Formulating Methodology to Build a Trust Framework for Cloud Identity Management

Full Paper

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

Eghbal Ghazizadeh
AUT University
eghaziza@aut.ac.nz

Abstract

The vital element in outsourcing data to the cloud is trust and trustworthiness that information is protected, unaltered and available on demand. To facilitate service expectations efficient and effective infra-structures are required to host the functional processes. A principle security process is identity management that provides authorisation for access rights based on verification checks. In this paper cloud security architecture is reviewed by focusing on the issue of trust and the role of identity management design. Methodology is built to produce cloud artefacts and then it is theoretically applied to produce an innovative solution to assess cloud identity providers (CIdP). Such a design solution lays out an information security architecture that enhances utility for CIdPs and gives better options for users to make trust decisions in the cloud. The contribution of the research is to provide a generic methodology that may be applied to evaluate other security artefacts for the cloud environment.

Keywords

Trust, Cloud, Cloud Identity, Security, Privacy, Design

Introduction

Cloud computing integrates various computing technologies to provide services to the end users. Goutas et al. (2016) defines cloud computing as: “an on demand network service that allows individual users or businesses to access configurable resources. It can also be defined as an on-demand delivery model enabling the synchronised delivery of computing resources... there are three cloud computing delivery models, software as a service (SaaS), ... platform as a service (PaaS) and, infra-structure as a service (IaaS)“ (p.90). The NIST’s (2013) definition of the cloud computing is widely applied and it puts that cloud computing has four separate models of service provisioning which are common characteristics, essential characteristics, service models, and deployment models. Five essential features of the cloud computing are broad network access, resource pooling, on-demand self-service, and measured Service.

These features are all made accessible through the network (Internet) and on-demand by self-service. The services are made available to multiple consumers simultaneously and hence responsive resource pooling and scalability are two key performance requirements. In addition to the four service delivery models, Ali et el., (2015) described one particular approach named Anything-as-a-Service (XaaS), referring to the fact that the cloud systems are able to support and offer everything, in the form of services, ranging from large resources to personal, specific, and granular requirements. Examples include Trust-as-a-Service (TaaS), Identity-as-a-Service (IDaaS), Data-as-a-Service (DaaS), Routing-as-a-Service (RaaS), and Security-as-a-Service (SecaaS). Figure 1 summarises the scope of characteristics and models depicted in the literature. An identity management system describes the management of individual identities, their authentication, authorization, roles, and privileges within or across a system. Storing and managing of identities is crucial to security concerns for cloud services and necessary for end user confidence. These issues are also crucial for the cloud user to increase their trust towards a cloud provider and the services. Various challenges for implementing identity management systems are found in; trust in a provider to authenticating their users, authentic and integrated storage of identities and the recycling of identities. These are central problem areas that require further research (Goutas et al., 2016). Every cloud service has a method of managing identities that may address some or all these challenges but a user requires to know the trust that may be put in the service. The techniques and methods used can be measured by the trust measurement system to help a user to make a good decision

(Shaikh et al. 2013). Each cloud service provider needs relevant and efficient measures for turning cybersecurity from an uncontrollable extra cost into an efficiently managed competitive advantage. To run a trusted cloud business, an organization utilizing cloud-based services requires trusted operations, trusted networks and trusted products enabling trusted services. Data integrity and data encryption technologies with other security orchestration and management tools enable and promote trust in the cloud area (Habib et al. 2012). The biggest challenge is to make these mechanisms of trust visible to the end user and to provide metrics on which they may confidently choose the service.

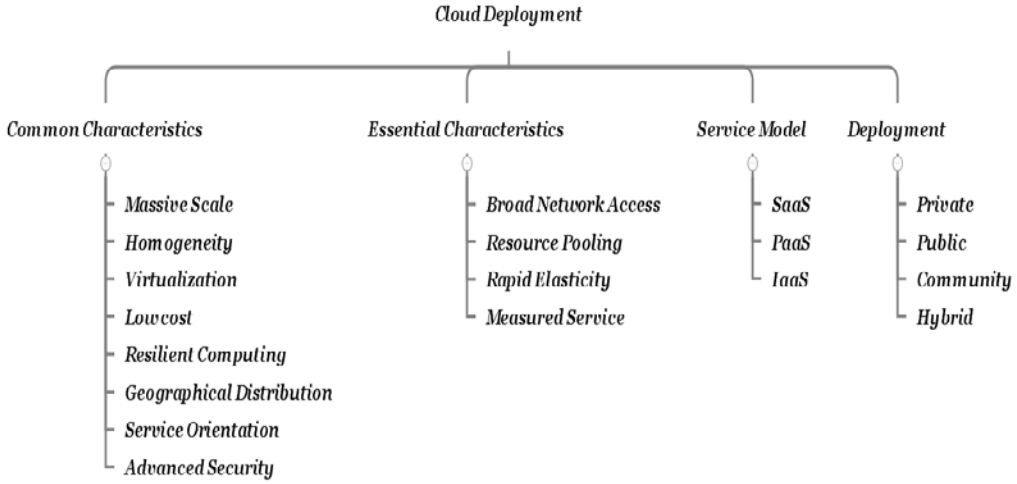

Figure 1: Cloud Characteristics and Deployment Models

To address the problem of security architecture for cloud identity management systems we propose a mediated architecture where the end user has access to data that reports the trust measure of each CIdP. These decisions can also be automated so that when machine to machine interaction occurs decisions can be made on trust measures. In this paper a brief review of literature is made of Cloud Identity and trust computing. A research process for conducting design science in cloud and cloud identity environments is developed based on design science methods (Offermann et al. 2009). The process combines qualitative and quantitative research methods used in IS studies to guide the overall research process (Gregor et al. 2013; Johannesson et al. 2014b). Our motivation stems from the aim of creating a method for the cloud environment and the potential to generalise to other security artefacts. The select review of relevant literature relating to defining Cloud Computing, Cloud Identity, Trust Computing, and the related security issues is made. The brief review provides a context for the problem and the proposed solution.

