Managing Trust in the Cloud: State of the Art and Research Challenges

Talal H. Noor, Taibah University
Quan Z. Sheng, University of Adelaide
Zakaria Maamar, Zayed University
Sherali Zeadally, University of Kentucky

Cloud computing is a highly promising technology, but deficient trust management is hindering market growth. A proposed framework for analyzing trust management systems can help researchers develop innovative solutions to challenges such as identification, privacy, personalization, integration, security, and scalability.

Over the past few years, cloud computing has emerged as a new paradigm for providing flexible and on-demand infrastructure as a service (IaaS), platform as a service (PaaS), and software as a service (SaaS). Cloud computing combines the best of grid computing[1] and service-oriented computing.[2] In grid computing, multiple organizations pool their hardware resources to achieve specific goals, such as high performance and reduced costs; in service-oriented computing, software resources are provided as services. In cloud computing, however, both hardware and software resources are configured as services using virtualization techniques—for example, the creation of virtual instances of the hardware platform, OS, and network storage—to automate business process execution over distributed systems.

Cloud computing promises several benefits such as expense reduction, resource elasticity, and simplicity.[1,3] On the other hand, cloud services' highly dynamic, distributed, and nontransparent nature makes establishing and managing trust among cloud service providers and consumers a significant challenge. In fact, a recent study showed that inadequate trust management is among the top obstacles to cloud computing adoption.[4]

Numerous researchers have explored trust management in Web services. For instance, Audun Jøsang, Roslan Ismail, and Colin Boyd discussed general ideas of trust, such as trust classes and trust purpose, and

0018-9162/16/$33.00 © 2016 IEEE

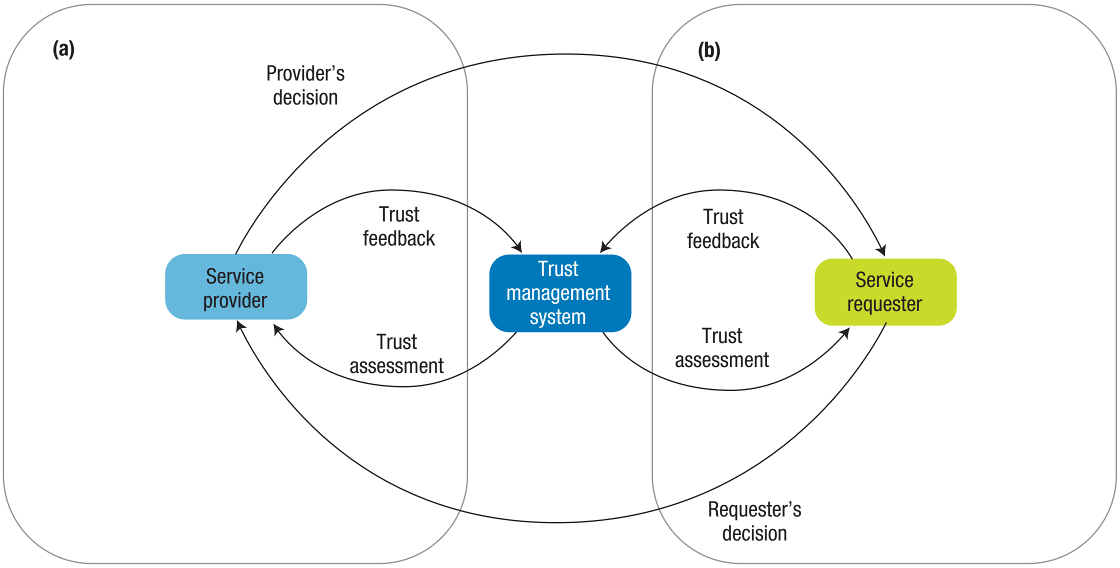

FIGURE 1. Trust management from the perspectives of the (a) service provider and (b) service requester.

explained the overlap between trust and reputation.[5] Yao Wang and Julita Vassileva systematically reviewed multiple trust and reputation systems, classifying them into centralized versus decentralized, persons/agents versus resources, and global versus personalized.[6] Kevin Hoffman, David Zage, and Cristina Nita-Rotaru surveyed techniques to attack and defend reputation systems, particularly in peer-to-peer (P2P) environments; they considered which components were most vulnerable and suggested appropriate defenses to integrate into existing or future systems.[7] However, most studies preceded the recent surge in cloud computing and thus do not reflect the state of the art; moreover, they do not cover many issues such as distrusted feedback, poor identification of trust feedback, trust participant privacy, and lack of trust feedback integration.

Here, we look at the problem of managing trust in the cloud holistically. We describe different trust management perspectives and techniques, identify the trust characteristics of four major cloud service providers, and propose a generic analytical framework with a set of 14 criteria to assess trust management systems in cloud computing. We also discuss open research challenges revealed by an analysis of 30 available systems.

TRUST MANAGEMENT PERSPECTIVES AND TECHNIQUES

The concept of trust management was introduced a decade ago by Matt Blaze, Joan Feigenbaum, and Jack Lacy in describing a prototype system designed to address the deficiencies of decentralized security mechanisms.[8] These deficiencies include centralized control of trust relationships (global certifying authorities), the inflexibility to support complex trust relationships in large-scale networks, and heterogeneous policy languages. A trust management service can be independent of cloud services, but the trust techniques and assessment functions must be compatible with the underlying IaaS, PaaS, or SaaS cloud service model. We argue that it is vital to consider the possible trust management perspectives and techniques to identify the types of cloud services that these techniques support and to develop the most suitable trust management system per cloud service type.

