Journal of Information Technology Management

ISSN #1042-1319

A Publication of the Association of Management

TRUST IN CLOUD COMPUTING: MAINTAINING LONG-TERM RELATIONSHIPS

THOMAS L. NGO-YE
ALABAMA STATE UNIVERSITY
tngoye@alasu.edu

DEREK L. NAZARETH
UNIVERSITY OF WISCONSIN-MILWAUKEE
derek@uwm.edu

JAE J. CHOI
PITTSBURG STATE UNIVERSITY
jchoi@pittstate.edu

ABSTRACT

This paper examines the maintenance of trust relationships in a cloud computing environment. It specifically examines the impact of trust violations and subsequent attempts to repair the relationship in an environment characterized by multiple cloud service providers, and switching between providers is permitted. The paper develops an agent-based simulation model to probe the dynamic interaction among multiple cloud service providers and cloud service customers. The model assumes that customers select service providers on the basis of the price and trustworthiness of the services they provide. In the event of a trust violation, which typically involves a breach of contract, customers have the option to switch providers or withdraw from the cloud environment altogether. The nature and extent of the reconciliation effort will also shape the customers' decision. The model is assembled in a manner that permits varying the number of providers, the number of customers, the severity of the trust violation, the extent of the remedial action, and the prevailing economic conditions. This paper examines the effect of trust violation severity and remedial action appropriateness, under a variety of economic conditions. A model is executed for a variety of scenarios. The results indicate that there is a clear interaction effect between trust violation severity and economic conditions. Implications for cloud providers are discussed.

Keywords: cloud computing, trust violation, trust restoration, agent-based models, simulation

INTRODUCTION

Over the last decade, cloud computing has become an increasingly significant phenomenon. It has been ranked second in critical information technology issues for managers [19]. The global market for cloud computing is predicted to skyrocket, reaching $241 billion in 2020 [27]. It is considered a prime vehicle to facilitate IT-Business alignment, combining the benefits of IT efficiency and business agility [21]. Numerous advantages can be offered through cloud computing, including economy of scale, on-demand resource provisioning, and a pay-as-you-go billing model [13].

Cloud computing is rapidly becoming a preferred computing architecture for many small to medium enterprises. Aside from cost savings that accrue from not having to run an in-house datacenter, use of a public cloud eliminates the travails of operating a datacenter. This is particularly attractive when the enterprise lacks the necessary skills and expertise, and is more appealing in an era when security threats to information systems have been increasing steadily. Selection of an appropriate cloud provider is based on many factors, including provision of appropriate functionality, cost, provider reputation and reliability, and long-term stability. While switching from one provider to another is always possible, the frequency of switching is expected to be low, given the non-trivial start-up costs associated with establishing with a cloud service provider. Nonetheless, effective customer relationship management becomes crucial for the long-term viability of cloud service providers. Although trust has been identified as a key component that shapes the character of customer relationship, the majority of the prior research in the trust domain focuses on the establishment of initial trust, and does not address the maintenance of on-going trust between customer and cloud service provider. This paper adopts a longer-term aspect to trust, viewing it as a relationship that needs to be built and nurtured, but can be eroded quickly in the event of a violation of that trust. Given the on-going nature of the relationship, violations of trust can be repaired through the use of appropriate remedial action, though the assessment of the effectiveness rests solely with the aggrieved party.

In the case of cloud computing, the aggrieved party will almost always be the cloud customer. It is up to the cloud provider to recognize that a violation has occurred and offer some remedial action. The nature of violation and remedial action will shape the cloud customer's attitude to on-going trust in the provider. While the relationship is an individual one, involving two parties, in all likelihood, the trust violation will affect several customers, e.g. data breach, cloud unavailability, among others. Each customer's decision is independent, but understanding the impact at the cloud ecosystem level represents a more meaningful facet to study. In order to study the market-level effects of trust violation, a dynamic strategy is called for, wherein individual customers can be modeled. This research assembles an agent-based model that encompasses cloud providers and customers and examines the impact of varying levels of trust violation, remedial action, under a variety of economic conditions.

The rest of the paper is organized as follows. Trust in the cloud computing environment is discussed in the next section, in light of trust formation and maintenance, including trust violation and repair. An agent-based approach to study the dynamic aspect of trust in a market that encompasses multiple providers and customers is assembled and verified. The model is then applied to a number of scenarios involving trust violation. The results are presented, and implications for cloud providers are discussed.

TRUST IN THE CLOUD COMPUTING CONTEXT

Online Initial and Ongoing Trust

With the advent of e-commerce, trust has assumed an increasingly important role. Early studies in the field have established definitions and a reliable set of constructs [22], devised measurement instruments [23], and empirically tested models for trust formation in the context of e-commerce [14]. Subsequently, different forms of trust were identified throughout the transactional relationship, namely, initial trust during the establishment of the relationship, and ongoing trust with the continued existence of the relationship [2]. Initial trust refers to trust in an unfamiliar trustee, a relationship in which the actors do not yet have credible, meaningful information about, or effective bonds with each other [4]. Trust, however, plays a critical role when the relationship is long term [26]. This type of trust characterized as ongoing trust, which is formed by a calculus based trust rather than perception or initial impression [18]. Knowledge based trust is another basis for ongoing trust because ongoing trust develops over time with the accumulation of trust-relevant knowledge resulting from experience with the other party [18].

Implication of Trust in Cloud Computing

Unlike the case of e-commerce, where trust is transactional-based, the cloud computing context requires that trust assume a more long-term orientation. Trust in an e-commerce setting is shaped by individual transactions, and trust violations can be countered by low switching costs to another vendor. In the cloud computing case, the relationship has a more long-term nature, and switching costs are far greater. Nonetheless, trust has to be earned and maintained by cloud providers. Initial trust in the cloud computing case represents the trust when a customer first considers and assesses a cloud service provider. It involves customer perceptions of cloud services and their providers [20]. Factors affecting the initial trust of cloud computing include reputation and brand [24].

Ongoing trust in the cloud computing context represents the customer's trust that is built upon knowledge and calculation from outcomes resulting from long-term relationship with the cloud service provider. It is built by the cloud provider fulfilling the expectations set out in the relationship, whether they are explicitly spelled out in a service level agreement, or implicit in the customer-provider contract. A number of factors have been identified as contributing to degrading ongoing trust in the cloud computing context. These include blurred trust boundary in a cloud system (e.g. confidential information may be processed outside the known trust areas), data handling not in compliant with laws and regulations, the loss of control in data throughout its lifecycle, inappropriate use of data along the processing chain, among others [24], all of which represent issues relating to security management. Not surprisingly, security and privacy are ranked as one of the most important factors affecting trust in cloud computing [30].