Cloud Identity

Identity Management (IDM) is a key element for cloud security, and in general for the secure use of any internet services. Every cloud service has a process of generating identities for the cloud users. The process can be examined to determine the security strength associated and it can be reported to users. Identity generation is one of the trust components of an IDM system. Various parameters relevant to the IDM process include identity creation, storage and the life cycle management of the identity. These processes can be measured against the IDM strength component of a trust model.

Cloud computing is a union of various technologies to meet the demands of a mutually dependent network of software and services. This necessitates several IDMs, based on various technologies to interoperate and to function as one consolidated body over a cautiously shared user space. The challenge in this area is a movement towards outsourcing the IDM. The concept of identity-management-as-a-service (IdMaaS) is also developing. IdMaaS vendors focus on comprehensive, interoperable and quick-to-deploy solutions. OpenID, SAML, OAuth, Higgins, Identity Mixer, and OpenID Connect are some popular identity management technologies and solutions which allow the end users to manage their personal attributes required for accessing services. Figure 2 shows the example of entities and relationships in a secure architecture. *OpenID Connect* (Sakimura et al. 2014) is a simple identity layer on top of the OAuth 2.0 protocol. It allows Clients to verify the identity of the end user based on the authentication performed by an Authorization Server, as well as to obtain basic profile information about the end user in an interoperable and trusted manner.

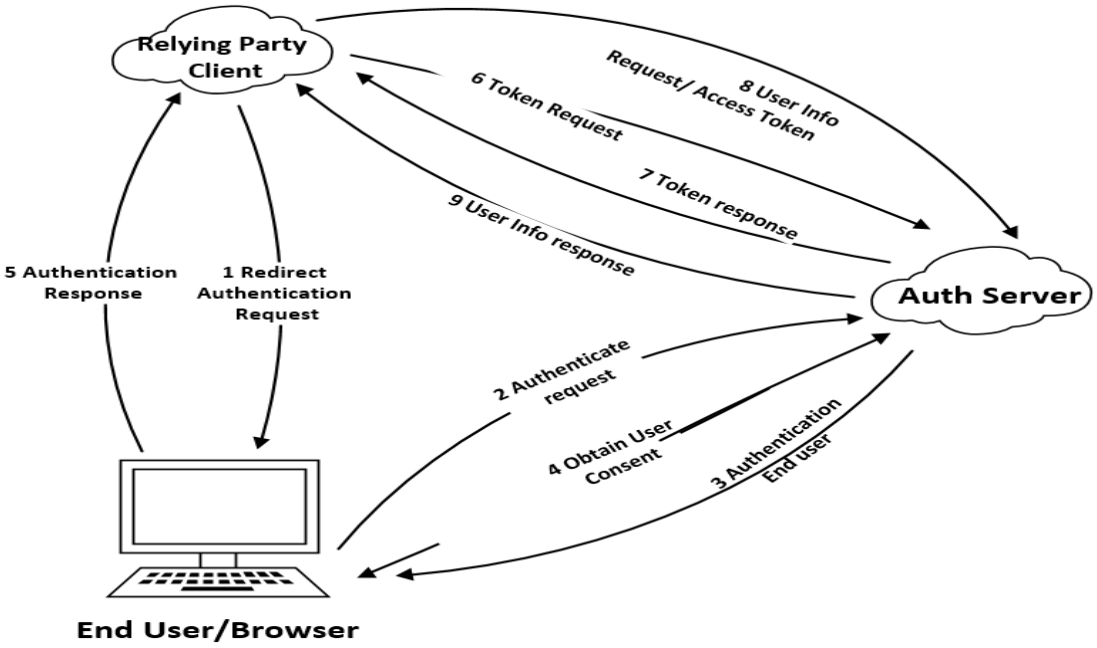

Figure 2: General workflow of OpenID Connect.

The literature analysis suggests that IDMS are inconsistent in supporting essential security features and each has their own adoption of different standards. Identity management systems need to deploy mechanisms to allow entities to trust each other. This requires measurements, compliance and standardisation agreements. Each requires threat resistance and vulnerability mitigation that prevents an attacker to negatively impact a system. Protection from stealing information, impersonation and acting on the end user behalf, and the interruption of services are critical defences (Dólera Tormo et al. 2012; Marmol et al. 2009). Privacy is a desired feature of any communication system. End users usually want to keep the information of their digital identities secret. However, having information about the end user is increasingly a valuable target for malicious attacks. Furthermore, some organizations do not need to know the real identities of their end users, but they want to collect the behaviour of each of them. Identity management systems have to deploy mechanisms to preserve the end users' privacy. It requires anonymity which means a service cannot know the real identity of an end user, unlink-ability which means a service provider cannot link different end user's accesses and un-traceability which means an identity provider cannot know the services that one of its end users (Mármol et al. 2010).