As Figure 1 shows, trust management can be viewed from the perspective of either the service provider, who wants to assess service requesters' trustworthiness, or the service requester, who wants to assess service providers' trustworthiness.

Trust management can be based on policies, recommendations, reputation, or prediction. The best way to illustrate these techniques is to represent trusted parties as abstract entities (they can be service providers or consumers), as shown in Figure 2.

Policies

A popular way to establish trust among independent entities is to control end-user authorization through a policy. End users are granted access subject to meeting the policy's trust threshold, which typically follows a *trust result* or *credential* approach. The former monitors service-level agreement (SLA) violations of cloud services or measures a service's credibility based on parameters such as security, latency, and availability; the latter is based on standards such as X.509v3,[9] simple public-key infrastructure (SPKI),[10] or the Security Assertion Markup Language (SAML).[11]

As Figure 2a shows, an inquiring entity (for example, a consumer) and an unknown entity (for example, a cloud service provider) adopt specific policies to disclose their respective credentials for the purpose of access

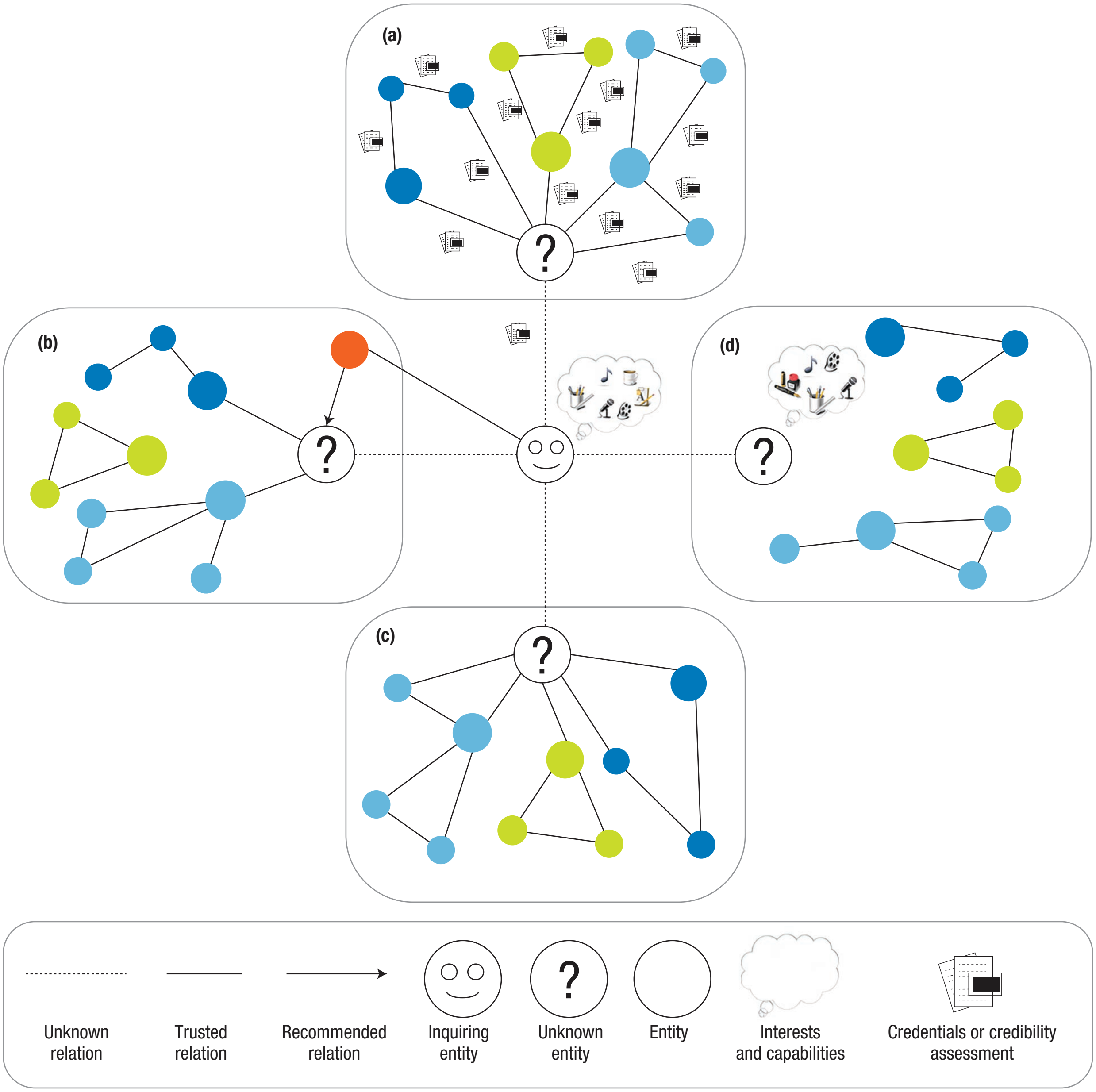

FIGURE 2. Trust can be managed through (a) policies, (b) recommendations, (c) reputation, or (d) prediction.

control. If the inquiring entity satisfies the unknown entity's minimum trust threshold, the inquiring entity is granted access.

Recommendations

Recommendations leverage entities' prior knowledge of trusted parties, especially when the entity knows the trust feedback's source, in trust management systems. It is well known from social psychology theory that a person's trust assessment of an unknown entity can be influenced by other known entities who recommend it.[12]

Figure 2b depicts a scenario in which the inquiring entity (say, Alice) trusts another entity (Bob). Bob recommends an unknown entity (for example, a cloud-based file-hosting service) to Alice, who adopts his recommendation because she trusts Bob.