Trust Violation and Rebuilding Trust

Trust violations represent a breach of the customer-provider contract, whether explicit or implicitly stated. These include problems relating to pricing, availability, confidentiality, access, reliability, and integrity, among others. They can be manifested in several ways, including price changes, overcharges, unauthorized data access, data corruption and erasure, resource unavailability, data spillage, data breaches, account hacking, extortion, and a host of other manifestations. These trust violations lead to lower knowledge and calculus based trust, and tend to degrade ongoing trust. The magnitude of offense severity (significance of trust degrading incidents) together with reconciliation tactics (correction strategies by cloud service providers) shape not only the next stage of ongoing trust in cloud customer and service provider relationship, but also the likelihood of trust rebuilding [17]. A process view of trust violation and reconciliation is presented in Figure 1, as adapted from [17].

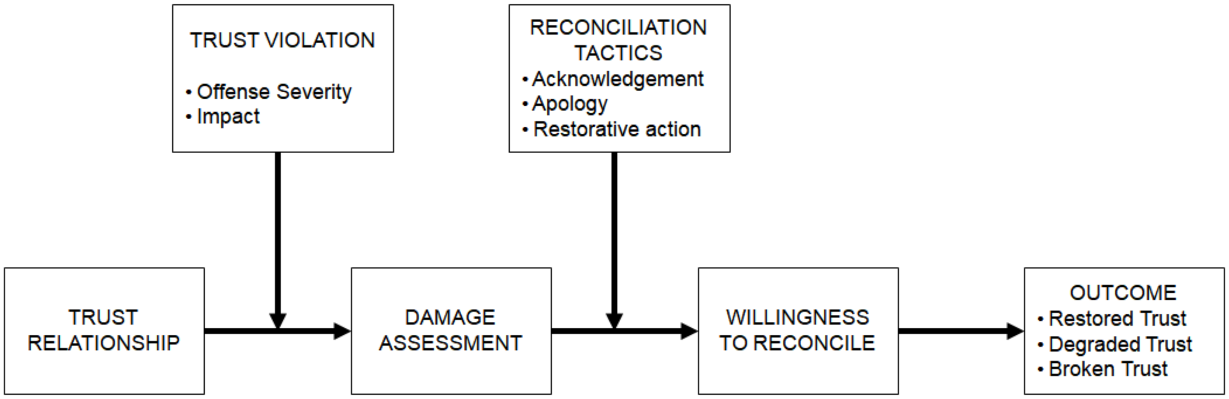

Figure 1: Trust Violation and Reconciliation Process

Reconciliation is a precedent to restored trust [29]. The offender needs to take the lead in initiating reconciliation procedure in order to successfully restore degraded trust [28]. Echoing Lewicki and Bunker [17]'s framework of reconciliation, Boyle and Panko [7] presented a three-step approach for remedial action when security breaches occur. This includes making an official apology that acknowledges responsibility, communicating complete details of the violation, and spelling out the details on actions that will be taken to compensate the damages incurred by the cloud customers. A broad range of reconciliation tactics are available, including clear definition of trust boundary in a cloud ecosystem, stricter compliance with regulations in data handling, the complete control of data throughout its lifecycle, tangible assurance of proper use of data along the processing chain, to name a few [24].

Differences in the Cloud Computing Context

Though the nature of the contract in the cloud computing context is still between two parties, the customer and provider, the manifestation of trust violations and their repair are quite different from an interpersonal trust relationship. It is unlikely that a provider will single out a customer for treatment that degrades ongoing trust. Rather, a violation is likely to affect a large number of customers simultaneously. A data breach for example, will likely affect several customers. Unavailability of the site will undoubtedly affect many more. Another key difference is that in some cases the violation may not be recognized as having occurred for an extended period, by both provider and customer. However, once the activity that constitutes the trust violation is discovered, it is incumbent on the provider to disclose this to the customers, and offer a remedy in case of harm to the customer. Anecdotal evidence in the Target and Yahoo cases suggests that providers are reluctant to disclose this, often denying or failing to acknowledge the problem. This invariably results in degraded trust, and a perception that the provider is not being transparent, and therefore not offering a meaningful remedy. The passage of time between the event and its discovery increases the possibility and magnitude of harm that can befall the customer. Yet another difference is the potential inability to repair the damage done through the trust violation. For example, a data breach involves a spill that cannot be undone. Data that is lost or corrupted through an attack may not be completely recoverable. Site unavailability represents a loss that may not be easily remedied. These differences point to the need to adopt a more nuanced approach to modeling the trust violations and their remedial actions.

METHODOLOGY AND CLOUD TRUST LIFECYCLE MODEL

The conventional social science research methodology, in all likelihood, will be inadequate to explore the dynamic aspect of the trust lifecycle in cloud computing. While the methodology is strong in areas of investigating cause and effect relationships in controlled environments, it requires intervention and observation in real world settings. The ability to examine the impact of different interventions under a variety of scenarios is often impractical, particularly with emerging technologies. Accordingly, a modeling based approach, that permits systematic variation of variables of interest, under a variety of controlled scenarios, would be better suited to understanding the dynamic effect of trust in the cloud computing environment. To this end, a design science approach will be employed as the principal research methodology. A core aspect of the design science methodology is the adoption of an IT artifact that can be studied under a variety of conditions. In this research, a simulation model will be adopted to assess the impact of trust in the cloud computing environment. Several options are available for the simulation model, including discrete event simulation, continuous simulation, agent-based modeling, and system dynamics, among others. Given that the cloud environment is composed of a number of independent and interacting decision makers, in this case providers and customers, the most appropriate approach is an agent-based approach.

Agent-based modeling is a form of computational simulation that permits the study of phenomena over time by modeling the individual actors in the simulation context [5] and is a technique used to generate a simplified representation of social reality [15]. Agents represent entities in the system with the ability to function autonomously. Candidate agents in this case include customers, providers, regulators, competitors, and the like. A review of previous literature forms the basis for identifying key agents and their behavior. Once the behavior of an individual agent is programmed, it becomes important to assess the effectiveness of their logic, not as independent operators, by as interacting operators. This process of calibration and testing in essence forms a behavioral preproduction test. The model is then tested for both structural robustness and behavioral reproduction. Subsequent stages involve scenario development, analysis of simulation outcomes, and interpretation of results. In this research, the modeling and simulation were conducted using NetLogo, currently one of the most popular agent-based simulation platforms. The user interface of cloud trust lifecycle model is presented in Figure 2.

