to ensure the long-term success of a cloud balancing strategy. But, combining high availability with security is arising the importance of the resource and infrastructure management. To sum up, the ability to distribute connections across the globe based on device type, geographic location, the state of servers in one location or another, and balanced loads is essential system characteristics [44].

2.5.1.2. Single sign on

Authentication across multiple vendors is one of the first issues that should be solved in Cloud area. SSO technology, regarding data protection, confidentiality, and privacy issues can be limited by the different barriers. SSO streamlines secure access to all applications and resources with one set of credentials, regardless cloud, mobile, web, and VPN resources. The result is an improved user experience and trust without tedious login procedures and high friction authentication workflows and user-friendly. SSO is a simple solution to user identity issues because since they are already authenticated, no password is required and because no password is required, there is no password for anyone to steal. It increased application adoption, employee productivity, and decreased helpdesk costs [45].

2.5.1.3. Lifecycle

The goal of cloud lifecycle management is to manage the dynamic nature of the cloud environment, accelerating provisioning, facilitating flexibility, and rapidly meeting the needs of the business. With the cloud lifecycle management solution, organizations can deliver flexible, customizable cloud services while maintaining a structured, controlled, and dynamic IT environment. Moreover, Iriberri and Leroy [46] indicated the features that should be selected and gradually added depending on the type of community under development and the purpose of the community as shown in **Figure 5**.

2.5.1.4. Privacy

Identity management systems have existed offering privacy and anonymity in a the cloud environment for CIdUs [47]. Trust management, as well as efficient CIDMS and user keys, are required to achieve privacy. It is therefore difficult to design a system which provides privacy and security to the sensitive CIdUs' data. As a result, there is a significant gap between CIDPs' claim and CIdUs' views of the cloud's privacy and security [48].

2.5.1.5. Risk

Among all privacy and security issues, this part treats the challenges posed by identity management in the cloud, focusing on risk assessment. Federation as a vital feature of cloud and cloud identity needs strong integration, cooperation, and collaboration among different clouds. Consequently, it introduces complex tasks in risk assessment to quantify CIdPs and investigate new metrics in the CIDMS [49]. Djemame, Armstrong, Guitart, and Macias [50] designed a risk assessment model and focused on a specific aspect of risk assessment applied

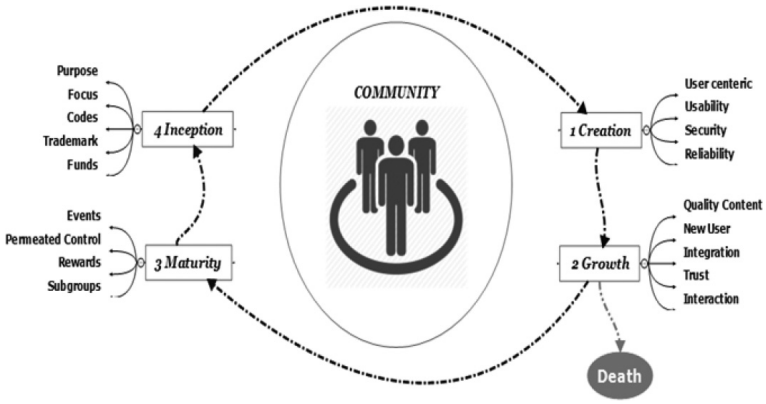

Figure 5. Online community life-cycle perspective ([45], p. 9).

in cloud computing and they described the various stages in the service lifecycle whereas risk assessment takes place. Theoharidou et al. [51] examined privacy risk assessment for cloud and identifies threats, vulnerabilities, and countermeasures that clients and providers should implement in order to achieve privacy compliance and accountability.

2.5.1.6. Standard

Securing information and the systems that store, process, and transmit users' identity information is a challenging task for organizations. Standardized facilitates to collect, verify, and update system security configurations and they can work in concert or be implemented separately. It also would allow authentication to be automated. The goal of any authentication standard is to produce technical specifications that define an open, scalable, interoperable set of mechanisms that reduce the reliance on passwords to authenticate users and to operate industry programs to help ensure successful worldwide adoption of the user authentication.