Reputation

Reputation strongly influences trust management systems.[13] Various entities' opinions can dramatically impact, either positively or negatively, an unknown entity's reputation. Unlike the case with recommendations, an inquiring entity does not know the source of the trust feedback—that is, there are no trusted relations.

As Figure 2c shows, an unknown entity (for example, a social network) has a set of trusted relations with other parties (for example, network members) who provide trust feedback to the unknown entity. The more positive this feedback is, the more likely an inquiring entity (for example, a potential new member) will trust the unknown entity.

Prediction

Prediction benefits trust management systems when inquiring entities have no prior information about an unknown entity's interactions.[14] Research shows that entities with like-minded capabilities and interests are more likely to trust one another.[15]

As Figure 2d shows, the more similar an inquiring entity (for example, an enterprise consumer) is to other entities using an unknown entity (for example, an IaaS), the more likely the inquiring entity will trust the unknown entity.

TRUST CHARACTERISTICS OF CLOUD SERVICES

Identifying trustworthy cloud services is difficult because of their diversity and the similar functionalities they provide. Therefore, we define the following five trust characteristics that consumers should pay attention to when comparing IaaS, PaaS, and SaaS cloud services from various representative providers.

- *Authentication*. The techniques used to establish consumers' identities when registering for a service give some indication of how trustworthy the service is. Consumer credentials contain sensitive private information that can be compromised if the service does not apply a proper identity scheme.
- *Security*. The security mechanisms employed by a cloud service also hint at its trustworthiness. These mechanisms can be at the communication level (for example, Secure Sockets Layer technology), data level (for example, replication techniques for data recovery), and physical (hardware) level.
- *Privacy*. Knowing a cloud service's privacy policy can help determine whether to trust that service with essential data. Based on SLAs, privacy responsibility can be split between the provider, who deploys all necessary security measures, and consumers, who take their own steps to preserve data privacy.
- *Virtualization*. The type of virtualization deployed by a cloud service impacts the resources consumers have control over (for example, storage), which can be an indicator of trustworthiness. Virtualization can occur at either the OS or application container level. Providers use virtualization techniques to control the underlying cloud environment, whereas consumers control storage, processes, and some network communication components through virtual machines.
- *Accessibility*. The type of accessibility a cloud service offers can help determine whether the service can be reliably trusted. Consumers access cloud services through several means including GUIs, APIs, and command-line tools.

[IDENTIFYING TRUSTWORTHY CLOUD SERVICES IS DIFFICULT BECAUSE OF THEIR DIVERSITY AND THE SIMILAR FUNCTIONALITIES THEY PROVIDE.]

We used these characteristics to benchmark four representative cloud service providers: IBM, Microsoft, Google, and Amazon. The results are listed in Table 1. Some providers deploy several technologies for the same trust characteristic, and the choice is open for consumers regardless of whether the consumer is a business that hosts its services on the cloud or an individual who uses the cloud for personal storage. However, many of these technologies are not suitable for all consumers. Therefore, flexible techniques are required to customize provisioned technologies based on consumers' specific needs. In addition, given the large number of technologies available, consumers face many configuration options while using cloud services including the number and type of virtual machines, time of tenancy, and access control policy. Thus, there is a need for intelligent techniques that make cloud platforms "learn" consumers' normal usage patterns to simplify the configuration process.

TRUST MANAGEMENT ANALYTICAL FRAMEWORK

Knowing the cloud services that trust management techniques support is

TABLE 1. Trust characteristics of representative cloud service providers.

	Cloud service provider								
Category	**IBM**			**Microsoft**			**Google**		**Amazon**
Supported service models	IaaS	PaaS	SaaS	IaaS	PaaS	SaaS	PaaS	SaaS	IaaS
Service types	Computation, storage	Web apps	Web apps	Storage	Web apps	Web apps	Web apps	Web apps	Computation, storage
Service names	Ensembles	Blue Cloud, WebSphere CloudBurst Appliance (WCA), Research Compute Cloud (RC2)	LotusLive	Live Mesh	Azure	.NET service, dynamic customer relationship management (CRM)	App Engine	Gmail, Docs	Elastic Compute Cloud (EC2), Simple Storage Service (S3), Simple Queue Service (SQS), SimpleDB
Authentication	Public-key infrastructure (PKI) and access management services			Rule-based access control and password-based protection			Secure Shell (SSH) and rule-based access control		Password-based protection or SSH*
Communication security level	Secure Sockets Layer (SSL) or virtual private network (VPN)* for data transfers			SSL for data transfers			SSL for data transfers		SSL for data transfers
Data security level	Data de-duplication practices			Replicated data for data recovery			Grid-based data redundancy		Elastic Block Store (EBS) for data recovery
Physical security level	Hardware security in datacenters			Hardware security in datacenters			Local and central monitoring techniques for hardware security		Hardware security in datacenters
Privacy	Consumer's responsibility			Provider's responsibility			Provider's responsibility		Consumer's responsibility
Virtualization	OS level, running on IBM PowerVM			OS level			Application container level		OS level, running on Xen hypervisor
Accessibility	Browser-based accessible GUI using Dojo Toolkit			Web-based Live Desktop			Web-based administration		EC2 command-line tools or API*

*The consumer has the choice of provisioned technologies.

vital to developing the most suitable trust management solution for each type of service. Toward this end, we propose a generic analytical framework to evaluate existing trust management systems. As Figure 3 shows, the framework consists of three layers—namely, trust feedback sharing, trust assessment, and trust results distribution—that each contain a set of assessment criteria.

Trust feedback sharing

The trust management system collects trust feedback from various consumers and providers and stores these results for later assessment. Storage can be centralized, decentralized, or maintained in the cloud by a trusted provider.