The conventional social science research methodology, in all likelihood, will be inadequate to explore the dynamic aspect of the trust lifecycle in cloud computing. While the methodology is strong in areas of investigating cause and effect relationships in controlled environments, it requires intervention and observation in real world settings. The ability to examine the impact of different interventions under a variety of scenarios is often impractical, particularly with emerging technologies. Accordingly, a modeling based approach, that permits systematic variation of variables of interest, under a variety of controlled scenarios, would be better suited to understanding the dynamic effect of trust in the cloud computing environment. To this end, a design science approach will be employed as the principal research methodology. A core aspect of the design science methodology is the adoption of an IT artifact that can be studied under a variety of conditions. In this research, a simulation model will be adopted to assess the impact of trust in the cloud computing environment. Several options are available for the simulation model, including discrete event simulation, continuous simulation, agent-based modeling, and system dynamics, among others. Given that the cloud environment is composed of a number of independent and interacting decision makers, in this case providers and customers, the most appropriate approach is an agent-based approach.

Agent-based modeling is a form of computational simulation that permits the study of phenomena over time by modeling the individual actors in the simulation context [5] and is a technique used to generate a simpli-

fied representation of social reality [15]. Agents represent entities in the system with the ability to function autonomously. Candidate agents in this case include customers, providers, regulators, competitors, and the like. A review of previous literature forms the basis for identifying key agents and their behavior. Once the behavior of an individual agent is programmed, it becomes important to assess the effectiveness of their logic, not as independent operators, by as interacting operators. This process of calibration and testing in essence forms a behavioral preproduction test. The model is then tested for both structural robustness and behavioral reproduction. Subsequent stages involve scenario development, analysis of simulation outcomes, and interpretation of results. In this research, the modeling and simulation were conducted using NetLogo, currently one of the most popular agent-based simulation platforms. The user interface of cloud trust lifecycle model is presented in Figure 2.

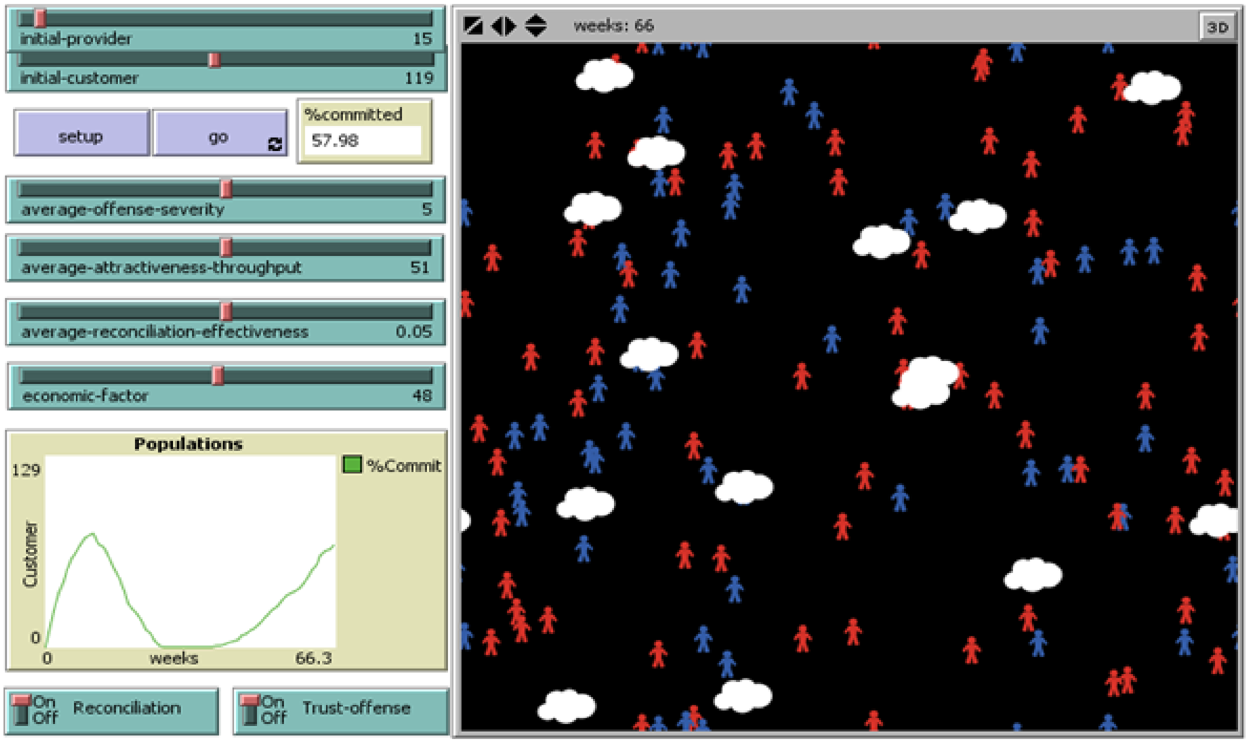
initial-provider 15
initial-customer 119
setup
go
%committed 57.98
average-offense-severity 5
average-attractiveness-throughput 51
average-reconciliation-effectiveness 0.05
economic-factor 48
On Off Reconciliation
On Off Trust-offense
weeks: 66

Figure 2: Cloud Trust Lifecycle Model

The model was developed using the Dynamic Security–Trust lifecycle model as a basis [11]. The Dynamic Security-Trust lifecycle model is equipped with the fundamental features, capturing the role of trust in dynamic interactions between e-commerce vendors and customers. An extensive series of modification, recalibration, and extension has been performed to ensure that the model truly reflects the cloud computing industry. The original Dynamic Security-Trust lifecycle model comprises a single provider and multiple customers to investigate trust in the e-commerce market. However, this approach is a little simplistic, and not truly representative of the cloud computing ecosystem. In this case, it is necessary to model multiple cloud providers, with the understanding that switching is possible in the case of broken trust, though it entails non-significant costs. As illustrated in Figure 2, the population of both cloud service providers and customers are now user-adjustable. It allows decision makers to simulate different market conditions where multiple cloud service providers interact with many customers. Accordingly, cloud services are available at various price points from multiple service providers. Information on two critical factors affecting the choice of cloud service provider, namely, price and trustworthiness is available to all potential cloud customers in the model.