There are six methods and standards that industry collaborates to make major progress in term of mitigating identity theft and improve strong authentication. The first one continues with Fast IDentity Online (FIDO) [52] to eliminate the password by strong authentication tight with the hardware. There is a need of keep working with fishing protection like Internet Engineering Task Force (IETF) [53] and Organization for the Advancement of Structured Information Standards (OASIS). Work for share intelligence and IP practically OpenID Connect Reduced Instruction Set Computing (OIDC-RISC) is super important for the strong authentication. There are two new methods, token binding and session revocation. The aim of token binding is to mitigate impersonate a user identity by binding token with hardware against man in the middle attack. CIdUs want to revoke all sessions and access tokens that have been handed out.

2.5.1.7. Eliminating password

Fast Identity Online (FIDO) and Wide Web Consortium (W3C) (WebAuthn) could eliminate, or at least significantly mitigate the risk of passwords. The mission of these standards is to define a client-side API that provides strong authentication functionality to Web Applications.

This specification standard helps simplify and improve the security of authentication. As the steward for the Web platform, the W3C is uniquely positioned to focus the attention of Web infrastructure providers and developers on the shortcomings of passwords and the necessity of their replacement. The FIDO protocol employs public key cryptography, relying on users' devices to generate key pairs during a registration process. The user's device retains the generated private key and delivers the public key to the service provider. The service provider retains this key, associates it with a user's account, and when a login request is received, issues a challenge that must be signed by the private key holder as a response [54].

2.5.1.8. Phishing protection

Phishing is a technique that involves user to steal confidential information and passwords by using email. Security Automation and Continuous Monitoring (SACM) reuse existing protocols, mechanisms, information and data models preferably Internet Engineering Task Force (IETF) standards that could support automation of asset, change, configuration, and vulnerability management. Therefore, Trusted Automated Exchange of Indicator Information (TAXII), Cyber Observable Expression (CybOX), and Structured Threat Information Expression (STIX), as some common foundational cybersecurity specifications are now being advanced through the OASIS and they will support sharing for cyber security situational awareness, automated information analysis, real-time network defense, and sophisticated threat characterization and response. Obviously, Security professionals are overwhelmed and simply do not have time for analyzing data in disparate formats. Therefore, TAXII, CybOX, STIX are focusing on cyber intelligence to analyzing data in the cloud. Hence, STIX is a language for describing cyber threat information, TAXII defines services and message exchanges that enable organizations to share the information they choose with the providers they choose, however, CybOX is a language for specifying, capturing, and communicating events properties that are observable in cloud area [55]. To sum up, the ability to analyzing the threat and phishing protection is essential system characteristics for any CSPs, and especially any CIdPs.

2.5.1.9. Shared intelligence and IP

The ability to react quickly to identity theft attacks will effectively stop the access of hackers before they grape CSC's information. But, it requires a trusted community wherein organizations share security and threat intelligence, such as IP addresses of attackers, new types of malware or techniques criminals are engaging. The goal of Risk and Incident Sharing and Coordination (RISC) is to provide privacy recommendations, data sharing schemas, and protocols to Share information about critical events in order to thwart attackers from leveraging compromised accounts from one CSPs to gain access to accounts on other CSPs and enable both CSPs and CSCs to coordinate in order to securely restore accounts following a compromise [56]. Therefore, TAXII, CybOX, and STIX are an open community-driven effort that help with the automated exchange of identity theft information. This allows identity theft information to be represented in a standardized format and it is essential system characteristics for any CIdPs. So, the intelligence combination of STIX and TAXII allow researchers and developers to easily share consistence identity information [57].

2.5.1.10. Token binding

CIdPs generate various security tokens such as OAuth tokens for CIdUs to access cloud service providers. Attackers export bearer tokens from CIdU machines or from compromised network connections, present these bearer tokens to CSPs and impersonate authenticated users. Token Binding enables defense against such attacks by cryptographically binding security tokens to a secret held by the CIdU [58].

2.5.1.11. Session revocation

In term of any CIdUs' system compromising, they want a way to revoke all sessions and access tokens that have been handed out. It is important that any outstanding access tokens are not revoked by clicking Logout all. They have to expire naturally. Based on the OIDC standard, Revoke refresh token, SSO Session Idle, SSO Session Max, Offline Session Idle, Access Token Lifespan, and client login timeout are some term should be considered in cloud federated identity management systems [59].