Credibility. Credibility can apply to both the trust management system itself and the feedback obtained. Without a proper scheme to identify credible feedback, trust results accuracy will be low—for example, the system can be subverted by Sybil attacks.[13]

Privacy. A trust management system can inadvertently leak consumers' personal details (username, password, address, and so on) as well as behavioral information—for example, who a consumer interacted with or a cloud service in which a consumer expressed interest. Traditional anonymization techniques used to protect such data are inadequate in a cloud environment due to its highly dynamic and distributed nature. On the other hand, cryptographic and encryption techniques can decrease data utilization—for example, plaintext search.[8]

Personalization. Some trust management systems allow consumers and providers to select both the trust feedback process (automated or manually driven) and the trust management technique used by the system. Personalization is applicable if the system supports fully autonomous collaboration. Well-defined interfaces let trust participants control their feedback as well as change the feedback process without affecting one another.

Integration. The ability to combine different trust management perspectives (provider and consumer) and techniques (for example, policies and reputation) can enhance trust management system performance. Integrating several trust management techniques generally increases trust results accuracy but is challenging.

Trust assessment

Trust assessment can involve several metrics such as transaction size, feedback credibility, and so on. The trust management system responds to trust assessment queries from interested consumers and providers by applying different trust management techniques to the feedback it has collected and then distributing the results.

Perspective. Trust management systems can support the service provider's perspective, the service requester's perspective, or both. Systems that support both perspectives are more comprehensive than those that support only one.

Technique. Trust management systems can employ one technique (for example, policies only) or multiple techniques (for example, policies and reputation). A system that uses several techniques will achieve more accurate trust results.

Adaptability. Trust assessment can follow customized criteria (for example, weighing the trust feedback based on the transaction cost) or a general metric to determine an entity's trustworthiness. The ability to update trust feedback and assessment results in response to changing criteria indicates the trust management system's adaptability.

Security. Trust management systems are subject to attacks at two security levels. At the assessment function level, potential attacks include providing misleading feedback to increase the trust results (self-promotion) and to decrease the trust results (slandering). At the communication level, man-in-the-middle and denial-of-service attacks are among the most common. Systems that provide strong defenses against such attacks are more secure.

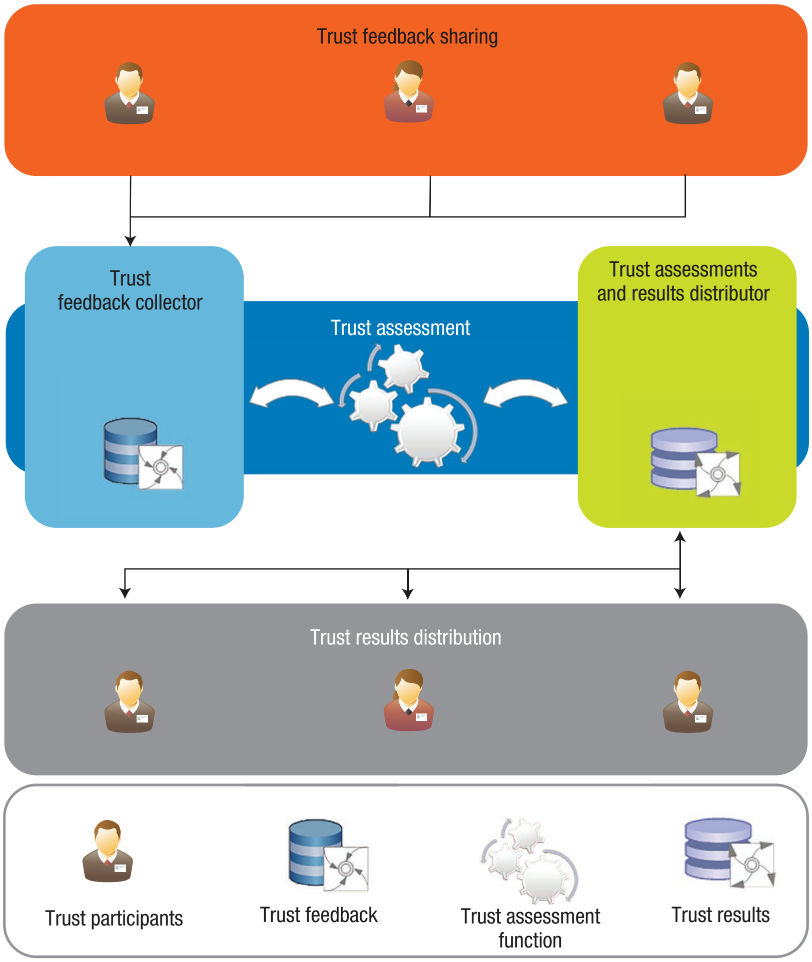

FIGURE 3. Three-layered architecture of our proposed trust management analytical framework.

TABLE 2. Trust management system evaluation.