Price is mainly determined by economic factor, a user-input variable to represent overall economic performance in industry. Growing economies involve short term disparities between available supply and increasing demand, thereby triggering a price increase. As a result, there are noticeable impacts on the market share of each cloud provider. Although overall price index follows the trend mandated by economic factor, individual prices are chosen by the model at the time of running the simulation.

Another critical piece of information to determine the choice of cloud service provider is trustworthiness. This is determined based on the combination of initial and ongoing trust for a specific cloud service provider. The initial value of trustworthiness at the beginning stages of simulation runs exclusively represents initial trust, and is shaped primarily by the customer's perceptions of cloud services and their providers [20]. The typical basis for these perceptions include reputation and brand [24]. As the simulation progresses, trustworthiness is degraded or strengthened as ongoing trust assumes a more prominent role. The sources of ongoing trust degradation includes data transactions outside of known cloud trust boundary, non-compliant data handling, the loss of control in data handling, inappropriate use of data, and any incidents related to mismanaged security and privacy [24; 30].

An individual cloud service provider's attractiveness is determined by the price of its offered cloud service and trustworthiness. When the cloud service provider's attractiveness exceeds an individual customer's psychological throughput, the customer enters into a contractual relationship with a specific cloud service provider. Once subscription is initiated, a mutual commitment is formed between the cloud service provider and the customer for the given cloud service in the scenario. The relationship remains in force as long as the customer is satisfied with the services provided. In the event of an offense that represents a breach of trust, the overall trustworthiness of the provider degrades to some extent. As long as the provider's trustworthiness is above a specific threshold, the relationship continues. The model permits the user to set an average level of trustworthiness, but specific decisions by individual customers are shaped by conditions during the simulation, representing the ability of individual customers to behave independently. The attractiveness can degrade over time as price or trustworthiness changes. In a growing economy, the price increases accordingly. This has an adverse effect on the attractiveness of a provider. Eventually, price increases will decrease the market share of individual providers by reducing their attractiveness. Trustworthiness, another critical component of attractiveness, degrades significantly due to trust offense related to the known cloud trust boundary, data handling compliance, control/authorship of data handling, or security/privacy breaches. Depending on the level of offense severity, the degradation of trustworthiness can become critical enough to push the overall attractiveness below the customer's threshold. The average offense severity in cloud computing economy is a user-input; however, the level of severity in each incidence in the simulation is set by the model.

A successful long-term relationship can be achieved through proper pricing strategies and trust management by cloud service providers. This research focuses more on ongoing trust management. It is accomplished by maintaining proper security control, appropriate security policy, incidence responses, privacy management, trust network management, implementation of data processing compliance mechanism. When a trust offense occurs, leading to degraded trustworthiness, a reconciliation process (trust rebuilding strategies) to restore trust for the cloud service provider is critically needed. The process involves the aforementioned theoretical trust rebuilding procedure for ongoing trust, corrective actions to correct the major source of trust violation. This could include ensuring that confidential information is processed within the clear boundary of trust in the cloud ecosystem, implementing policies to comply laws and regulations, improvements in privacy and security protection, and the like. The magnitude of reconciliation strategies lies on the effectiveness of these actions. The effectiveness is adjustable by the model users. Once again, however, individual effectiveness will be randomly set by the model. Reconciliation strategy will eventually rebuild trustworthiness and push the attractiveness over the threshold if it is effective enough. Economic factor and relevant price, however, can intervene the trust rebuilding procedure in the model. Such intervening effect can be extensively scrutinized in simulation analysis.

The model incorporates two breeds (categories) of agents, namely, cloud service providers and cloud customers. As depicted in Figure 2, cloud shaped agents represent cloud service providers while person shaped agents represent customers. Blue colored customers signify customers without committed cloud service subscriptions. On the other hand, red colored customers represent customers who are currently subscribing to one of cloud services offered by the providers in the model. The cloud provider behavior is shaped by several variables – price, offense severity, trustworthiness, and attractiveness. The price at the start of the simulation is determined by the overall economic conditions. Initially, all providers have the same level of attractiveness. However, since ongoing trust is managed differently for each provider, the values of trustworthiness diverge over the simulation. When a trust-breaking event occurs, the offense severity specifies how critical it was. Offense severity is initially zero for all providers, but as time goes by the industry average parameter starts to shape the overall level of trustworthiness. Examples of functions and variables utilized in the model are listed in Table 1.

Table 1: Model Method and Variable Description

Variable/method	Function structure	Limits
Assign-price	Random-near (ln(economic conditions))	0 – 50
Assign-attractiveness	f(price, trustworthiness)	No limit
Assign-attractiveness-throughput	User input	1 – 100
Assign-reconciliation-effectiveness	User input	0 – 0.1
Trustworthiness	Initially 50 at the beginning of simulation run	No limit
nCustomer (i)	Number of customers for provider(i)	0 – 250
nProvider	Number of provider	0 – 250
Offense severity	User input	0 – 10
Economic conditions	{shrinking, steady-state, growing}	2 – 100

MODEL VALIDATION AND SCENARIO ANALYSIS

Pilot Test under Moderate Economic Conditions

The initial validation of current version is accomplished through a behavioral reproduction test. In this case, the simulation outcomes are compared to historical real-world data. Three scenarios were used to develop a robust model. In the pilot assessment, no reconciliation tactics are applied so as to better understand the impact of offense severity. The experimental scenarios are described in Table 2, and the results appear in Figure 3.