2.5.1.12. Interning of thing

There are seemingly competing, complex security requirements to be deployed on IoT platform with potentially limited resources like authenticate to multiple networks securely, and provide strong authentication and data protection. Thus IoT must be secure in order for its value to be realized. If we do not have confidence of what IoT entity, then we cannot protect the potentially sensitive sensor data being shared or the transactions being conducted [60].

The Cloud Security Alliance (CSA) has established the IoT Working Group (WG) [61] to focus on providing relevant guidance to cloud users who are implementing IoT solutions. Their aim is to provide understandable recommendations to information technology staff charged with securely implementing and deploying IoT solutions considering IoT Identity and Access Management (IAM). Moreover, ISO 27 is to development of standards for the protection of information and ICT. This includes generic methods, techniques, and guidelines to address both security and privacy aspects such as security aspects of identity management, biometrics and privacy [62].

3. Conclusion

In conclusion, the chapter has provided an evaluation framework for the relationship between cloud service providers and cloud service users. It critically evaluates the context and provides an assessment of the current trust models that are available and suggests that further innovation is required. A justification for the selection of a CIdPs is made and a framework for decision-making provided. In addition, data gathering tools have been provided and guidance on the synthesis of theory and data made. A hybrid MCDM technique is advocated for trust evaluation in fuzzy and complex environments, in order to effectively evaluate and prioritize trust elements. Each element of the research contributes a partial view of cloud trust, and the

suggested improvements will lead towards a complete picture of how cloud identity entities work together to form an integrated trust system. It will have a solid grounding in trust, serving to facilitate trusted paths to trusted cloud identity services. Furthermore, these models need to incorporate all aspects of security quantification measures for cloud identity.

Therefore, to evaluate the trust of service nodes scientifically, a new framework and evaluation method is needed to determine the weight of different indexes, and fully reflect the objectivity and accuracy of monitoring attributes. Instead, a whole evaluation framework of trust evaluation is required for CSCs' decision making, which can help them choose and monitor the operation state. In summary, current research of trust evaluation is still in its infancy, and there is yet a considerable problem space to explore and resolve. On the one hand, the influence factors are usually limited, which neglects the other factors which have an effect on trust. Novel trust establishment mechanisms that evaluate the trustworthiness of CIdPs have been advocated and provided (**Figure 2**). Likewise, to support the CIdUs in reliably identifying trustworthy CIdPs, a multi-faceted trust management system architecture for a CIdP is advocated. The concerns of evaluating cloud trust management systems, data gathering, and synthesis of theory and data, have been addressed so that the relationship between cloud identity providers and Cloud identity users can be improved.

Author details

Eghbal Ghazizadeh* and Brian Cusack

*Address all correspondence to: eghaziza@aut.ac.nz

Digital forensic Lab, Auckland University of Technology, New Zealand

References

[1] Blaze M, Feigenbaum J, Lacy J. Decentralized Trust Management. pp. 164-173

[2] Calheiros RN, Ranjan R, Beloglazov A, De Rose CA, Buyya R. CloudSim: A toolkit for modeling and simulation of cloud computing environments and evaluation of resource provisioning algorithms. Software: Practice and Experience. 2011;**41**(1):23-50

[3] Habib SM, Hauke S, Ries S, Mühlhäuser M. Trust as a facilitator in cloud computing: A survey. Journal of Cloud Computing. 2012;**1**(1):1-18

[4] Habiba U, Masood R, Shibli MA, Niazi MA. Cloud identity management security issues & solutions: A taxonomy. Complex Adaptive Systems Modeling. 2014;**2**(1):1-37

[5] Noor TH, Sheng QZ. Trust as a service: A framework for trust management in cloud environments. In: Web Information System Engineering–WISE 2011. Springer; 2011. pp. 314-321

[6] Al-Sharawneh J, Williams M. Credibility-Based Social Network Recommendation: Follow the Leader. pp. 1-11

[7] Alabool HM, Mahmood AKB. A novel evaluation framework for improving trust level of infrastructure as a service. Cluster Computing. 2015:1-22

[8] Lopez M. An Evaluation Theory Perspective of the Architecture Tradeoff Analysis Method (ATAM), DTIC Document. 2000

[9] Huang, Nicol DM. Trust mechanisms for cloud computing. Journal of Cloud Computing. 2013;**2**(1):1-14

[10] Samani R, Reavis J, Honan B. CSA Guide to Cloud Computing: Implementing Cloud Privacy and Security: Syngress. 2014