Trust Computing

While security might be the dominant term when it comes to protection of sensitive data, trust is a much stronger concept that goes beyond confidentiality, availability, integrity, and nonrepudiation (the basic security pillars). Trust tries to formulate a good-faith relationship between computing machines as well as between their users. From the IT perspective, trust is not only about securing the communication channel or authenticating the data sender but also trusting that the sent information are legitimate, they do not include malicious codes and they will not harm the receiver in an unforeseen way. Trust extends to the sender by believing that they will obey the specific communication rules and will not abuse communication by non-responsiveness or selfish behaviour (Fournaris et al. 2014). Trust is a complex concept for which there is no universally accepted scholarly definition. Trust is a psychological state comprising the intention to accept vulnerability based upon positive expectations of the intentions or behaviour of another (Pearson 2013). Moreover, trust is a broader notion than security as it includes subjective criteria and experience. Correspondingly, there exists both hard (security-oriented) and soft trust solutions. 'Hard' trust involves aspects like authenticity, encryption and security in transactions, whereas 'soft' trust involves human psychology, brand loyalty and user-friendliness. An example of soft trust is reputation, which is a component of online trust that is perhaps a company's most valuable asset (Wang et al. 2008). People often find it harder to trust online services than offline services because in the digital world there is an absence of physical cues and there may not be established centralized authorities. The distrust of online services can negatively affect the level of trust accorded to organizations that may have been long respected as trustworthy. Security is a component of trust and the level of security management affects trust (Pearson 2013).

Research Methodology

A substantial literature was reviewed to select four different processes groups to create a methodological context in which cloud security artefacts could be formed. The first process group concerned Trust and the capability to calculate a trust value for an entity. The second process group calculates a reputation measurement for an organisation. The third process group collects the evidence required by the second process group; and the forth process group is capable of building and evaluating a security artefact. The forth process group was guided by Design Science (DS) as an organising framework and philosophy for making and building artefacts. DS has been made relevant to Information Systems (IS) research as a methodology and in this research the framework is applied to IS security (Fournaris et al. 2014). The benefit of the approach is that an artefact may be investigated in context and improved through continuous iterations and testing (Offermann et al. 2009). The purpose of the DS research methodology is not only to develop an artefact but also to answer research questions. Depending on the characteristics and the goals of the research, a researcher can shape the processes to deliver innovative or confirmatory outcomes (Johannesson et al. 2014a). The research is based on four constructs that group process knowledge for trust value (Håvaldsrud et al. 2012), reputation system (Hoffman et al. 2009), evidence (Sun et al. 2012), and Design science (Offermann et al. 2009). As summarised in figure 3.

Development and Specification of Policies for Trust negotiation (DeSPoT) is a method for the trust behaviour which tries to realize opportunities while keeping risks at an acceptable level. The method aims to support decision makers in understanding the potential implications of trust mechanisms without going into the low level details of trust protocols regarding the criteria for risk and trust at an organizational level. The method supports negative as well as positive evidences, sensitive assets, separation between the trust formation and the asset exposure, static adherence check of the policy with respect to the trust policy requirements, and prospects that verify the properties of other prospects which are the general mechanisms behind delegation of trust. The method is built around a five step process of for an organisation. The overview of the five steps of the DeSPoT process is given in figure 3. This method is independent from specific trust negotiation protocols, and does not assume such protocols to be predefined (Håvaldsrud et al. 2012). The overarching goal of a trust and reputation system is to produce a metric encapsulating reputation for a given domain for each identity within the system. Each system receives input from various types of sources. Based on this input, a system produces a reputation metric through the use of a calculation algorithm. Once calculated, reputation metric values are then disseminated throughout the system in advance or on demand as the metric values are requested. Finally, higher-level systems or users can then utilize these reputation metric values in their decision making processes for penalties or rewards in order to achieve the goals of the user application. Figure 3 presents the general structure of a trust and reputation system, including the location of each of the fundamental dimensions and demonstrates how each dimension of the trust and reputation system can be comprised of different components, determining the unique properties of each system. (Hoffman et al. 2009).

In figure 3 we summarise the four process groups of knowledge required for the research as a methodology of aggregated process methods. The DeSPot system collects evidence about the trust in a system and calculates values for each relationship. The FCD aggregates and computes singular values for different risk configurations. The reputation properties of individual objects are assessed, analysed and aggregated with evidence, and then disseminated as reputation scores. The DS process (Offermann et al. 2009) is structured in three main phases “problem identification”, “solution design” and “evaluation” that can interact with each other knowledge group within the research process. Each phase is divided into steps and sequentially; they often refer back to each other. In the first phase of the research process, a problem will be identified. In the second phase, the solution will be designed. Once the solution reaches a sufficient state, the evaluation can be started. Finally, some of the questions which might be answered in the communication step are: How to establish the process and move forward? How to balance between action and reflection and how to enable equal participation? The consequence is that any action that is taken is balanced by evaluation and the outcome of the evaluation can deliver forward propagation to the next phase or a return to an earlier phase for improvement.

