Computer Standards & Interfaces 35 (2013) 1–5

Contents lists available at SciVerse ScienceDirect

Computer Standards & Interfaces

journal homepage: www.elsevier.com/locate/csi

Data security services, solutions and standards for outsourcing

Kevin W. Hamlen, Bhavani Thuraisingham *

The University of Texas at Dallas, United States

ARTICLE INFO

Article history:
Received 4 May 2011
Received in revised form 9 December 2011
Accepted 6 February 2012
Available online 4 May 2012

Keywords:
Web services
Access control
Inference control
Identity management
Mobile code security

ABSTRACT

Globalization has resulted in outsourcing data, software, hardware and various services. However, outsourcing introduces new security vulnerabilities due to the corporation's limited knowledge and control of external providers operating in foreign countries. Security of operation is therefore critical for effectively introducing and maintaining these business relationships without sacrificing product quality. This paper discusses some of these security concerns for outsourcing. In particular, it discusses security issues pertaining to data-as-a-service and software-as-a-service models as well as supply chain security issues. Relevant standards for data outsourcing are also presented. The goal is for the composite system to be secure even if the individual components that are developed by multiple organizations might be compromised.

1. Introduction

Data has become a critical resource in many organizations, including efficient data access, data sharing, data mining, and their applications for effective decision-making. Data and information must be protected from unauthorized access as well as malicious corruption. The advent of the World Wide Web (WWW) in the mid 1990s has resulted in even greater demand for managing data, information and knowledge effectively. There is now so much data on the web that managing it with conventional tools is becoming almost impossible. For example, Google's indexing system stores tens of petabytes of data with updates processed in parallel by thousands of machines per day worldwide [1]. These demands exceed the capabilities of traditional centralized operating systems and file systems, requiring new tools and techniques to effectively manage such large and dynamic data repositories.

Web services are an important class of technologies that has emerged in recent years in response to this need. In service-oriented web architecture, data processing and other tasks that would otherwise need to be performed internally are shifted to external servers that communicate via standard web protocols. Typical examples of web services include making an airline reservation or filing an income tax return, both of which can be carried out by external service providers with a small amount of communication overhead from the service recipient.

Globalization and various treaties such as NAFTA (North American Free Trade Agreement) and the founding of the European Union have resulted in increased outsourcing of data, software, hardware and various services. This is typically motivated by cost-cutting. For example, while it costs about $60 K plus benefits of about $30 K per year to employ a software engineer with a BS education in the US, it only costs the corporation about $16 K to employ that same software engineer in India. The explosion of the web and tools such as web services that support light-weight distributed computing have multiplied outsourcing activities by many times during the past decade. Many of the computing activities as well as data management, banking and telecommunication services are now being outsourced to foreign countries such as India and China. Due to this explosion of services, countries like India are unable to keep up with the demand for IT professionals. It was mentioned at the Indo-US Summit on Infrastructure Security sponsored by the US National Science Foundation (NSF) and the Indo-US Science and Technology Forum (IUSSTF) in Bangalore, India in January 2010 that India is planning massive expansions to their educational systems and infrastructure with an addition of possibly one hundred universities. It is very likely that this will increase the amount of outsourcing services and agreements between US and India significantly.

While many believe that outsourcing is good for both the service consumer and the service provider, outsourcing results in increased security vulnerabilities because organizations typically have more limited knowledge and control of externally located employees and business operations. Untrusted individuals may have access to critical components of the system located abroad, and can use this access to effect attacks, such as malicious code injection. Therefore, it is critical that security concerns be examined and addressed for outsourcing activities. Furthermore, it is also critical that the composite system operate securely even if some of the individual components of the system are not secure. This allows safe outsourcing to semi-trusted or untrusted partners, and is especially important for secure, efficient

* Corresponding author.
E-mail address: bhavani.thuraisingham@utdallas.edu (B. Thuraisingham).