[11] Saleh ASA, Hamed EMR, Hashem M. Building Trust Management Model for Cloud Computing. pp. PDC-116-PDC-125

[12] Huang L, He X, Liao HD, Ji M. Developing a trustworthy computing framework for clouds. International Journal of Embedded Systems. 2016;**8**(1):59-68

[13] Wang L, Li X, Yan X, Qing S, Chen Y. Service dynamic trust evaluation model based on Bayesian network in distributed computing environment. Distributed Computing. 2015;**9**(5)

[14] Hallappanavar VL, Birje MN. Trust Management in Cloud Computing. Security Solutions for Hyperconnectivity and the Internet of Things. 2016:151

[15] Shaikh R, Sasikumar M. Trust model for measuring security strength of cloud computing service. Procedia Computer Science. 2015;**45**:380-389

[16] Chhabra S, Dixit VS. Cloud computing: State of the art and security issues. ACM SIGSOFT Software Engineering Notes. 2015;**40**(2):1-11

[17] NIST. NIST Cloud Computing Standards Roadmap. 2013

[18] Wu X, Zhang R, Zeng B, Zhou S. A trust evaluation model for cloud computing. Procedia Computer Science. 2013;**17**:1170-1177

[19] ABC4Trust, "Attribute-Based Credentials for Trust. European Union Funded Project of the 7th Framework Programme.," 2015

[20] Pecori R. S-Kademlia: A trust and reputation method to mitigate a Sybil attack in Kademlia. Computer Networks. 2016;**94**:205-218

[21] Alaqra A, Fischer-Hübner S, Groß T, Lorünser T, Slamanig D. Signatures for privacy, trust and accountability in the cloud: Applications and requirements. In: Privacy and Identity Management. Time for a Revolution? Springer; 2016. pp. 79-96

[22] Aguirre E, Mahr D, Grewal D, Ruyter de K, and Wetzels M, Unraveling the personalization paradox: The effect of information collection and trust-building strategies on online advertisement effectiveness. Journal of Retailing. 2015;**91**(1):34-49

[23] Zhang M, Huo B. The impact of dependence and trust on supply chain integration. International Journal of Physical Distribution & Logistics Management. 2013;**43**(7):544-563

[24] DiMaria J. CloudTrust Protocol Working Group; https://cloudsecurityalliance.org/group/cloudtrust-protocol/

[25] Alshehri MD, Hussain FK. A Comparative Analysis of Scalable and Context-Aware Trust Management Approaches for Internet of Things. pp. 596-605

[26] Noor TH, Sheng QZ, Zeadally S, Yu J. Trust management of services in cloud environments: Obstacles and solutions. ACM Computing Surveys (CSUR). 2013;**46**(1):12

[27] Noor TH, Sheng QZ, Maamar Z, Zeadally S. Managing Trust in the Cloud: State of the art and research challenges. Computer. 2016;**49**(2):34-45

[28] Luo, Liu J, Xiong J, Wang L. Defending against Whitewashing Attacks in Peer-To-Peer File-Sharing Networks. pp. 1087-1094

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

[30] Lehrig S, Eikerling H, Becker S. Scalability, Elasticity, and Efficiency in Cloud Computing: A Systematic Literature Review of Definitions and Metrics. pp. 83-92

[31] Pearson S. Privacy, security and trust in cloud computing. In: Privacy and Security for Cloud Computing. Springer; 2013. pp. 3-42

[32] Dane E, Rockmann KW, Pratt MG. When should I trust my gut? Linking domain expertise to intuitive decision-making effectiveness. Organizational Behavior and Human Decision Processes. 2012;**119**(2):187-194

[33] Messina F, Pappalardo G, Rosaci D, Sarné GM. A Trust-Based, Multi-Agent Architecture Supporting Inter-Cloud Vm Migration in Iaas Federations. pp. 74-83

[34] Jahani A, Khanli LM. Cloud service ranking as a multi objective optimization problem. The Journal of Supercomputing. 2016:1-30

[35] Sun D, Chang G, Sun L, Wang X. Surveying and analyzing security, privacy and trust issues in cloud computing environments. Procedia Engineering. 2011;**15**:2852-2856

[36] Corradini F, De Angelis F, Ippoliti F, Marcantoni F. A Survey of Trust Management Models for Cloud Computing. 2015