The application of the process aggregation is integrated into a DS framework in figure 4. The methodology is structured in four main phases which are the problem identification, the solution design, evaluation and the communication of findings. Design Science is chosen for this study because it is solution oriented and not problem oriented. DS focuses on the creation process and refining of the artefact to get a good quality solution. We are looking for a good quality security solution to the IDM problem. The purpose of this study is to develop a solution for good decision making in a cloud and cloud identity environment. The design and development of the artefact concerns a support system for the cloud identity users by reliably identifying trustworthy cloud identity providers. A solution provides a

means to identify the trustworthy cloud identity providers in terms of different attributes assessed by multiple sources and trust information. In this proposed research a context and a scope is selected that is feasible for testing. The scope of research is narrowed to nine cloud identity standards. Our framework are based on a defined and simple measurement assumption that a cloud identity user might be interested in establishing trust in cloud identity provider and cloud infrastructure.

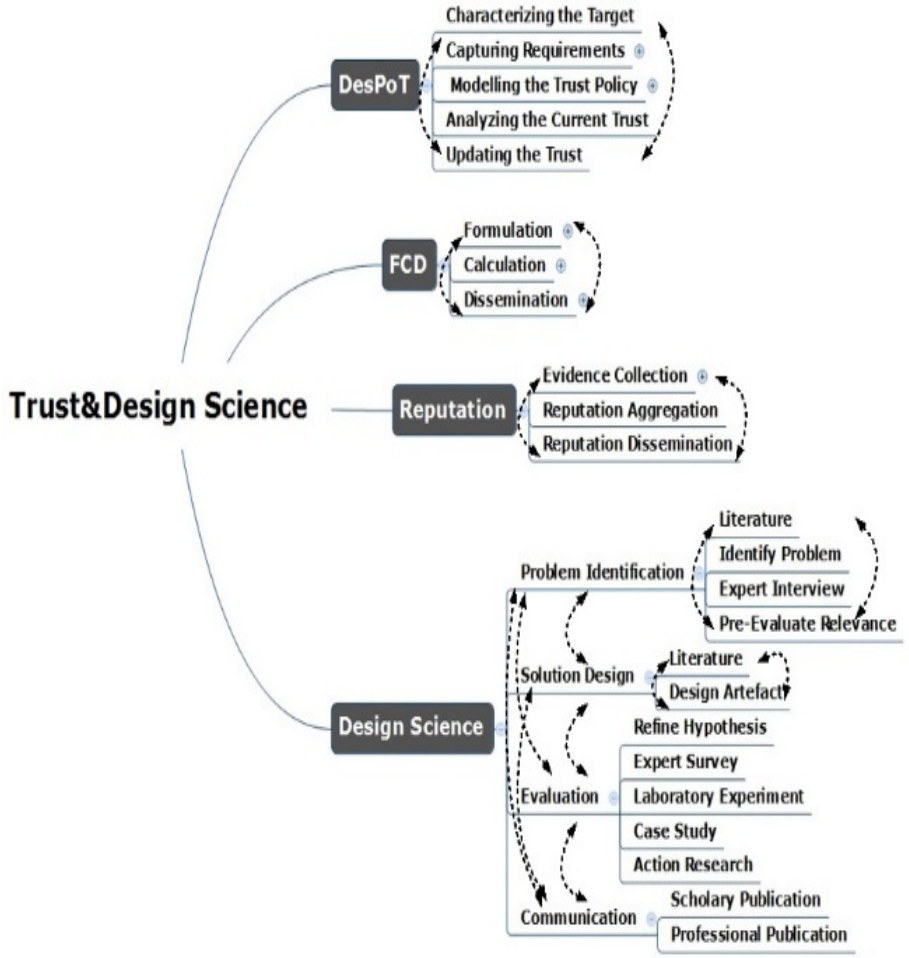

Figure 3. Design Science, Reputation, FCD, and DesPoT methodology

This is directly related to the service delivery of the cloud infrastructure factors. The trust factor expectations are, human factors which could be social trust and trustworthiness. Second, documentation which could be processes, procedures, and policies and third automated management services. The operational trust increases by enhancing documentation and automated management services, and decreases when human factors have greater prominence. The mechanisms for assessing, representing and computing trustworthiness should allow trustees to reliably represent their capabilities and allow trustors to make assessments and decisions regarding the dependability of the trustees. Moreover, the proposed architecture of the system integrates the formal framework and the computational trust mechanisms in order to comply with the requirements for trust systems. The final phase is the communication of the research findings to multiple audiences. The phase is completed in the reporting of the results and any other publications that may arise.

Method Application in Brief

The overview of the Trust Design Methodology (TDS) phases and steps is given in the figure 4. Each phase is divided into steps and the arrows indicate a transition from one step to another. The application of the methodology is elaborated by following and responding to each requirement beginning from problem identification. The following sub sections briefly elaborate the application of the methodology to the security problem of IDMS in cloud environments.