	Trust feedback sharing				Trust assessment						Trust results distribution			
System authors	Credibility	Privacy	Personalization	Integration	Perspective	Technique	Adaptability	Security	Scalability	Applicability	Response time	Redundancy	Accuracy	Security
Ko et al.[16]	EC	SR	N	NFC	SRP	PocT[a]	N	AFL/CL	C	IaaS	NAT	N	F	ACL/CL
Habib et al.[17]	EC	N	P	SFC	SRP	RecT/RepT/PrdT	P	AFL/CL	C	All	NAT	N	F	ACL/CL
Noor et al.[18]	FC/EC	SR	P	NFC	SRP	RepT/PrdT	F	AFL/CL	D	All	NAT	TR	F	ACL/CL
Krautheim et al.[19]	EC	SR	N	SFC	SRP/SPP	RecT/RepT	N	CL	C	IaaS	NAT	N	P	ACL/CL
Brandic et al.[20]	EC	SR	P	NFC	SRP	PocT[a]	P	CL	C	IaaS/PaaS	NAT	N	P	ACL/CL
Yao et al.[21]	EC	N	N	NFC	SRP	PocT[a]	P	CL	C	IaaS	SAT	N	P	ACL/CL
Hwang and Li[22]	EC	SR	N	NFC	SRP	PocT[b]	N	AFL/CL	C	All	SAT	N	F	ACL/CL
Santos et al.[23]	EC	SR	N	NFC	SRP	PocT	N	CL	D	IaaS	NAT	TDR	P	ACL/CL
Manuel et al.[24]	FC/EC	SR	N	SFC	SRP	PocT/RepT	N	AFL/CL	C	All	SAT	N	F	ACL/CL
Alhamad et al.[25]	EC	SR	P	NFC	SRP	PocT[a]/RepT	N	N	D	IaaS	SAT	N	P	N
Azzedin and Aheswaran[26]	FC/EC	N	N	SFC	SRP	RepT	N	AFL	D	IaaS	SAT	AR/TDR	P	ACL
Lin et al.[27]	FC/EC	N	N	SFC	SRP/SPP	PocT/RepT	N	AFL/CL	D	IaaS	SAT	AR/TDR	F	ACL/CL
Yu and Ng[28]	N	SR/SP	N	NFC	SRP/SPP	PocT	N	AFL	D	IaaS	NAT	AR/TDR	P	ACL
Domingues et al.[29]	EC[c]	N	N	NFC	SPP	RecT	N	N	C	All	NAT	N	N	ACL
Song et al.[30]	EC	N	N	NFC	SRP	PocT[b]	F	AFL/CL	C	IaaS	SAT	N	F	ACL/CL
Song et al.[31]	EC	N	N	NFC	SRP/SPP	PocT[b]	F	AFL/CL	C	All	SAT	N	F	ACL/CL
Weishaupl et al. [32]	N	SR	N	NFC	SRP/SPP	PocT	N	CL	C	IaaS	NAT	N	P	ACL/CL
Chen et al.[33]	N	SR	P	NFC	SRP	PocT	N	AFL/CL	D	All	SAT	AR/TDR	F	ACL/CL
Srivatsa and Liu[34]	FC/EC	N	N	NFC	SRP/SPP	RepT	F	AFL	D	All	SAT	TDR	F	ACL
Aringhieri et al.[35]	FC/EC	SR	N	NFC	SRP/SPP	RepT	P	AFL/CL	D	All	SAT	TDR	F	ACL/CL
Zhou and Hwang[36]	FC/EC	N	N	NFC	SRP/SPP	RepT	P	AFL/CL	D	All	SAT	TDR	F	ACL/CL

TABLE 2 CONTINUED. Trust management system evaluation.

	Trust feedback sharing				Trust assessment						Trust results distribution			
System authors	Credibility	Privacy	Personalization	Integration	Perspective	Technique	Adaptability	Security	Scalability	Applicability	Response time	Redundancy	Accuracy	Security
Kamvar et al.[37]	FC/EC	N	N	NFC	SRP/ SPP	RepT	P	AFL	D	All	NAT	TDR	N	ACL
Xiong and Liu[38]	FC/EC	N	N	NFC	SRP	RepT	F	AFL	D	All	NAT	AR/ TDR	P	ACL
Skopik et al.[14]	N	N	N	SFC	SRP	RecT/ PrdT	N	N	C	All	NAT	N	F	N
Skopik et al.[39]	N	N	N	SFC	SRP	PocT/ PrdT	N	CL	C	IaaS	SAT	TDR	P	ACL/CL
Koshutanski and Massacci[40]	N	SR	N	NFC	SPP	PocT	N	AFL	C	IaaS	NAT	N	F	ACL
Park et al.[41]	FC/EC	N	N	SFC	SRP	RecT/ RepT	N	AFL/CL	D	All	SAT	TDR	F	ACL/CL
Skogsrud et al.[42]	N	SR	P	NFC	SPP	PocT	F	AFL/CL	D	IaaS	SAT	TDR	F	ACL/CL
Connor et al.[43]	N	N	P	NFC	SPP	RepT	P	AFL	D	All	SAT	AR/ TDR	N	ACL
Malik and Bouguet-taya[44]	FC/EC	SR	P	NFC	SRP	PocT/ RepT	F	AFL	D	All	SAT	TDR	F	ACL/CL

[a] A service-level agreement is used to perform policy-based trust management.

[b] The technique is described as being reputation-based but is actually based on predefined policies that measure entities' credibility.

[c] Entities' credibility is identified through referral relationships.

TABLE 2 LEGEND.