Table 2: Pilot Scenarios for Trust Offense Severity in a Steady-State Economy

Scenario	Offense Severity	Economic Conditions
Pilot Scenario 1	Low	Steady-state
Pilot Scenario 2	Medium	Steady-state
Pilot Scenario 3	High	Steady-state

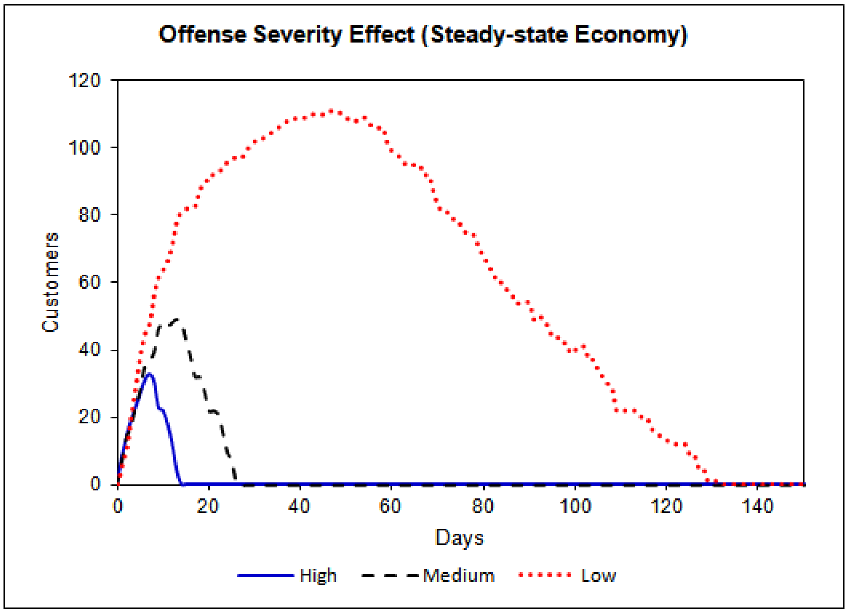

Figure 3: Trust Offense Severity Effect in a Steady-state Economy

The graph represents the number of cloud service subscribing customers at different levels of trust offense severity in a steady-state economy. The steady-state economy is not characterized by any expansion or contraction. It is a dynamic economy that involves entry of new and innovative firms, as well as sun-setting of older firms [12]. It is different from a stagnant economy, wherein the economic policies adopted to stimulate growth have failed. In a steady-state economy, customers have choices and can engage in switching behavior, if appropriate. In situations where the offense severity is low, customers initially stay with the providers. However, if the behavior persists over a long period, trust eventually degrades, and customers pull away from cloud computing as a viable alternative. If the offense severity increases, e.g. more conspicuous hacking and data spillage, then relatively few customers elect to use cloud computing as an alternative, and the cloud computing industry fails to gain traction. Given that this is a steady-state economy, customers will have resources at their disposal, which makes them less dependent on cloud providers to curtail computing costs. At very high levels of offense severity, e.g. widespread and well publicized hacking and data breaches, the industry faces an uphill battle to even establish itself, and peters out relatively quickly. The patterns in each scenario clearly illustrate that the model reflects expectation and demonstrates that it is functioning properly. It partially fulfills the behavioral reproduction test.

Extended Pilot Test under Varying Economic Conditions

The results from the previous section serve to demonstrate that the model can reproduce the expected reality at different levels of trust offense severity. However, further structural robustness and behavioral reproduction tests need to be conducted under different economic conditions since the initial pilot test addresses a steady-state economy only. A set of extended pilot test scenarios are developed and presented in Table 3.

Table 3: Trust Offense Severity under Various Economic Conditions

Scenario	Offense Severity	Economic Conditions
Scenario 1	Low	Growing
Scenario 2	Medium	Growing
Scenario 3	High	Growing
Scenario 4	Low	Shrinking
Scenario 5	Medium	Shrinking
Scenario 6	High	Shrinking

A growing economy is characterized by several aspects, including aggregate growth, exhibited by high rates of growth per capita and productivity, coupled with structural transformation, including shifts from traditional industries to new industries [16]. The growth needs to be sustained, and not fleeting or momentary in nature. A shrinking economy, on the other hand, is characterized by a reduction is gross domestic product. Typically, it involves a reduction in consumption as well as domestic product, higher unemployment, and a concomitant increase in government spending. In the cloud computing context, a growing economy offers more choices for the customers, while the shrinking economy will be characterized by very few cloud providers. In an effort to understand the role of economic conditions on the cloud computing market in the wake of trust breaches, several scenarios were simulated at varying levels of offense severity. As before, no reconciliation effort was attempted, so as to isolate the effect of offense severity. The results are presented in Figure 4 and 5.