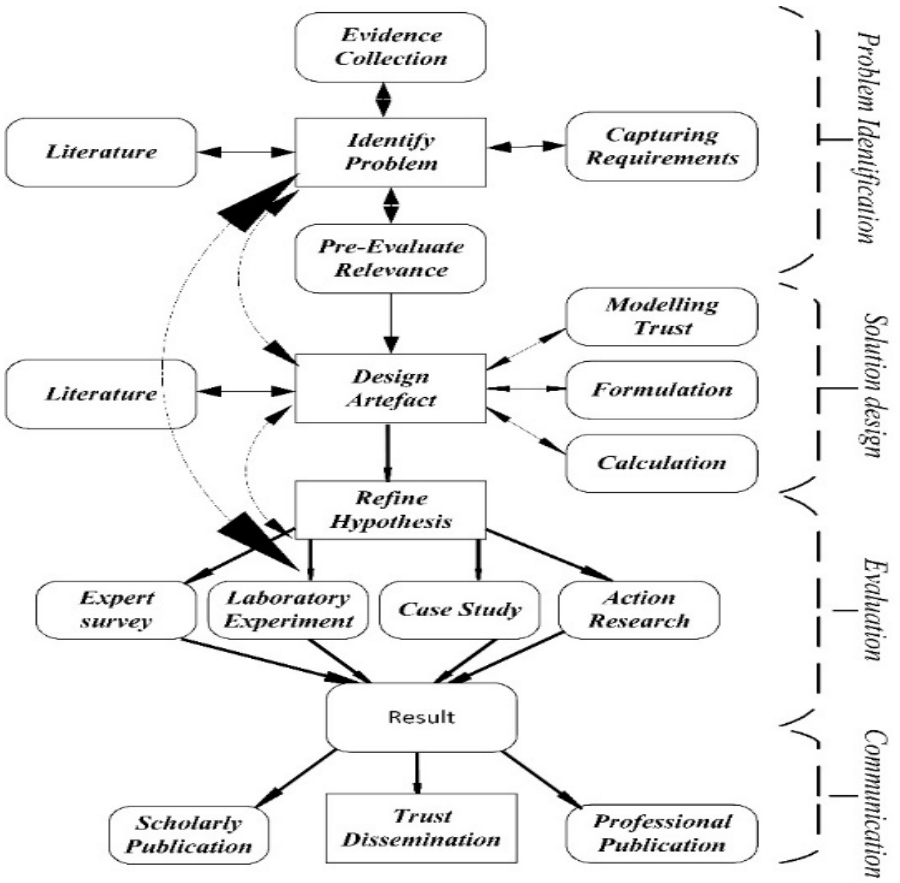

Figure 4. Trust Design Science Methodology

Problem Identification

The problem identification required input from the literature review and the requirements assessment. It is often termed the first entry point for research. Further assessment of relevance was also required. The in-depth analysis of various Cloud based IDMSs showed that most of the systems do not offer support for all essential security management features of Cloud IDMS and the ones that do, are yet to fully address interoperability and standardisation issues (Hashizume et al. 2013). In order to preserve privacy, some systems avoid direct communication between service providers and identity providers, so the latter could not trace an end users' accesses. For example, OAuth and Higgins issue authorization tokens to allow the service providers to directly access the user information under certain conditions, instead of sending the information directly into the token. Hence, the identity provider and the service provider could exchange information even if the end users go offline. Furthermore, in solutions like U-Prove or Idemix, where end users can present attributes without involving the identity provider, attribute revocation is hard to achieve. Additionally, since the identity provider cannot trace an end user accesses, and the end users are completely anonymous to the service provider, it is difficult to provide these systems with accurate audit mechanisms (Tormo et al. 2013). Attribute aggregation is another issue. For instance, SAML, OpenID and OAuth are focused on having a unique identity provider for managing all identity-related information about the end users, and without attribute aggregation. CardSpace, Higgins, U-Prove and Idemix support credentials and attributes from different identity providers, for instance, having an Information card from each of them. However, they do not allow presenting information asserted by different providers at the same time. Identity management systems assume that trust relationships are established, so they usually require the end users attributes to be asserted by a reliable entity (Habiba et al. 2014). However, in many instances researched in the literature these trust attributes are absent in IDMS or the expected attributes are only partially represented. This identifies a problem for end users who must find a way of assessing IDMS and to establish a trust value for each.

Evidence may be obtained from three types of action. The first type is direct observation, usually based on the experiences of the employees of a business or auditor from trusted third party. The second type

is opinions from experts, who have verifiable expertise and provide feedback either voluntarily or for a fee. Both types of evidence are considered reliable, but costly to collect for a large number of objects. Interviews with practitioners and experts in the field can be used to identify relevant and addressed problems. The third type is feedback pis rovided by users, which have been the main source of evidence in most of today's popular reputation systems, such as the product rating system at Aliexpress, Amazon, and Trademe. However, user feedback is also the least reliable source of evidence because it can be easily manipulated (Sun et al. 2012). The trust requirements specify how the target is allowed to use incoming prospects as evidence to form a trust relationship. In general, the trust requirements restrict how the target is allowed to perceive the world with respect to the relationship. The prospect value might be between 1 and 10, and trust level could be Low, Medium, and High. The asset exposure policy requirements specify the trust level the target must have in order to expose assets with a specific value. The trust level is an indirect measure of the likelihood of something going wrong, and the level of this risk can be deduced from the trust level and asset value. The asset exposure policy requirements, hence specify the acceptable risk level in this setting. Pre-evaluation relevance is also required in the problem identification. The main goal of the evaluation is to demonstrate the applicability and technical feasibility of contributions to the domain of cloud identity providers. Customized trustworthiness value, parameters, and weights based on the opinions associated with the domains that are specified by a consumer provide relevance assessment. The pre-evaluation of the relevance of an hypothesis is found by literature research and it is based on analysis (Habib et al. 2012), (Noor et al. 2011), (Saleh et al. 2014), (Shaikh et al. 2015), (Shaikh et al. 2013), (Basin et al. 2011, Chou 2015, Djemame et al. 2014).