Trust feedback sharing

Credibility		Privacy		Personalization		Integration	
FC	Feedback credibility	SP	Focus on service provider's privacy	F	Full	SFC	Strong use of feedback combination
EC	Entity's credibility	SR	Focus on service requester's privacy	P	Partial	NFC	No strong use of feedback combination
N	None	N	None	N	None		

Trust assessment

Perspective		Technique		Adaptability		Security		Scalability	
SPP	Service provider per spective	PocT	Policies	F	Full	AFL	Supports assessment function level	C	Centralized
SRP	Service requester perspective	RecT	Recommendations	P	Partial	CL	Supports communication level	D	Decentralized
		RepT	Reputation	N	None	N	None		
		PrdT	Prediction						

Trust results distribution

Response time		Redundancy		Accuracy		Security	
SAT	Strong emphasis on assessment time	AR	Supports assessment redundancy	F	Full	ACL	Supports access-control level
NAT	No strong emphasis on assessment time	TDR	Supports trust data redundancy	P	Partial	CL	Supports communication level
		N	None	N	None		

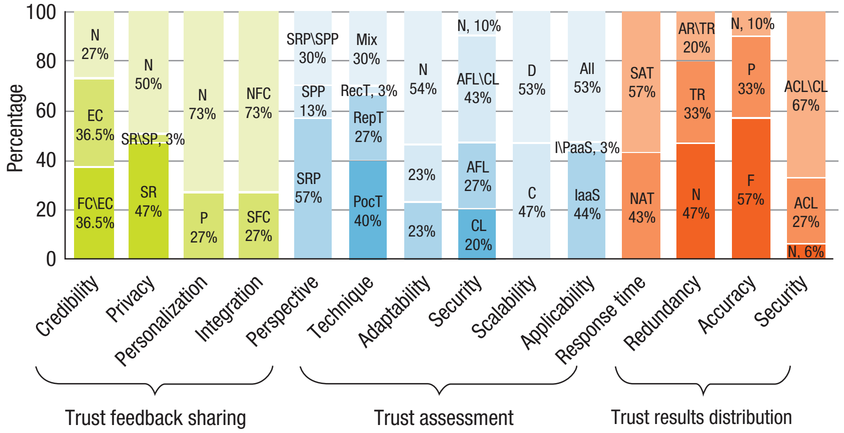

FIGURE 4. Statistical analysis of trust management systems (see Table 2 for an explanation of the abbreviations).

Scalability. The trust management system's ability to grow with demand depends on whether trust assessment inquiries and results are stored in one place or across several distributed resources. Centralized systems are more prone to problems including scalability, availability, and security than decentralized systems.

Applicability. Trust management systems can support a particular cloud service model (IaaS, PaaS, or SaaS) or a combination of models. It is important to differentiate the suitability of trust assessment functions for each service. The more types of cloud services a trust management system can support, the more comprehensive it is.

Trust results distribution

Consumers and providers submit trust assessment inquiries about other parties (for example, a cloud service) to the trust management system. The system stores the assessment results in a database where the inquiring parties can retrieve them.

Response time. An important aspect of trust management is the time required to handle trust assessment inquiries, access feedback, and distribute results, especially when there is a large number of trust relationships. If the trust management system's response time is long, the number of inquiries it can handle will be low.

Redundancy. Trust management systems can unnecessarily duplicate assessment processes; they also replicate trust feedback and results to enable broader access to their data. Failure to address assessment and trust data redundancy can lead to inefficient resource usage and weaken both system performance and security.

Accuracy. The accuracy of trust assessment results depends on both the correct identification of trust feedback and effective assessment function security. Poor identification of trust feedback and/or failure to prevent attackers from manipulating trust results can lead to inaccurate results in trust management systems.

Security. Trust results distribution requires appropriate security mechanisms at both the access control and communication levels.

EVALUATION OF TRUST MANAGEMENT SYSTEMS

We used our proposed framework to evaluate 30 representative trust management systems for cloud computing and related areas such as grid, P2P, and service-oriented computing. Table 2 summarizes the results, and Figure 4 provides a statistical breakdown. Our analysis yielded several open research challenges.

Identification. Of the systems we evaluated, 63.5 percent do not use any mechanism to identify credible trust feedback. This is a significant challenge in the cloud because of the overlapping interactions between service providers and consumers.

Privacy. Consumers of cloud services face several privacy threats such as leaking their personal information and tracking their behavior—for example, which services they used. Half of the trust management systems we analyzed do not have a mechanism to preserve participants' privacy, highlighting the urgent need for efficient techniques that protect users' privacy while minimizing the impact to system performance.

Personalization. Fifty-four percent of the trust management systems we evaluated do not support personalization. Flexible techniques must be developed to ensure that consumers can control their trust feedback, create their own assessment criteria, control their trust results, and change their feedback processes according to need.

Integration. Combining several techniques like reputation and recommendations can increase trust results' accuracy; it can also lead to better trust results by matching appropriate consumers to trustworthy providers. Unfortunately, 73 percent of the trust management systems we examined do not support the integration of trust feedback. Techniques that can efficiently integrate various trust feedback are needed to improve trust results.

Security. Thirty-three percent of the trust management systems we evaluated do not provide security at the assessment function level. However, attacks might come from system users themselves. The situation becomes even worse in cloud environments due to dynamic interactions and the distributed nature of cloud services, which make it difficult to identify attackers. Proper techniques to mitigate such attacks are needed.

Scalability. Forty-four percent of the trust management systems we evaluated have a decentralized architecture. In a cloud environment, where the number of consumers could be very large and highly dynamic, the system must be adaptive and scalable to efficiently collect all trust feedback and constantly update trust results.

Cloud computing is a highly promising technology, but deficient trust management is hindering market growth. Despite many efforts to address this problem, several issues such as identification, privacy, personalization, integration, security, and scalability continue to be major impediments to cloud adoption. Our proposed framework for analyzing trust management systems can help researchers develop innovative solutions to these challenges.