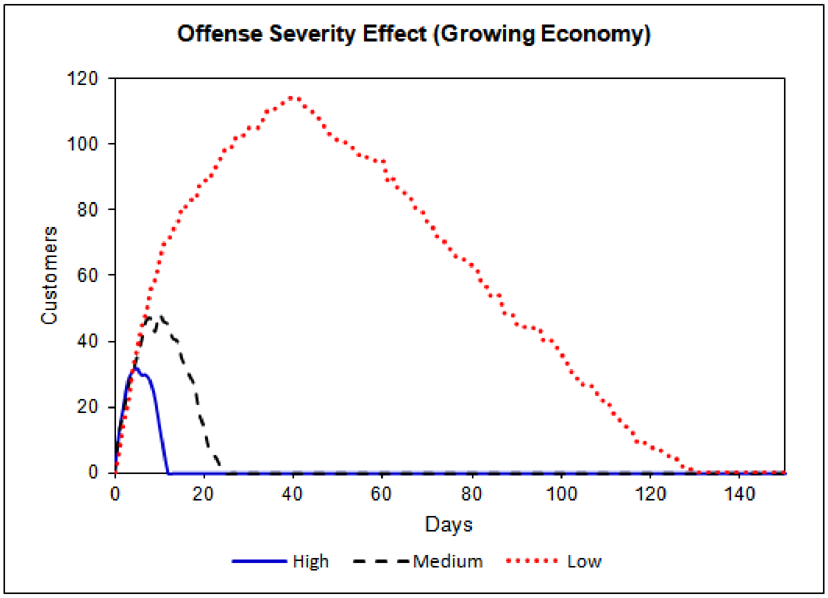

Figure 4: Trust Offense Severity Effect in Growing Economy

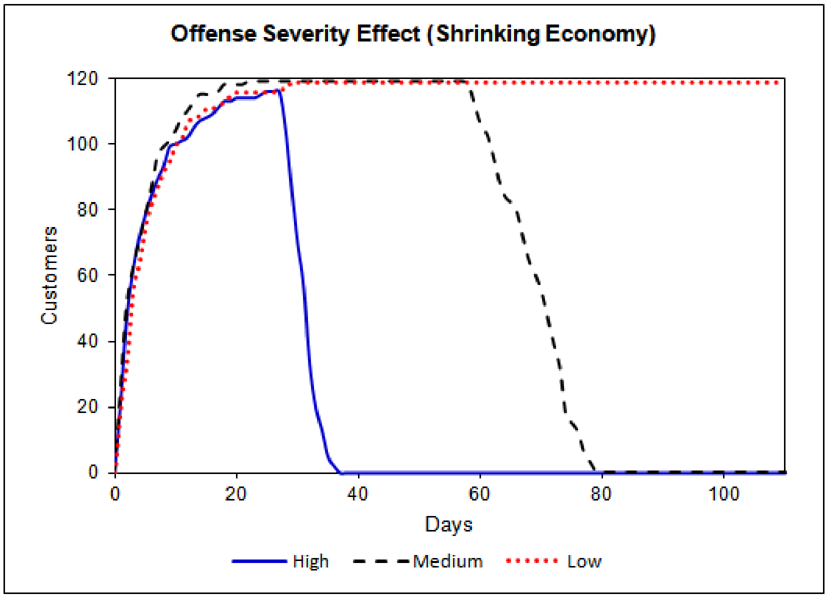

Figure 5: Trust Offense Severity Effect in Shrinking Economy

The growing economy reflects the steady-state economy to a large extent, except that the observed effects are a little more pronounced. Once again, the growing economy is indicative of a situation where the customers have resources at their disposal, and are not dependent on cloud providers to offer savings in data center operating costs. It also drives home the point that breaches of trust have a clear and prominent effect in a growing economy.

Scenarios involving a shrinking economy display a considerably different pattern. In all cases, the cloud economy is able to garner a large number of customers in the early stages of the simulation. This reflects the need to use cloud-based solutions as a means of keeping computing costs down. For situations involving minor trust violations, customers are willing to give the providers the benefit of the doubt, and continue with the use of cloud-based computing as an alternative to in-house data centers. However, as the offense severity increases, customers begin to rethink the relationship. For sustained trust breaches, customers elect to drop the subscription relationship. However, in the case of serious offenses, the degradation of trust is immediate, and the fall-off in customers is precipitous. This indicates that the expected savings through the use of cloud computing is not enough to offset the degradation in trustworthiness This is a significant result, indicating that customer behavior is not consistent across different economic conditions.

Another obvious observation in Figure 5 is that the number of cloud service subscribers reaches almost the same level regardless of the magnitude of trust offenses before any changes are made. This is a contrasting pattern from cases under medium or flourishing economy where scenarios involving more severe trust violations lead to considerably lower participation in the cloud economy.

These two sets of simulations indicate that the model is reasonably robust and can represent the reality of cloud industry under a variety of different conditions. The model will be used to evaluate the effectiveness of reconciliation tactics in the face of a trust violation.

Scenario Analysis

The simulations described so far illustrate that trust, once broken, will not repair on its own, leading to an unsuccessful cloud economy in almost all cases. Clearly, cloud providers cannot simply stick their heads in the sand and expect that customers will flock back, on the assumption that customers have no other feasible alternative. Customers need to safeguard their data, and prolonged exposure through hacking and data breaches will trigger an exodus. Providers need to take some actions that indicate acknowledgement and reconciliation. Reconciliation can range from an acknowledgement and a promise to do better in the future, to gestures involving financial compensation. Ideally, the reconciliation will match the extent of the trust violation. The extent of reconciliation will shape the propensity of customers to return to the cloud economy. The new set of simulations examines the impact of three levels of reconciliation tactics in the face of trust violations. The scenarios are described in Table 4, and the results depicted in Figure 6.

Table 4: Reconciliation Effectiveness in a Steady-state Economy

Scenario	**Reconciliation Effectiveness**	**Economic Conditions**	**Offense Severity**
Scenario 1	Low	Steady-state	Medium
Scenario 2	Medium	Steady-state	Medium
Scenario 3	High	Steady-state	Medium

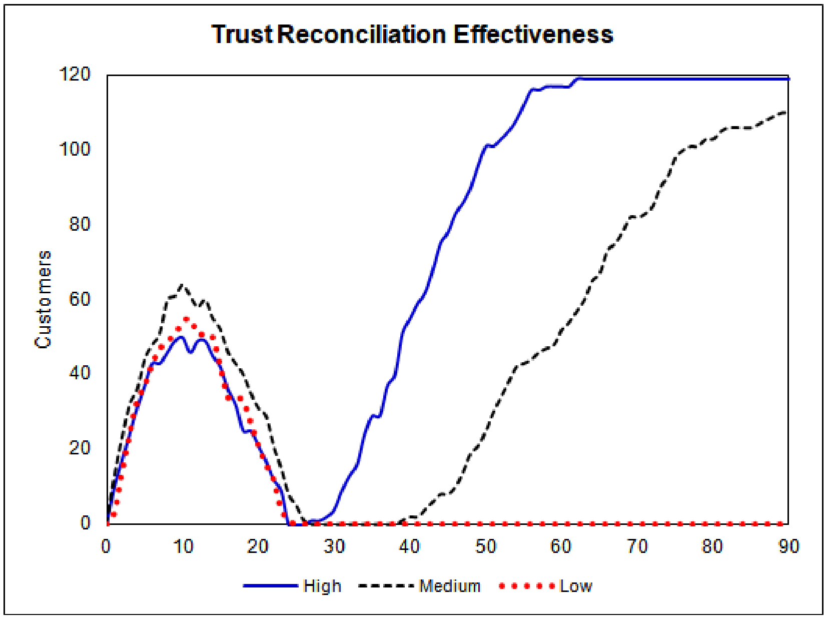

Figure 6: Effect of Trust Rebuilding Strategies

The graph illustrates the number of cloud service subscribing customers at different levels of trust rebuilding strategies implemented to correct trust violations. In the earlier stages of simulation runs, the curves in all the scenarios closely follow the pattern of pilot test cases shown in the previous figures. The number of subscribers initially increases as simulation progresses. However, the onset of trust violations causes customers to abandon their relationship with the providers. At this point, different trust reconciliation actions are employed, and the effect on the customer population is depicted.