0920-5489/$ – see front matter © 2012 Elsevier B.V. All rights reserved.
doi:10.1016/j.csi.2012.02.001

supply chain management. Many US manufacturers obtain parts and services from a variety of foreign countries, including Eastern Europe, South Asia and East Asia. The composite supply chain must operate securely even though it may be infeasible to demand such stringent security requirements for certain externally-located portions of the worldwide supply chain. This is a significant challenge. Security must be addressed at the outset of the outsourcing activity, and the participating organizations must include security in their service level agreements.

In this paper we discuss some of the security challenges that result from outsourcing. In Section 2, we discuss the emerging popular concept of "Data and Software as Services," and we examine the security impact. Mobile code security in the data outsourcing process is discussed in Section 3. In Section 4, we discuss security for supply chain management. The novel notion of data supply chain management in assured information sharing is discussed in Section 5. Section 6 concludes with a discussion of incentives and risks in data outsourcing. Relevant standards are discussed in Section 7. Assured cloud-based data sharing for outsourcing is discussed in Section 7. The paper is concluded in Section 9 with a discussion of the directions.

2. Data and software as services

"X as a service" (XaaS) is an increasingly popular mantra in IT circles [2], where "X" can be data, software platforms, computing infrastructure, or various other resources. With data as a service, an organization can utilize a data provider to obtain and process data externally to the organization itself. In the case of software, an organization can obtain a compiler, operating system, or software application as a service from a service provider. In this section, we will elaborate on such services for outsourcing and describe their security impact [3].

The Data-as-a-Service (DaaS) model is increasing in popularity [4]. For example, corporations such as ChoicePoint and Acxiom manage data for various corporations in the financial and medical industries. These data services may include data security and privacy as well as data quality and cleansing services. Integrating data services with web service technology is a recent concept. Standards such as WSO2 Data Services [5] are emerging for enabling data as a service. For example, the WSO2 Enterprise Service Bus enables the loose-coupling of services, connecting systems in a managed virtualized manner that allow administrators to control and direct communication without disrupting existing applications. WSO2 has many components, and the data server component essentially provides data services including mashups, such as data source integration, database management and related services.

Database management as a service is another emerging paradigm. Sharad Mehrotra and his team at the University of California at Irvine (UCI) together with researchers at IBM, Purdue and The University of Texas at Dallas (UTD) are working on this concept. The idea is to allow third party service providers to host an entire "database as a service," providing customers a seamless mechanism to create, store, and access their databases at the host site. Such a model alleviates the need for organizations to purchase expensive hardware and software, deal with software upgrades, and hire professionals for administrative and maintenance tasks, all of which are shifted to the service provider. The UCI team has developed and deployed a database service on the Internet, called NetDB2, which is in constant use. In a sense, data management models supported by NetDB2 provide an effective mechanism for organizations to purchase data management as a service, thereby freeing them to concentrate on their core businesses.

Software-as-a-Service (SaaS) is the progenitor of the various XaaS models [6], and has really exploded in recent years. In a SaaS architecture, software providers license their applications to customers for use on-demand. Vendors may host the application on their own web servers or allow consumers to download the application to local devices, disabling it on contract expiration. Licenses may be shared within an organization, or a third-party application service provider (ASP) may be utilized to share licenses between organizations. SaaS can also leverage service-oriented architectures (SOAs) for communication purposes. For example, each software service can act as a service provider, exposing its functionality to other applications in the SOA.

SOAs provide a lightweight means for enterprises to outsource their services to different parts of the organization or even different companies in different locations. The SOA bus can then compose the services for an application. Enterprises needing data for an operation can thereby invoke the data as a service model. Those needing a piece of software can invoke the software as a service. If a data management capability is required, a data management service is invoked.

When these various functions are outsourced, it is critical that the data not fall into the wrong hands. It is crucial that appropriate security strategies are implemented to ensure the confidentiality of the data and the privacy of the associated individual. Proper encryption of private data when it is stored or transmitted is an obvious strategy, but there are open challenges related to how to realize such encryption in an SOA. These include (1) avoiding prohibitively high computational overheads for the SOA due to encrypting or decrypting large data chunks even for small data requests, (2) inadvertently restricting access to metadata that is required for the SOA to locate data and distribute computation tasks efficiently, or (3) introducing the need for expensive, non-commodity hardware to support SOA-specific encryption strategies. Researchers at UTD, UCI and Purdue University are conducting research on querying encrypted data which will become an invaluable tool for data management services [7,8].