REFERENCES

1. I. Foster et al., "Cloud Computing and Grid Computing 360-Degree Compared," *Proc. Grid Computing Environments Workshop* (GCE 08), 2008; doi:10.1109/GCE.2008.4738445.
2. Y. Wei and M.B. Blake, "Service-Oriented Computing and Cloud Computing: Challenges and Opportunities," *IEEE Internet Computing*, vol. 14, no. 6, 2010, pp. 72–75.
3. B. Sotomayor et al., "Virtual Infrastructure Management in Private and Hybrid Clouds," *IEEE Internet Computing*, vol. 13, no. 5, 2009, pp. 14–22.
4. M. Armbrust et al., "A View of Cloud Computing," *Comm. ACM*, vol. 53, no. 4, 2010, pp. 50–58.
5. A. Jøsang, R. Ismail, and C. Boyd, "A Survey of Trust and Reputation Systems for Online Service Provision," *Decision Support Systems*, vol. 43, no. 2, 2007, pp. 618–644.
6. Y. Wang and J. Vassileva, "Toward Trust and Reputation Based Web Service Selection: A Survey," *Int'l Trans. Systems Science and Applications*, vol. 3, no. 2, 2007, pp. 118–132.
7. K. Hoffman, D. Zage, and C. Nita-Rotaru, "A Survey of Attack and Defense Techniques for Reputation Systems," *ACM Computing Surveys*, vol. 42, no. 1, 2009; doi:10.1145/1592451.1592452.
8. M. Blaze, J. Feigenbaum, and J. Lacy, "Decentralized Trust Management," *Proc. IEEE Symp. Security and Privacy* (SP 96), 1996, pp. 164–173.
9. D. Cooper et al., *Internet x.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*, IETF RFC 5280, May 2008; http://tools.ietf.org/pdf/rfc5280.pdf.
10. C. Ellison et al., *SPKI Certificate Theory*, IETF RFC 2693, Sept. 1999; http://tools.ietf.org/pdf/rfc2693.pdf.
11. S. Cantor et al., *Assertions and Protocols for the Oasis Security Assertion Markup Language (SAML) v2.0*, Oasis, 15 Mar. 2005; http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf.
12. G. Liu, Y. Wang, and M. Orgun, "Trust Inference in Complex Trust-Oriented Social Networks," *Proc. Int'l Conf. Computational Science and Eng.* (CSE 09), vol. 4, 2009, pp. 996–1001.
13. C. Dellarocas, "The Digitization of Word of Mouth: Promise and Challenges of Online Feedback Mechanisms," *Management Science*, vol. 49, no. 10, 2003, pp. 1407–1424.
14. F. Skopik, D. Schall, and S. Dustdar, "Start Trusting Strangers? Bootstrapping and Prediction of Trust," *Proc. 10th Int'l Conf. Web Information Systems Eng.* (WISE 09), 2009, pp. 275–289.
15. Y. Matsuo and H. Yamamoto, "Community Gravity: Measuring Bidirectional Effects by Trust and Rating on Online Social Networks," *Proc. 18th Int'l Conf. World Wide Web* (WWW 09), 2009, pp. 751–760.
16. R.K.L. Ko et al., "TrustCloud: A Framework for Accountability and Trust in Cloud Computing," *Proc. IEEE World Congress on Services* (SERVICES 11), 2011, pp. 584–588.
17. S.M. Habib, S. Ries, and M. Muhlhauser, "Towards a Trust Management System for Cloud Computing," *Proc. IEEE 10th Int'l Conf. Trust, Security, and Privacy in Computing and Comm.* (TrustCom 11), 2011, pp. 933–939.

ABOUT THE AUTHORS

TALAL H. NOOR is an assistant professor and head of the Department of Computer Information Systems in the College of Computer Science and Engineering at Taibah University in Yanbu, Saudi Arabia. His research interests include cloud computing, service-oriented computing, security and privacy, and trust management. Noor received a PhD in computer science from the University of Adelaide, Australia. He is a member of IEEE. Contact him at tnoor@taibahu.edu.sa.

QUAN Z. SHENG is a professor and deputy head of the School of Computer Science at the University of Adelaide. His research interests include the Web of Things, the Internet of Things, Internet computing, service-oriented computing, cloud computing, and big data analytics. Sheng received a PhD in computer science from the University of New South Wales, Australia. He is a member of IEEE and ACM. Contact him at qsheng@cs.adelaide.edu.au.

ZAKARIA MAAMAR is a professor and acting dean of the College of Information Technology at Zayed University in Dubai, United Arab Emirates. His research interests are primarily related to service-oriented computing and social computing. Maamar received a PhD in computer science from Laval University, Canada. He is a member of ACM. Contact him at zakaria.maamar@zu.ac.ae.

SHERALI ZEADALLY is an associate professor in the College of Communication and Information at the University of Kentucky. His research interests include computer networks, cybersecurity, mobile computing, ubiquitous computing, multimedia, and performance evaluation of systems and networks. Zeadally received a PhD in computer science from the University of Buckingham, UK. He is a Fellow of the British Computer Society and the Institute of Engineering Technology. Contact him at szeadally@uky.edu.

