Benefit and Cost of Cloud Computing Security

Wen Zeng and Vasileios Germanos

School of Computer Science and Informatics
De Montfort University, LE1 9BH, U.K.
wen.zeng.wz@gmail.com, vasileios.germanos@gmail.com

Abstract. Running information security technologies and policies in cloud computing systems will create negative impact to business organizations. Chief information security officers, as potential users, need a solution to analyze the cost and benefit of implementing information security technologies and policies in cloud computing systems. Petri nets can be used to analyze the workflow security in cloud computing systems, diagnose possible malicious behavior, and analyze invisible executions and failures in such systems.

Keywords: Petri nets · security · cloud computing · opacity.

1 Introduction

The importance of cloud computing is increasing due to the ever-increasing demand for internet services and communications. However, the large number of services and data stored in the clouds creates security risks due to the dynamic movement of data, connected devices, and users among various cloud environments. Information security technologies and policies are developed to keep the data and information secure in the systems. However, the implementation of these technologies and policies in cloud computing systems will create negative impact to the business organizations. For example, increasing the complexity of services in the system will increase the rate of failure. Therefore, it is important to evaluate the cost and benefit of implementing information security technologies and policies in cloud computing systems.

2 Cloud Computing Security

In 1995, Bill Gates wrote a memo entitled "The internet tidal wave" which described how the internet was going to forever change the landscape of computing [1]. He indicated that the rich foundation of the internet will unleash a services wave of applications available instantly over the internet to millions of users. Services designed to scale to hundreds of millions will change the nature and cost of software solutions. Now all his predictions became reality.

Cloud computing is a type of internet-based computing which provides shared computing resources and data to computers and other devices on demand.

Instead of building individual information technology infrastructures to host databases or software, a third party can host them in its large server clouds.

Cloud computing platforms are designed to automatically replicate data across a worldwide infrastructure. Therefore, the cloud providers can dynamically engage more resources, such as, servers and storage, as your site needs them. However, security is the most significant barrier to widespread adoption of cloud computing.

Firstly, although cloud computing services are relatively new, data breaches in all forms have existed for years [2]. Over 50 percent of the IT and security professionals believed their organization's security measures to protect data on cloud services are low [2]. Data breaching was three times more likely to occur for businesses that utilize the cloud than those that do not [2].

Secondly, the cloud's unprecedented storage capacity has allowed both hackers and authorized users to easily host and spread malware, illegal software, and other digital properties [2]. Consequently, this practice affects both the cloud service providers and their clients [2].

Thirdly, application programming interfaces give companies the ability to customize features of their cloud services to fit business needs; however, this practice can potentially leave exploitable security risks [2]. The vulnerability of application programming interfaces lies in the communication that takes place among applications [2]. A simple example is YouTube, where developers have the ability to integrate YouTube videos into their sites or applications [2].

3 Information Security Technologies and Policies

Information security technologies have been investigated and developed to keep the data and information secure in cloud computing systems.

Large IT companies, like Microsoft, IBM and Google, provide authentication technologies that only authorized users can access data resources and applications in the clouds. For example: Microsoft Azure develops Azure active directory to ensure that only authorized users can access clients' environments, data and applications [3]. IBM provides identity and access management capabilities designed to strengthen compliance management and reduce risk in today's cloud environments [4]. IBM Cloud lets users build authentication and authorization into users' cloud-native apps, and manage access to cloud resources [4]. Google Cloud Identity offers the identity services and endpoint administration that are available in G Suite as a stand-alone product [5].

Protocols are used to keep the data secure in the clouds. For example: Microsoft Azure uses industry standard protocols to encrypt data in transit. These secure users' data as their travel between devices and Microsoft datacenters [3]. IBM Cloud also provides encryption of data at rest and while data are moving across storage and data services, along with a key management service [4]. Google Cloud Platform, by default, encrypts customer data stored at rest, without requiring any additional action from its users [5].

Security analytics technologies are developed to monitor servers, networks and applications in order to detect and respond to threats in the clouds. For example: Microsoft Azure multipronged threat-management approach includes technologies and processes to constantly strengthen Azure's defenses and reduce risks [3]. IBM Cloud provides a main set of network segmentation and network security services to secure workloads from network threats [4]. IBM Cloud has built in features that allow users proactively monitor and gain security intelligence across users' hybrid cloud deployments [4]. Users, based on security analytics, can detect and respond to threats quicker, dramatically accelerate investigation times and proactively manage compliance [4]. Google Cloud Security Scanner is a web security scanner for common vulnerabilities in Google App Engine application, which can automatically scan and detect common vulnerabilities [5].

One would notice that cloud leading companies are focusing on security technologies, data and application security in cloud computing systems. The cost and benefit of executing these technologies and policies on cloud computing have not been analyzed. Digital Institute Newcastle proposed [6] cost models for multi-clouds systems, which considered the access control policies on the multi-clouds. However, trade-off between running access control policies and potential cost in the multi-clouds has not been considered. There are some cloud comparison website companies (e.g., CloudOrado.com) that provide the information about basic security policies/services/certifications of each cloud provider (e.g., encrypted storage, ISO/IEC 27001, and Firewall). However, the security and cost of workflow deployment in these multi-clouds, and security metrics of the workflow have not been considered.