The three levels of trust rebuilding strategies (each consists of reconciliation process, remedial correction activity for data handling, and general security/privacy management) attempt to rectify the trust violation. If a minor reconciliation effort is attempted, it proves to be wholly unsuccessful in enticing customers to sign up again. This illustrates the need for a match between the trust violation and the degree of reconciliation offered. In this case, the trust violation is of a medium magnitude, and the reconciliation effort is low. Customers will perceive this to be an inadequate response, and hence not reengage with the cloud providers. On the other hand, if a more suitable reconciliation action is proffered, there is a greater likelihood that the customers will reengage, as illustrated in the figure. In the case of overly generous reconciliation efforts, the extent of reengagement is the same, but will occur sooner. The decision as to which tactic to adopt remains a subjective one. The overly generous reconciliation approach will cause earlier reengagement of customers, leading to a larger revenue stream, and possibly more loyal customers. This has to be traded off against the greater cost incurred during reconciliation. On the other hand, the more moderate reconciliation efforts will entail reduced up-front costs, but will reach the same results in terms of total number of reengaged customers, albeit at a slower rate. This involves an initial tradeoff in lost revenue, but that may be acceptable in the long run.

DISCUSSION AND MANAGERIAL IMPLICATIONS

The simulations provide an illustrative backdrop for the role of trust in the decision making in the cloud computing adoption process. In essence, there are five decision points – three for the customer, and two for the provider, though some of these may be involuntary and not within the complete control of the decision maker.

The first decision is for customers to engage with the cloud providers. There are several factors that are relevant to the decision, including the need for computing capability, the availability of in-house computing, the relative cost of in-house computing vis-à-vis cloud computing, the reputation of the providers, among others. This decision is driven by the initial trust formed by the customer in the provider. The decision will occur at different points in time for various customers, and will entail different thresholds. Customers will engage with different cloud providers, based on their relative attractiveness.

The second decision point is that of the trust violation, on the part of the cloud provider. In all likelihood, this is an involuntary event, though it is often attributable to a conscious decision made earlier. Thus, for example, hacking and data breaches are the result of inadequate security deployed by the provider. The recent spate of ransomware attacks stem from decisions to not patch old operating systems. It is conceivable, but unlikely, that the trust violation is a conscious decision on the part of the cloud provider, e.g. violations of the terms of the contract, price increases, service reductions, and the like. At this stage, it is on-going trust that is being eroded by the violation. It is the magnitude of the trust violation that will determine the extent of customers disengaging from the cloud economy. In all cases, the greater the offense severity, the sooner the customers will disengage. Even small trust violations will cause customers to disengage.

The third decision is the act of disengaging or continuing to engage with the cloud provider in the face of trust violations. The customer determines if the trust violation is serious enough that the costs of further exposure will outweigh the benefits of continuing to use the cloud provider. Once again, this is an individual decision, and different customers will arrive at independent outcomes, and at varying points of time. Clearly the magnitude of the offense severity will have a major impact on the decision, with higher levels of offense severity leading to faster and greater abandonment by customers. In the trust context, this is a case of broken trust, and is shaped by the trustworthiness of the provider relative to a customer specific threshold. This decision is also dependent on prevailing economic conditions, wherein customers in a shrinking economy are more reluctant to disengage from their cloud provider, whereas steady-state and growing economies prompt more flight.

The next decision represents the reconciliation tactics to be adopted by the cloud provider. This represents an effort to rebuild the broken trust. The simulations indicate that doing nothing is not an option, since the number of engaged customers is eventually driven down to zero under all levels of offense severity. However, if inadequate remediation tactics are employed, there is no reengagement from the customer. From a strictly economic perspective, this approach can be dispensed with, since it only entails costs, with absolutely no benefit in terms of reengaged customers. The cloud provider may as well not offer any reconciliation effort, since it results in the same level of customer reengagement. The moderate and aggressing reconciliation efforts both result in restored trust, though the speed at which customers reengage is different. Cloud providers need to trade off the increased cost of aggressive reconciliation tactics with the increased short-term revenue, and the potentially greater loyalty among customers. It should be borne in mind that these findings are relative and not absolute, i.e. the nature of reconciliation should match the level of offense severity. Thus, low levels of reconciliation tactics may be adequate when the trust violations are minor, and moderate reconciliation tactics may be inadequate for severe trust violations.

The last decision point is that of the customer determining to reengage in light of the reconciliation efforts on the part of the cloud provider. As before, this is an individual decision that is shaped by the nature of the trust violation, the adequacy of reconciliation effort, the relative price of the cloud services, and the demand for service, among others. This decision addresses whether to restore the trust relationship, and represents repaired trust if the relationship is resumed. The decision as to when and under what circumstances to reengage remains an independent decision, and will occur at different points in time, and with different providers for different customers.

CONCLUSIONS

This research examines the role of trust in the cloud computing environment. It characterizes trust as something that needs to be earned, that can be lost through a violation, but can be restored through appropriate reconciliation. It develops an agent-based model to simulate the phenomenon. The model was validated through a series of simulations under a variety of conditions. The role of offense severity, and trust rebuilding strategies, under different economic conditions were examined to elicit useful implications for managers at cloud service provider firms.

REFERENCES

[1] Ackoff, R. L. (1961), "Management Misinformation Systems," *Management Science*, 14*(*4), 147-156.

[2] Beldad, A., De Jong, M. and Steehouder, M. (2010), “How shall I trust the faceless and the intangible? A literature review on the antecedents of online trust,” *Computers in Human Behavior, 26* (1), 857-869.

[3] Benbasat, I., and Zmud, R.W. (2003), “The Identity Crisis within the IS Discipline: Defining and Communicating the Discipline’s Core Properties,” *MIS Quarterly*, *27*(2), 183-194.

[4] Bigley, G.A., and Pearce, J.L. (1998), “Straining for shared meaning in organization science: Problems of trust and distrust”, *Academy of Management Review*, *23* (3), 405-421.

[5] Bonabeau, E. (2002), “Agent-based modeling: Methods and techniques for simulating human systems”, *Proceedings of the National Academy of Sciences, 99* (3), 7280-7287.

[6] Bonini, C.P. (1963), *Simulation of Information and Decision Systems in the Firm*, Englewood Cliffs, NJ: Prentice-Hall.

[7] Boyle, R., and Panko, R. (2013), *Corporate Computer Security*, Upper Saddle River, NJ: Pearson Education.

[8] Broadbent, M., Weill, P., O’Brien, T., and Neo, B.S. (1996), “Firm Context and Patterns of IT Infrastructure Capability,” in *Proceedings of the 14th International Conference on Information Systems*, Cleveland, OH, 174-194.