Other security issues include third party publication of data. Today many large documents are prepared and published by multiple parties, each of which are authorized to access only a subset of the information required to prepare the entire document. When publishing such documents, it is important that confidentiality of the sensitive information is maintained. In addition, the resulting document is itself subject to stringent integrity and confidentiality requirements—often there are different requirements for different portions of the document or user access patterns. Users who query the document should receive all parts of the document for which they have authorization, with high assurance that the received data has not been corrupted by an attacker. Researchers at the University of Milan, UTD and Purdue have developed schemes for secure third party publication of such documents [9]. In addition, with the emergence of cloud computing, it is now desirable to store data anywhere in the cloud. This also means that the data could be compromised. Therefore, secure storage strategies are critical for storing data on a cloud (e.g., [10]). Finally, the process of data outsourcing will be vulnerable to malware attacks. Therefore, detecting and preventing such attacks are crucial for the security of the outsourcing process. We address this in Section 5.

3. Mobile code security for data outsourcing

Many SOAs allow clients to efficiently access served data by also serving specialized applications that retrieve the data and render it for the user. These *mobile code* applets are essential for efficiently serving data to large numbers of clients because they allow service-providers to shift computational and communicational overhead from the provider to the recipient. However, when service-providers are not fully trusted, any mobile code they provide must be distrusted as well. This security concern is typically negotiated by imposing limits on the programs that clients are willing to accept. For example, mobile code expressed in type-safe bytecode languages, such as Java, .NET, or ActionScript bytecode, can be safely type-checked (i.e., validated) by a client-side virtual machine (VM) before execution.

A drawback of this approach to mobile code security is its inflexibility. Different organizations often have radically different security concerns and policies for remotely provided binary code, yet most VMs for standard bytecode languages enforce only baseline security policies,

such as memory and control-flow safety. Enforcing organization- and application-specific custom policies therefore typically requires development of a new VM or VM extensions—an impractical undertaking for many organizations. What is needed is a form of security as a service for mobile code, allowing code-recipients to shift the burden of enforcement to a trusted service provider.

Our current work examines *in-lined reference monitors* (IRMs) as a basis for realizing a security-as-a-service paradigm in web SOAs [11]. IRMs enforce custom policies by in-lining runtime security checks into the untrusted code itself. The resulting code is self-monitoring, allowing recipients to safely execute such code without any specialized, client-side monitoring. The instrumentation process that in-lines the security checks can be implemented by an external service that produces IRMs on-demand for clients in response to client-specified security policies. Recent work has even extended the technology to type-unsafe binary languages, such as x86 native code [12], affording service-providers even greater power and flexibility for offering their clients safe, practical, and efficient mobile code.

4. Supply chain security

One of the major applications of outsourcing is supply chain management. This concerns effective coordination of activities involved in subcontracting component development or services so that these activities are synchronized.

While traditional supply chain management examples typically involve acquisition and assembly of physical parts or materials, the increasing ubiquity of web services and distributed computing paradigms demand strong supply chain management techniques for software and data as well. For example, a company may want to custom-build an Enterprise Resource Planning application. It may get accounting software from one vendor, human resources software from another vendor, and order management software from a third vendor. These components must be received on time and with an adherence to various data integrity and interoperability standards so that they can be effectively integrated by the organization.

There are therefore numerous security challenges in supply chain management. Mitigations tend to fall into two distinct categories: *Fault tolerant* approaches ensure that the composite system is secure even if the individual parts may fail. These typically leverage high redundancy and diversity to cross-validate data and software behavior dynamically [13,14]. In contrast, *insider threat detection* takes the more direct approach of discovering and preventing attacks launched by malicious insiders in subcontracting organizations. These aim to deceive and misdirect malicious insiders in an attempt to frustrate their mission objectives. One of the greatest challenges in this approach, however, is to accurately distinguish behavior related to malicious insider objectives from legitimate activity even when insiders are highly knowledgeable about organization procedures and security controls. This remains an ongoing challenge in the field [15].