Solution Design and Design Artefact

The second entry point is known as the design solution based on the literature research. In contrast to the literature used in the previous step for problem identification, the focus of this step is on relevant scientific publications. This entry point is designed to support the designing of the artefact and the supporting literature research. The resolution, consequently impacted the problem as a comprehensive but partial solution. It was a deliberate ploy to make the trust based framework and proof of concept feasible. The phase was documented in the literature review and scoped in the methodology section so that the defined solution acted as a target or a goal to achieve in the research. The resultant artefact is the Cloud Identity Trust Unified Evaluation Framework (figure 5) that describes a trust management (TM) system that aggregates and manages trust-related information from different sources (user ratings, provider statements, measurements, property certificates); which are relevant (and often available) when assessing the trustworthiness of a cloud provider. The structure is based on existing work and presented in a systematic way that helps the cloud identity consumers (and end users) to find the particular trust model that fulfils their requirements. Furthermore, it gives a benchmark on the basis of which one can analyse and assess the different cloud identity models to investigate their strengths and weaknesses. The main objective is to provide novel concepts and mechanisms for trust establishment in cloud identity environment. The trust model incorporates various security challenges and can be used to evaluate the security strength of the cloud identity services. It is a taxonomy where all the entities can be incorporated within a cloud computing service provider and cloud identity environment. It is divided into the steps modelling the trust, trust aggregation, formulation, and trust calculation.

One input into the design artefact is the modelling of trust. The first task is to specify the Prospect description and Prospect value. A trust formation rule defines what may form evidence and how this evidence should influence the target's trust level with respect to a vendor. The evidence to make a trust level consists of a prospect, a prospect property and an evidence type. The prospect is received from a vendor and can be anything that may give insight into this vendor's capability, such as intention or capabilities to take care of the target's assets. A second input is the formulation of a trusted system. This is the abstract mathematical specification of how the available information should be transformed into a usable metric. The specification may be made through an explicit equation, or implicitly through describing an algorithm that will result in the correct values.

The formulation determines the theoretical properties of the system and thus the upper bound on its resilience to attacks. As a result, the formulation is a critical component since any weakness in the design. The third and fourth inputs are trust aggregation and calculation. Trust aggregation algorithms calculate the reputation scores of objects based on the collected evidence. A good trust aggregation scheme should be able to compute trust scores that accurately describe the quality of objects. The calculation receives input information and produces the reputation metric values. While the formulation is an idealized method for determining a trust and reputation value, the calculation dimension characterizes how the formulation is implemented within the constraints of a particular reputation system. The dimension strives to be accurate to the reputation metric formulation while remaining

practical to implement and resilient to malicious attack. Two components relevant to the reputation calculation are the calculation structure and calculation approach.