[9] Carr, N.G. (2005), “The end of corporate computing”, *MIT Sloan Management Review, 46* (3), 67-73.

[10] Carroll, J. (2005), “The Blacksburgh Electronic Village: A Study in Community Computing,” in *Digitial Cities III: Information Technologies for Social Capital*, P. van den Besselaar and S. Kiozumi (eds.), New York: Springer-Verlag, 43-65.

[11] Choi, J. and Nazareth, D.L. (2014), “Repairing trust in an e-commerce and security context: an agent-based modeling approach,” *Information Management & Computer Security, 22* (5), 490-512.

[12] Daly, H.E. (1991), *Steady-state economics: with new essays*, Washington DC: Island Press.

[13] European Parliamentary Research Service (2014), *Potential and Impacts of Cloud Computing Services and Social Network Websites*, Research Report.

[14] Gefen, D., Karahanna, E., and Straub, D. (2003), "Trust and TAM in online shopping: An integrated model source", *MIS Quarterly, 27* (1), 51-90.

[15] Gilbert, N. (2008), *Agent-Based Models*, Thousand Oaks, CA: SAGE Publications.

[16] Kuznets, S. (1966), *Modern Economic Growth: Rate, Structure and Spread,* New Haven: Yale University Press.

[17] Lewicki, R, and Bunker, B. (1996), “Developing and maintaining trust in working relationships", in Kramer, R.M. & Tyler, T.r. (Eds.), *Trust in organizations: Frontier of theory and research,* Thousand Oaks, CA: Sage, 114-139.

[18] Lewicki, R. and Bunker, B.B. (1995), “Trust in Relationships: A Model of Trust Development and Decline” in Deutsch, M., Bunker, B.B, and Rubin, J.Z. *Conflict, Cooperation and Justice,* Jossey-Bass, San Francisco, 133-173.

[19] Luftman, J. and Zadeh, H.S. (2011), “Key information technology and management issues 2010–11: an international study”, *Journal of Information Technology, 26* (3), 193-204.

[20] Lynn, T., van der Werff, L., Hunt, G., and Healy, P. (2016) "Development of a Cloud Trust Label: A Delphi Approach", *Journal of Computer Information Systems, 56* (3), 185-193.

[21] Marston, S., Li., Z., Bandyopadhyay, S., Zhang, J., and Ghalsasi, A. (2011), “Cloud computing – The business perspective”, *Decision Support Systems, 51* (1), 176-189.

[22] McKnight, D.H. and Chervany, N.L. (2002), “What trust means in E-Commerce customer relationships: An interdisciplinary conceptual typology*”, International Journal of Electronic Commerce, 6* (2), 35-59.

[23] McKnight, D.H., Choudhury, V., and Kacmar, C. (2002), “Developing and validating trust measures for e-Commerce: An integrative typology”, *Information Systems Research,13* (3), 334-359.

[24] Pearson, S. and Yee, G. (2013), *Privacy and Security for Cloud Computing: Computer Communications and Networks,* London, UK: Springer-Verlag.

[25] Pearson, S., & Benameur, A. (2010), “Privacy, security and trust issues arising from cloud computing”, *Proceedings of the 2010 IEEE Second International Conference on Cloud Computing Technology and Science (CloudCom),* Indianapolis, IN, 693-702.

[26] Ping Li, P. (2012), “When trust matters the most: The imperatives for contextualising trust research”, *Journal of Trust Research, 2* (2), 101-106.

[27] Reid. S. and Kilster, H. (2011), *Sizing the Cloud,* Forrester Research Report.

[28] Tomlinson, E. and Lewicki, R. (2003), “Trust and Trust Building”, *Intractable Conflict Knowledge Base Project, Conflict Research Consortium,* University of Colorado.

[29] Tomlinson, E., Dineen, R., and Lewicki, R. (2004), “The road to reconciliation: Antecedents of victim willingness to reconcile following a broken promise”, *Journal of Management, 30* (2), 165-187.

[30] Uusitalo, I., Karppinen, K., Juhola, A., and Savola. R. (2010), "Trust and cloud services-an interview study", in *Proceedings of 2010 IEEE Second International Conference on Cloud Computing Technology and Science (CloudCom),* Indianapolis, IN, 712-720.

[31] Varpe, Y.D. and Nirmal, M.D. (2016), “A Trust Label System For Communicating Trust in Cloud Services”, *International Journal of Advanced Engineering and Global Technology, 4* (6), 1381-1384.

AUTHOR BIOGRAPHIES

Thomas L. Ngo-Ye is Assistant Professor of Computer Information Systems in College of Business Administration at Alabama State University. He received his Ph.D. in MIS from the University of Wisconsin-Milwaukee. His research interests include business intelligence and analytics, data mining, text mining, sentiment analysis, e-Commerce, enterprise information systems, cloud computing, and trust in information technology. Dr. Ngo-Ye's research has been featured at *Decision Support Systems, Expert Systems with Applications, ACM Transactions on Management Information Systems, Journal of Computer Information Systems, International Journal of Intelligent Information Processing, Journal of Integrated Enterprise Systems, and Issues in Information Systems,* and several leading IS conferences. He received the best research paper award at the BI Congress held in Orlando in 2012. He is the recipient of numerous grants and scholarships.

Derek L. Nazareth is Associate Professor of IT Management at the University of Wisconsin-Milwaukee. He received his PhD in MIS from Case Western Reserve University. His current research interests include web services composition, medical informatics, and information security. His papers appear in *IEEE Transactions on Knowledge and Data Engineering, ACM Transactions on Management Information Systems, Journal of Management Information Systems, IEEE Transactions on Systems Man & Cybernetics, Decision Support Systems, Communications of the ACM, Information & Management,* and other journals and conference proceedings. He served as the Program Chair for AMCIS, and the Treasurer for ICIS.

Jae J. Choi is Associate Professor of Computer Information Systems in the Kelce College of Business at Pittsburg State University. He received his Ph.D. in MIS from the University of Wisconsin-Milwaukee. His research interests include IT infrastructure, web services, simulation/modeling, information security, and electronic commerce. Dr. Choi’s research has been featured at *Journal of Management Information Systems, Information & Management, ACM Transactions on Management Information Systems, IEEE Transactions on Systems Man &*

Cybernetics, and several leading IS conferences. He served as a program committee member for the DESRIST and a mini-track chair for AMCIS. He is the recipient of numerous grants and scholarships.