5. Data supply chain modeling for information sharing

We have examined supply chain modeling for data production in assured information sharing [16]. When data is outsourced, several organizations must share data but at the same time enforce various policies such as confidentiality, privacy, and trust. We believe that techniques from supply chain modeling may be used to securely share data under outsourcing conditions.

A data supply chain is the network of facilities and distribution options that perform the functions of the production of data, transforming the data into intermediary and finished data products, distributing the data products to customers, and sharing the data products among customers. Our work expands the definition of supply chain management to include a new step that shares the data among the customers who request the data from partners in the chain. This facilitates application of various types of decision-making to the information sharing problem in SOAs.

Location decision in a standard supply chain is the geographic placement of the production facilities and stocking points. In the electronic world, geographic placement is largely irrelevant, but there is a corresponding cyber-placement problem: From which data source should we request the data? Here, the location decision is driven by considerations related to the network topology, trade-offs between quality and quantity of service, and security guarantees provided by each service. Locations and production decisions together determine where to produce and what data to produce.

When there are multiple options, optimization theories may be used to determine the best options for the location and the substance. Inventories for data supply chain are the data sub-products in the production. These inventories need storage facilities. Push vs. pull approaches may also apply, as in the case of regular supply chain management. Should we pull the data (i.e. the inventory) when we need it or should the system push the data periodically? Transportation decisions determine how the data is moved from location to location (e.g., optimized routing). Furthermore, at each location the data may undergo transformation processes. For example, different pieces of data may be merged or data may be sanitized. Optimized routing algorithms as well as transformation algorithms may be applied here.

With respect to the modeling approaches, network design methods may be used to determine the location, stocking, and transfer of the data. Rough cut methods modularize the task by considering the policies on the data and the processes at each stage independent of the location or the distribution. Simulation methods help us analyze the data supply chain model.

With respect to information sharing for supply chain, a data supply chain is created mainly for the purpose of information sharing among the customers and service providers. The different parties are the partner organizations in the data outsourcing process. Thus, information sharing is needed to produce the data supply chain. The end product is data that may be shared among partner organizations. In addition to the data, we may need to share metadata for supply chain management. Sharing data and metadata for a data supply chain may have risks if confidential data is leaked to an adversary. Therefore, theories such as the Principal–Agent theory must be examined for data supply chains in the data outsourcing process [17].

6. Economics, incentives and risks

Information exchange among the partners occurs in many contexts during the outsourcing process. It has been considered in economics and in supply chains and has led to important scientific developments. In this context, one has a principal and an agent (or several agents), basically a supplier. They have different utility functions and they proceed with an economic exchange; for example, the agent is providing a part or a subsystem to the principal and receives a payment. However, the principal does not have accurate information on the agent, either as far as his capability to perform the commitment is concerned, or as far as his attitude is concerned (moral hazard). Incentives are a useful technique to get the agent behaving in the way the principal wants (or as close as possible to it). Of course the economic exchange is also linked to an information exchange, but the information is partial and possibly distorted. The principal can increase its efforts to acquire information from the agent, but that entails a cost which should be minimized.

Security issues occur in the information exchange. This is also a reason to limit the exchange. Information exchanges can be reduced when sufficient trust exists. The trust depends on the reputation of both entities—the principal and the agent. It is not just a problem for the principal. The agent may fear the behavior of the principal and be reluctant to provide complete information. In our research we are looking at organizational information sharing in general, and aim at extending the framework developed for economic exchange

or supply chain to benefit from the concepts and methods of the theory of incentives and contracts. Since the sharing of information must be considered in a specific context, where each of the entities wants to use the information with some objective in mind, we define utilities for each entity, which will be functions of the information acquired. It is important to introduce the enemy as a player who creates the risk and is interested in getting the information with fully hostile objectives [18].