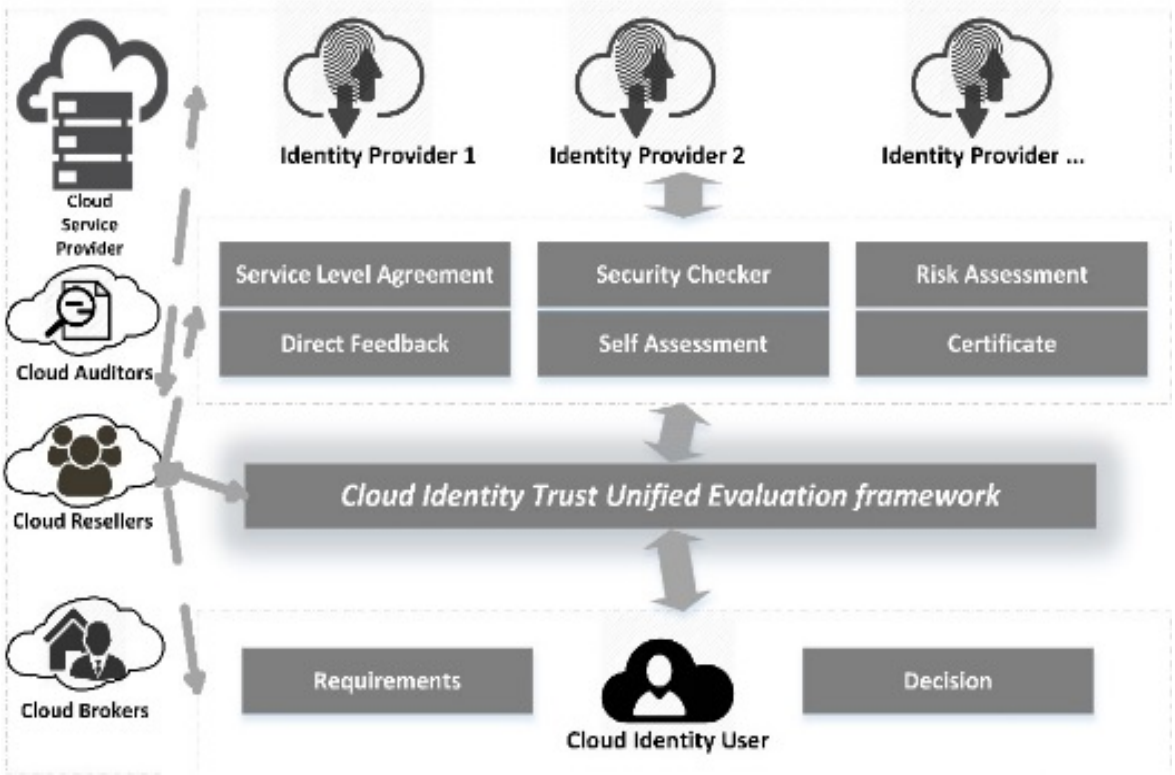

Figure 5. Cloud Identity Trust Unified Evaluation Framework

In complex distributed environments such as cloud, it is important to evaluate the trustworthiness of a cloud provider, by considering the knowledge on the architecture of the systems and the trustworthiness of its components and subsystems. Evaluation is the third phase of the TDS research methodology; this involves observing and evaluating how effective and how efficient that the framework solves the trust issues and problems. In this phase, the evaluation and observation results are compared with the objectives of a solution. It is possible to iterate back to design an artefact or even identify the problem if necessary, and bring quality improvement. At this point the system has both the trust and its requirements. In evaluation it looks for possible gaps, exceptions and errors. Once the solution reaches a sufficient state, its evaluation can be started. Every trust formation rule forms trust based on a prospect with a specific value. It can therefore be easily checked against the corresponding trust formation rule requirement which specifies the highest acceptable trust to be formed for a prospect of this value. The evaluation is to be achieved by the means of a case study or action research, by arranging a broad expert survey and by laboratory experiments or simulations.

Refine Hypothesis

Usually, the general research hypothesis are difficult to evaluate as a whole. Therefore, the hypothesis are refined by smaller and object oriented hypotheses with a more constricted but precise scope. The refined hypotheses should be mutually exclusive and collectively exhaustive with regard to the general hypothesis. It means if all refined hypotheses are supported, the general hypothesis should be supported as well. The general hypothesis make a trustworthiness framework to evaluate a cloud identity provider if they provide cloud identity by using single sign on services. For the evaluation, the general hypothesis is split into smaller hypotheses that were simpler to evaluate. The following hypotheses were developed:

- ✓ Our trust framework is better than other methods for trust and reputation and provides better support for business rules derivation than other reviewed methods.
- ✓ Our trust framework is usable in cloud identity environments and it can be used in practice.
- ✓ Our trust framework is useful for cloud customers and enhances a trust make decision understanding.

To support the first hypothesis, a survey is conducted. For each method used, a questionnaire form is filled out. To support the second hypothesis, action research is carried out in cloud identity companies. The aim is to ensure applicability in practice as well as to improve the method's quality by including solutions to problems encountered in the trust and reputation. A project member of the company's team will be instructed in the usage of the method and tool. The team member takes the double role of practitioner and researcher, documenting the usage of the method as well as the results. The results are evaluated according to the predetermined quality criteria. As action research works on a limited sample size, an additional expert survey is performed on the general hypothesis to show that there is general interest in the solution. This can be done by presenting the problem and its solution to practitioners during research. Afterwards a survey is performed to evaluate the perceived viability. The survey might contain the question: "Do you think the presented artefact provides a viable solution to the problem?" Additionally, the survey might include a question about the relevance of the problem, even though relevance has already been tested during problem identification. An expert survey could be used to evaluate the third hypothesis.

Communication

The final phase of TDS research methodology is known as Communication. This phase is designed to allow the researcher to employ various scholarly and industry outlets to communicate the outcome of the study. It is to communicate the trust problem and its importance, the trust framework artefact, its utility and novelty, the rigor of its design, and its effectiveness. Also to release extra information to help users understand the meaning of the scores. For example, Amazon shows all the feedback given by each reviewer. YouTube starts to provide visualization of viewing the history for video clips, accompanied by some statistical features. Once trust has been calculated, it needs to be readily accessible to interested parties while remaining resilient to alteration. Calculated values must be efficiently disseminated to other recipients or made available upon request. These responsibilities of a reputation system fall within the dissemination dimension. Although calculation and dissemination are often intertwined in the implementation. Dissemination structure, dissemination approach, storage strategies, and dissemination redundancy are four aspects of the dissemination dimension.

Conclusion

In this paper, an approach to design research in the area of information systems was presented based on the literature. Cloud computing provides cost-efficient opportunities for enterprises by offering a variety of dynamic, scalable, and shared services. Identity and advanced identity management are the ways to overcome many of the issues cloud users face when attempting to use cloud services. The application of theory in this paper has been to address the problem faced by cloud users as they attempt to assess the trust that may be had in any CIdP. The methodology developed integrated four requirements for building an improved security artefact: Trust and the capability to calculate a trust value for an entity; calculate a reputation measurement for an organisation; collect the evidence required by the second process group; and, building and evaluating a security artefact. In figure 4 the DS framework is applied to integrate the research processes into a methodology of multiple entry points and potential quality improvement cycles. To support the cloud customers in reliably identifying trustworthy cloud providers, we proposed a trust framework in cloud identity areas for a cloud computing decision making. This system provides a means to identify the trustworthy cloud providers in terms of different attributes assessed by multiple sources and on trust information.