18. T.H. Noor, Q.Z. Sheng, and A. Alfazi, “Reputation Attacks Detection for Effective Trust Assessment of Cloud Services,” *Proc. IEEE 12th Int’l Conf. Trust, Security, and Privacy in Computing and Comm.* (TrustCom 12), 2013, pp. 469–476.
19. F.J. Krautheim, D.S. Phatak, and A.T. Sherman, “Introducing the Trusted Virtual Environment Module: A New Mechanism for Rooting Trust in Cloud Computing,” *Proc. 3rd Int’l Conf. Trust and Trustworthy Computing* (TRUST 10), 2010, pp. 211–227.
20. I. Brandic et al., “Compliant Cloud Computing (C3): Architecture and Language Support for User-Driven Compliance Management in Clouds,” *Proc. IEEE 3rd Int’l Conf. Cloud Computing* (CLOUD 10), 2010, pp. 244–251.
21. J. Yao et al., “Accountability as a Service for the Cloud,” *Proc. IEEE Int’l Conf. Services Computing* (SCC 10), 2010, pp. 81–88.
22. K. Hwang and D. Li, “Trusted Cloud Computing with Secure Resources and Data Coloring,” *IEEE Internet Computing*, vol. 14, no. 5, 2010, pp. 14–22.
23. N. Santos, K.P. Gummadi, and R. Rodrigues, “Towards Trusted Cloud Computing,” *Proc. Conf. Hot Topics in Cloud Computing* (HotCloud 09), 2009; www.usenix.org/legacy/event/hotcloud09/tech/full_papers/santos.pdf.
24. P.D. Manuel et al., “Trust Management System for Grid and Cloud Resources,” *Proc. 1st Int’l Conf. Advanced Computing* (ICAC 09), 2009, pp. 176–181.
25. M. Alhamad, T. Dillon, and E. Chang, “SLA-based Trust Model for Cloud Computing,” *Proc. 13th Int’l Conf. Network-Based Information Systems* (NBiS 10), 2010, pp. 321–324.
26. F. Azzedin and M. Aheswaran, “Integrating Trust into Grid Resource Management Systems,” *Proc. Int’l Conf. Parallel Processing* (ICPP 02), 2002, pp. 47–54.
27. C. Lin et al., “Enhancing Grid Security with Trust Management,” *Proc. IEEE Int’l Conf. Services Computing* (SCC 04), 2004, pp. 303–310.
28. C.-M. Yu and K.-W. Ng, “A Mechanism to Make Authorization Decisions in Open Distributed Environments without Complete Policy Information,” *Computational Science—ICCS 06*, LNCS 3994, 2006, pp. 1007–1014.
29. P. Domingues, B. Sousa, and L.M. Silva, “Sabotage-Tolerance and Trust Management in Desktop Grid Computing,” *Future Generation Computing Systems*, vol. 23, no. 7, 2007, pp. 904–912.
30. S. Song, K. Hwang, and Y.-K. Kwok, “Trusted Grid Computing with

Security Binding and Trust Integration," *J. Grid Computing*, vol. 3, no. 1, 2005, pp. 53–73.

31. S. Song et al., "Trusted P2P Transactions with Fuzzy Reputation Aggregation," *IEEE Internet Computing*, vol. 9, no. 6, 2005, pp. 24–34.
32. T. Weishaupl, C. Witzany, and E. Schikuta, "gSET: Trust Management and Secure Accounting for Business in the Grid," *Proc. IEEE 6th Int'l Symp. Cluster Computing and the Grid* (CCGrid 06), 2006, pp. 349–356.
33. K. Chen, K. Hwang, and G. Chen, "Heuristic Discovery of Role-Based Trust Chains in Peer-to-Peer Networks," *IEEE Trans. Parallel Distributed Systems*, vol. 20, no. 1, 2008, pp. 83–96.
34. M. Srivatsa and L. Liu, "Securing Decentralized Reputation Management Using Trust-Guard," *J. Parallel and Distributed Computing*, vol. 66, no. 9, 2006, pp. 1217–1232.
35. R. Aringhieri et al., "Fuzzy Techniques for Trust and Reputation Management in Anonymous Peer-to-Peer Systems," *J. Am. Soc. for Information Science and Technology*, vol. 57, no. 4, 2006, pp. 528–537.
36. R. Zhou and K. Hwang, "Trust Overlay Networks for Global Reputation Aggregation in P2P Grid Computing," *Proc. 20th Int'l Conf. Parallel and Distributed Processing* (IPDPS 06), 2006; doi:10.1109/IPDPS.2006.1639268.
37. S.D. Kamvar, M.T. Schlosser, and H. Garcia-Molina, "The EigenTrust Algorithm for Reputation Management in P2P Networks," *Proc. 12th Int'l Conf. World Wide Web* (WWW 03), 2003, pp. 640–651.
38. L. Xiong and L. Liu, "PeerTrust: Supporting Reputation-Based Trust for Peer-to-Peer Electronic Communities," *IEEE Trans. Data and Knowledge Eng.*, vol. 16, no. 7, 2004, pp. 843–857.
39. F. Skopik, D. Schall, and S. Dustdar, "Trustworthy Interaction Balancing in Mixed Service-Oriented Systems," *Proc. ACM Symp. Applied Computing* (SAC 10), 2010, pp. 799–806.
40. H. Koshutanski and F. Massacci, "A Negotiation Scheme for Access Rights Establishment in Autonomic Communication," *J. Network and Systems Management*, vol. 15, no. 1, 2007, pp. 117–136.
41. S. Park et al., "Resilient Trust Management for Web Service Integration," *Proc. IEEE Int'l Conf. Web Services* (ICWS 05), 2005, pp. 499–506.
42. H. Skogsrud, B. Benatallah, and F. Casati, "Trust-Serv: Model-Driven Lifecycle Management of Trust Negotiation Policies for Web Services," *Proc. 13th Int'l Conf. World Wide Web* (WWW 04), 2004, pp. 53–62.
43. W. Conner et al., "A Trust Management Framework for Service-Oriented Environments," *Proc. 18th Int'l Conf. World Wide Web* (WWW 09), 2009, pp. 891–900.
44. Z. Malik and A. Bouguettaya, "RATEWeb: Reputation Assessment for Trust Establishment among Web Services," *VLDB J.*, vol. 18, no. 4, 2009, pp. 885–911.