Each of the friendly entities needs some part of the information to perform the task under its responsibility, like supplying a subsystem in the supply chain problem. Its utility will depend on the task it is supposed to perform. On the other hand, it may be affected by some risk arising from its partners and the risk that relevant information has been obtained by the enemy. The model will use network-type concepts and ideas, such as Bayesian networks, for providing a good framework to incorporate the probabilistic considerations. Specific nodes are the principal on the one hand and the enemy on the other hand. In the standard Bayesian network model, the objective is to compute the diffusion of probabilities to obtain the probability of a main event. Here we introduce the optimization of the utility for each entity. These utilities depend also on the incentives which are incorporated. One way to introduce incentives is to define for each of the players a label of quality, on which the trust is based.

Performing the task will modify the level of this label. This is similar to the approach which is used in credit management, in which a label of quality increases the chances of the obligor to obtain its credit. Of course in the context of data outsourcing among partners who are not entirely friendly, several links, which may be somewhat contradictory, enter into consideration. The principal is interested in the fact that the each entity performs the task under its responsibility, but sharing information creates a risk of damage. The level of quality, which can be considered as a level of trust, plays a role in fixing the right level. Utility functions, level of trust, and Bayesian networks will be some of the concepts and methods we are envisaging in designing an assured information sharing framework. We are designing a static model to fix the various elements, state variables, decision variables, propagation of uncertainties, and incentives. We will then study a dynamic configuration and try to obtain stable configurations.

An important issue is the measure of global risk. Our approach is to define a level of confidence for the fulfillment of the global task. In a dynamic model, the evolution of the system with time—in other words, its capacity of fulfilling its task in an assured manner—will influence the design at future times. Here again, the economic literature provides interesting ideas which can be used in the present context. The concept of value at risk, which is very popular in economics and provides a measure for the global risk, can be adapted. The definition of the utility functions is a key element of the approach. It is not easy to define natural utility functions as in economics, in a general context. We shall try to define first preference functions and with some scaling approach fit for analytic functions representing utilities. This fitting approach depends on the availability of data. Simulation is an approach to provide data in order to calibrate the functions.

7. Data security standards for outsourcing

One of the key technologies for data outsourcing is the notion of service orientation. As we have discussed in Section 2, both data- and software-as-a-service play major roles in outsourcing. Therefore, security for service-oriented systems including technologies such as WSDL (Web Services Description Language), XML (eXtensible Markup Language), SOAP (Synchronous Object Access Protocol) and UDDI (Universal Description Discovery and Integration) is key to data outsourcing. Here, a client wishes to use a particular outsourcing service and will use the UDDI to locate the service. The services will publish their services with UDDI in WSDL. The message is exchanged in XML using the SOAP protocols. XML encryption and XML signatures are two of the critical security standards for XML messaging. While XML encryption ensures confidentiality, an XML signature ensures authenticity of the messages. Other relevant security standards for data outsourcing with respect to service orientation include XACML (eXtensible Access Control Markup Language) and SAML (Security Assertions Markup Language). While SAML assertions are used for identification and authentication, XACML is used to access control authorization.

With respect to mobile code, the Open Handset Alliance, which is a consortium of over 80 corporations in the mobile phone space, is developing standards and software (e.g., Android) including security standards for mobile code. The developments with this alliance will have a major impact on the standards for mobile code security and for data outsourcing. Data standards such as XBRL (eXtensible Business Reporting Language) as well as various RFID standards are also being developed for supply chain management. A discussion of security standards for outsourcing is given in [19] where the author discusses standards for credit card data as well as those for representing and managing contracts.

8. Assured cloud computing for data outsourcing

National Security Agency Chief Information Officer Lonny Anderson has stated that the agency is focusing on a “cloud-centric” approach to information sharing with other agencies. With this approach, one can envisage agencies sharing data stored in multiple clouds. The same paradigm may be applied for sharing outsourced data where organizations that form a coalition share data on a private cloud. Each organization also publishes its policies. Appropriate policies are enforced during data sharing.