References

Ali, M., Khan, S. U., and Vasilakos, A. V. 2015. "Security in cloud computing: Opportunities and challenges," *Information Sciences* (305), pp. 357-383.

Basin, D., Cremers, C., and Meadows, C. 2011. "Model checking security protocols," *Handbook of Model Checking*).

Chou, D. C. 2015. "Cloud computing risk and audit issues," *Computer Standards & Interfaces* (42), pp. 137-142.

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

Dólera Tormo, G., Gómez Mármol, F., and Martínez Pérez, G. Year. "On the application of trust and reputation management and user-centric techniques for identity management systems," XII Spanish meeting on cryptology and information security (RECSI 2012), San Sebastián, Spain2012.

Fournaris, A. P., and Keramidas, G. 2014. "From Hardware Security Tokens to Trusted Computing and Trusted Systems," in *System-Level Design Methodologies for Telecommunication*, Springer, pp. 99-117.

Goutas, L., Sutanto, J. and Aldarbesti, H. 2016. "The building blocks of a cloud strategy: Evidence from three SaaS providers," Communications of the ACM (59:1), pp. 90-97.

Gregor, S., and Hevner, A. R. 2013. "Positioning and presenting design science research for maximum impact," *MIS quarterly* (37:2), pp. 337-356.

Habib, S. M., Hauke, S., Ries, S., and Mühlhäuser, M. 2012. "Trust as a facilitator in cloud computing: a survey," *Journal of Cloud Computing* (1:1), pp. 1-18.

Habiba, U., Masood, R., Shibli, M. A., and Niazi, M. A. 2014. "Cloud identity management security issues & solutions: a taxonomy," *Complex Adaptive Systems Modeling* (2:1), pp. 1-37.

Hashizume, K., Rosado, D., Fernández-Medina, E., and Fernandez, E. B. 2013. "An analysis of security issues for cloud computing," *Journal of Internet Services and Applications* (4:1), pp. 1-13.

Håvaldsrud, T., Møller-Pedersen, B., Solhaug, B., and Stølen, K. 2012. "DeSPoT: A Method for the Development and Specification of Policies for Trust Negotiation," in *Computer Science and Convergence*, Springer, pp. 93-104.

Hoffman, K., Zage, D., and Nita-Rotaru, C. 2009. "A survey of attack and defense techniques for reputation systems," *ACM Computing Surveys (CSUR)* (42:1), p 1.

Johannesson, P., and Perjons, E. 2014. *An introduction to design science*, Springer.

Johannesson, P., and Perjons, E. 2014. "A Method Framework for Design Science Research," in *An Introduction to Design Science*, Springer, pp. 75-89.

Mármol, F. G., Girao, J., and Pérez, G. M. 2010. "TRIMS, a privacy-aware trust and reputation model for identity management systems," *Computer Networks* (54:16), pp. 2899-2912.

Marmol, F. G., and Pérez, G. M. 2009. "Security threats scenarios in trust and reputation models for distributed systems," *computers & security* (28:7), pp. 545-556.

Moody, D. L. 2003. "The method evaluation model: a theoretical model for validating information systems design methods," *ECIS 2003 proceedings*, pp. 79-96.

NIST 2013. "Final Version of NIST Cloud Computing Definition Published," E. Brown (ed.).

Noor, T. H., and Sheng, Q. Z. 2011. "Trust as a service: a framework for trust management in cloud environments," in *Web Information System Engineering–WISE 2011*, Springer, pp. 314-321.

Offermann, P., Levina, O., Schönherr, M., and Bub, U. 2009. "Outline of a design science research process," Proceedings of the 4th International Conference on Design Science Research in Information Systems and Technology, ACM.

Pearson, S. 2013. "Privacy, security and trust in cloud computing," in *Privacy and Security for Cloud Computing*, Springer, pp. 3-42.

Sakimura, N., Bradley, J., Jones, M., de Medeiros, B., and Mortimore, C. 2014. "Openid connect core 1.0," *The OpenID Foundation*, p S3.

Saleh, A. S., Hamed, E. M. R., and Hashem, M. 2014. "Building trust management model for cloud computing," Informatics and Systems (INFOS), 9th International Conference on, IEEE, pp. 116-125.

Shaikh, R., and Sasikumar, M. 2013. "Identity Management in Cloud Computing," *International Journal of Computer Applications* (63:11), pp. 17-19.

Shaikh, R., and Sasikumar, M. 2015. "Trust Model for Measuring Security Strength of Cloud Computing Service," *Procedia Computer Science* (45), pp. 380-389.

Sun, Y. L., and Liu, Y. 2012. "Security of Online Reputation Systems: The evolution of attacks and defenses," *IEEE Signal Process. Mag.* (29:2), pp. 87-97.

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

Wang, Y., and Lin, K.-J. 2008. "Reputation-oriented trustworthy computing in e-commerce environments," *Internet Computing, IEEE* (12:4), pp. 55-59.