[37] Dondio P, Longo L. Trust-based techniques for collective intelligence in social search systems. In: Next Generation Data Technologies for Collective Computational Intelligence. Springer; 2011. pp. 113-135

[38] Hillary N, Madsen K. You cannot Control What you cannot Measure, OR why it's Close to Impossible to Guarantee Real-Time Software Performance on a CPU with on-Chip Cache

[39] Quinn SD, Souppaya M, Cook M, Scarfone K. National Checklist Program for IT products —Guidelines for checklist users and developers. NIST Special Publication. 2011;**800**:70

[40] Barreira I, Fiedler A, Miękina A, Wanko C, Górniak S. Auditing framework for TSPs, https://www.enisa.europa.eu/publications/tsp1-framework

[41] Hu VC, Kent KA. Guidelines for Access Control System Evaluation Metrics: Citeseer, 2012

[42] Dixon-Woods M, Cavers D, Agarwal S, Annandale E, Arthur A, Harvey J, Hsu R, Katbamna S, Olsen R, Smith L. Conducting a critical interpretive synthesis of the literature on access to healthcare by vulnerable groups. BMC Medical Research Methodology. 2006;**6**(1):1

[43] Dixon-Woods M. Using framework-based synthesis for conducting reviews of qualitative studies. BMC Medicine. 2011;**9**(1):1

[44] Gopinath PG, Vasudevan SK. An in-depth analysis and study of load balancing techniques in the cloud computing environment. Procedia Computer Science. 2015;**50**:427-432

[45] Moreno-Vozmediano R, Montero RS, Llorente IM. Key challenges in cloud computing: Enabling the future internet of services. Internet Computing, IEEE. 2013;**17**(4):18-25

[46] Iriberri A, Leroy G. A life-cycle perspective on online community success. ACM Computing Surveys (CSUR). 2009;**41**(2):11

[47] Khalid U, Ghafoor A, Irum M, Shibli MA. Cloud based secure and privacy enhanced authentication & authorization protocol. Procedia Computer Science. 2013;**22**:680-688

[48] Kshetri N. Privacy and security issues in cloud computing: The role of institutions and institutional evolution. Telecommunications Policy. 2013;**37**(4):372-386

[49] Arias-Cabarcos P, Almenárez-Mendoza F, Marín-López A, Díaz-Sánchez D, Sánchez-Guerrero R. A metric-based approach to assess risk for "on cloud" federated identity management. Journal of Network and Systems Management. 2012;**20**(4):513-533

[50] Djemame K, Armstrong D, Guitart J, Macias M. "A Risk Assessment Framework for Cloud Computing," 2014

[51] Theoharidou, Papanikolaou N, Gritzalis D. Privacy Risk, Security, Accountability in the Cloud. pp. 177-184

[52] Loutfi I, Jøsang A. Fido trust requirements. In: Secure IT Systems. Springer; 2015. pp. 139-155

[53] Zhu L, Tung B. "Public Key Cryptography for Initial Authentication in Kerberos (PKINIT). IETF," 2015

[54] Jyotiyana JP, Mishra A. Secure authentication: Eliminating possible backdoors in client-server endorsement. Procedia Computer Science. 2016;**85**:606-615

[55] Alsharnouby M, Alaca F, Chiasson S. Why phishing still works: User strategies for combating phishing attacks. International Journal of Human-Computer Studies. 2015;**82**:69-82

[56] OpenID. "RISC (risk and incident sharing and coordination) WG," http://openid.net/wg/risc/

[57] Leicher A, Schmidt AU, Shah Y. Smart OpenID: A Smart Card Based OpenID Protocol. pp. 75-86

[58] Li W, Mitchell CJ. Security Issues in OAuth 2.0 SSO Implementations. pp. 529-541

[59] Yan L, Rong C, Zhao G. Strengthen Cloud Computing Security with Federal Identity Management Using Hierarchical Identity-Based Cryptography. pp. 167-177

[60] Mahalle PN, Anggorojati B, Prasad NR, Prasad R. Identity authentication and capability based access control (iacac) for the internet of things. Journal of Cyber Security and Mobility. 2013;**1**(4):309-348

[61] Russell B. "Internet of things working group," https://cloudsecurityalliance.org/group/internet-of-things/

[62] Disterer G. "Iso/Iec 27000, 27001 and 27002 for Information Security Management," 2013