We have examined developments in grid and cloud computing and explored security issues. In particular, we explored secure virtualization, secure storage, secure data management and secure cloud monitoring. In addition, we also developed various policy engines based on XACML as well as semantic web technologies. One of our significant contributions is a secure cloud data manager that could be utilized as the engine for assured information sharing. We developed two types of cloud data managers, one based on semantic web data and the other based on relational data. Current frameworks do not scale for large RDF graphs and as a result do not address these challenges. Here, we developed a framework using Hadoop to store and retrieve large numbers of RDF triples by exploiting the cloud computing paradigm. We developed a scheme to store RDF data in a Hadoop Distributed File System. More than one Hadoop job may be needed to answer a query because a triple pattern in a query cannot take part in more than one join in a Hadoop job. To determine the jobs, we developed algorithms to generate a near optimal query plan based on a greedy approach to answer a SPARQL Protocol and RDF Query Language (SPARQL) query. We use Hadoop's MapReduce framework to answer the queries. We implemented XACML-based policy management and integrated it with our query processing strategies. For secure query processing for relational data, we utilized the HIVE framework. More details of our work can be found in [20].

9. Summary and direction

Globalization has resulted in outsourcing data, software, hardware, and various services. However, outsourcing results in increased security vulnerabilities due to the corporation's limited knowledge and control of employees working in foreign countries. Therefore, security of operation is critical for effective outsourcing.

This paper summarized various security challenges for outsourcing both the data management and software development activities. We also discussed security for supply chains, which is an application of outsourcing. The goal is to secure the composite system even if the components may be compromised. Querying encrypted data is also

needed when data is outsourced. One of the major contributions we have made in this paper is the notion of data supply chain management in assured information sharing. We argue that data production has many similarities to developing a product in the supply chain process, and data must be securely shared in the outsourcing process. In addition, security concerns for mobile code in service-oriented architectures motivate the realization of security itself as a service.

Much additional research is needed to determine the security needs for outsourcing. Collaboration between researchers and corporations that are outsourcing their services is essential for identifying and formalizing outsourcing requirements, including security requirements. Corporations should consider cooperation with organizations such as the International Association of Outsourcing Professionals (IAOP) to determine the best strategies for outsourcing so that the outsourcing country as well as the service-providing country can both benefit. For example, what sort of jobs should be outsourced? What are the implications for both countries as increasing numbers of jobs are outsourced? Most importantly, can the jobs be outsourced in a way that meets the data integrity, confidentiality, and mobile code security requirements of both parties? What should be the primary research agenda and scope of an outsourcing security research program? These are all questions that must be answered for successful and secure outsourcing.

Acknowledgments

This paper resulted from a panel discussion in which the second author participated on January 15, 2009 organized by the International Association of Outsourcing Professionals in Dallas, Texas. This material is based upon work supported by the Air Force Office of Scientific Research under Awards FA-9550-09-0468 and FA-9550-08-1-0044.

References

[1] Daniel Peng, Frank Dabek, Large-scale incremental processing using distributed transactions and notifications, Proc. USENIX Symposium on Operating Systems Design and Implementation, 2010.
[2] H.E. Schaffer, X as a service, cloud computing, and the need for good judgment, IT Professional 11 (5) (2009) 4–5.
[3] Bhavani Thuraisingham, Secure Semantic Service Oriented Information Systems, CRC Press, 2010.
[4] Dyan Machan, The new information goldmine, The Wall Street Journal (August 19 2009).
[5] Sumedha Rubasinghe, Ayanthi Anandagoda, WSO2 data services: an executive overview, Whitepaper (October 2008).
[6] Software & information industry association: software as a service: strategic backgrounder, Whitepaper (February 31 2001).
[7] Murat Kantarcioglu, Chris Clifton, Security issues in querying encrypted data, Proc. DBSec, 2005, pp. 325–337.
[8] Hakan Hacigümüs, Balakrishna R. Iyer, Sharad Mehrotra, Ensuring the integrity of encrypted databases in the database-as-a-service model, Proc. DBSec, 2003, pp. 61–74.
[9] Elisa Bertino, Barbara Carminati, Elena Ferrari, Bhavani M. Thuraisingham, Amar Gupta, Selective and authentic third-party distribution of XML documents, IEEE Transactions on Knowledge and Data Engineering 16 (10) (2004) 1263–1278.
[10] Kevin Hamlen, Murat Kantarcioglu, Latifur Khan, Bhavani Thuraisingham, Security issues for cloud computing, UTD technical report, UTDCS-02-10, February 2010.
[11] Micah Jones, Kevin W. Hamlen, A service-oriented approach to mobile code security, Proc. 8th International Conference on Mobile Web Information Systems, 2011, pp. 531–538.
[12] Kevin W. Hamlen, Vishwath Mohan, Richard Wartell, Reining in windows API abuses with in-lined reference monitors, UTD Technical Report, UTDCS-18-10, June 2010.
[13] Manghui Tu, Peng Li, I-Ling Yen, Bhavani M. Thuraisingham, Latifur Khan, Secure data objects replication in data grid, IEEE Transactions on Dependable and Secure Computing 7 (1) (2010) 50–64.
[14] Elisa Bertino, Gabriel Ghinita, Kevin Hamlen, Murat Kantarcioglu, Hsien-Hsin S. Lee, Ninghui Li, Calton Pu, Ravi Sandhu, Waleed Smari, Bhavani Thuraisingham, Gene Tsudik, Dongyan Xu, Shouhuai Xu, Securing the execution environment applications and data from multi-trusted components, UTD technical report, UTDCS-03-10, February 2010.
[15] Eugene Santos, Hien Nguyen, Fei Yu, Keumjoo Kim, Deqing Li, J.T. Wilkinson, A. Olson, R. Jacob, Intent-driven insider threat detection in intelligence analyses, Proc. IEEE/WIC/ACM International Conference on Web Intelligence and Intelligent Agent Technology, 2008, pp. 345–349.
[16] B. Thuraisingham, Data supply chain management: supply chain management for incentive and risk-based assured information sharing, UTD Technical Report, 2010.
[17] Priscilla R. Manatsa, Tim S. McLaren, Information Sharing In a Supply Chain, Using agency theory to guide the design of incentives, Supply Chain Forum 9 (1) (2008).
[18] Ryan Layfield, Murat Kantarcioglu, Bhavani M. Thuraisingham, Incentive and trust issues in assured information sharing, Proc. CollaborateCom, 2008, pp. 113–125.
[19] Carter Santos, Security standards for outsourcing, Law Technology News (May 2009).
[20] Kevin W. Hamlen, Murat Kantarcioglu, Latifur Khan, Bhavani Thuraisingham, Security issues for cloud computing, International Journal of Information Security and Privacy 4 (2) (2010) 39–51.

Kevin Hamlen is an Assistant Professor and head of the Software Security Lab in the Computer Science Department at the University of Texas at Dallas. His research on software security, malware defense, and cloud computing security has received numerous federal research awards, including Young Investigator and Career awards from the Air Force Office of Sponsored Research and the National Science Foundation. He received his Ph.D. in Computer Science from Cornell University and his B.S. in Computer Science and Mathematical Sciences from Carnegie Mellon University.

Bhavani Thuraisingham, a Louis A. Beecherl, Jr. Distinguished Professor, is the Executive Director of the Cyber Security Research and Education Center (CySREC) at The University of Texas at Dallas. She is an elected Fellow of several organizations, including the IEEE, AAAS, British Computer Society, and SDPS, with over 30 years experience in industry, MITRE, NSF, and academia. Her work has received numerous awards, including the IEEE Computer Society 1997 Technical Achievement and ACM SIGSAC 2010 Outstanding Contributions awards. She has published 100+ journal articles, 200+ conference papers, and 12 books. She has three US patents and has given over 90 keynote addresses.