In addition, there has not been an established systematic approach to quantitatively evaluate the project economics of information security technologies in cloud computing systems, including their effectiveness, benefits and costs to organizations, although information security researchers proposed various methods for addressing security investment problems. As a top security expert, Ross Anderson at Cambridge University pointed out security researchers should consider the costs of subsequent maintenance of the software. For example: security protocols failures may be explained by economics. Especially, the failures of large systems would cost industry billions.

4 Benefit and Cost Analysis

There are several different types of clouds which the clients can operate with depending on their business model. Public clouds are the most commonly used; their resources are made available to the general public by a particular provider, such as Microsoft, IBM or Google. On the other hand, private clouds are operated for a single organization, which can be managed either internally or by a third party, and can be hosted either internally or externally. Private clouds require a significant amount of engagement and re-evaluation of business strategy to be used effectively. However, large organizations may wish to keep sensitive

information on their more restricted servers, rather than in the public cloud. This has led to the introduction of federated cloud computing, in which both public and private cloud computing resources are used [6].

Information flow refers to paths followed by data from their original positions to the end users in computational processes [7]. Workflows are used to specify the implementation of such processes [7]. Information flow security in software engineering becomes an active topic, due to access control cannot control internal information propagation once accessed. Information flow security is to ensure that the information propagates throughout the execution environment will not leak sensitive information to public. The large number of services and data on a cloud system creates security risks, due to the dynamic movement of the services and data resources on the cloud systems [7].

In our study, we introduce security lattices for the components of a federated cloud system. Moreover, we assign security levels to individual services, data resources and clouds, and sign clearance level to individual services. We also assign clouds to individual services and data resources.

Then, we adopt the Bell-LaPadula multi-level control model into cloud computing systems [6]. A service can only operate at a security level that is less than or equal to its clearance [6, 7]. A service cannot read data that are at a higher security level than its own clearance [6, 7]. A service cannot write data residing at a lower security level [6, 7]. If an entity is located in a cloud, the security level of the cloud must be higher or equal to the security level of the services and data resources [6, 7].

4.1 Cloud Computing Trade-offs

After we adopt Bell-Lapadula multi-level control model into the systems, we will have different valid mapping options of services and data resources to clouds [6]. In some cases, the performance and cost of private and public clouds are different. The data size, the length of time the data are stored in the clouds also affect the cost of the different options. CPU consumed in the execution of the services in different clouds affects the cost of the systems. Furthermore, the complexity of services in the system will affect system failure rate.

There are two parts we need to consider for analyzing the benefit and cost of implementing information security technologies and policies in cloud computing systems: 1) The value or benefit that information security technologies or policies can bring to the organizations; 2) the cost and impact that information security technologies and policies have on organizations.

Benefit Information is treated as a business asset with varying levels of commercial values as introduced by [8]. Since it is usually difficult to measure the benefits of information security technologies directly, costs of information disclosure or modification are measured instead to quantify the benefits. Therefore, the organization's digital information assets should be evaluated and classified. Information should be classified into different categories by their level of confidentiality according to company policies. Then, they are assigned estimated

values to digital information of each category. This information valuation process should be based on the business needs of the organization [8].

For a cloud computing system, observing patterns of users' behaviour can lead to leakages of secure information. Information sharing means that the behaviour of one cloud user may appear visible to other cloud users or adversaries, and observations of such behaviour can potentially help them to build covert channels [9, 10]. We consider using opacity as a promising technique for analysing information flow security. Opacity has been proposed as a uniform approach for describing security properties of computing systems expressed as predicates [9, 10]. A predicate is opaque if an observer of the system is unable to determine the truth of the predicate in a given system run [9, 10].

In a cloud computing system, the security policy is the architecture with public/private clouds, yielding an observation function, and a predicate that needs to remain opaque [10]. The cost of information leakage is based on the assumption that there is a security policy and a competing cost of opacity. The cost of the security policy is the financial cost of setting up and using a particular architecture. The cost of opacity is the financial cost of leaking confidential information that should remain hidden. The security policies play a key role in determining the best design of the system. In addition, the security policies also influence the opacity of the systems.

Due to the complexity of cloud computing systems and data distribution on them, the risk of information loss is high. Cloud providers should be able to provide techniques for detecting potential invisible malicious events in the systems. These techniques can increase the dependability of their services, and consequently organizations will feel more confident to use them. Thus, invisible malicious events, which violate the proposed security policies in cloud computing systems, must be detected. Diagnosis is the procedure of detecting abnormal behaviours of a system. A notion of diagnosability [17, 18] - an associated property of diagnosis - can been used to detect such events in clouds.

Cost Cloud costs are measured using the metrics by which cloud providers allocate charges and impact of the allocated strategies [6], which are affected by information security technologies and policies. Some costs are tangible, for example, the capital expenditures on information security technologies and associated hardware, software and daily operational expenditures associated with maintenance. These tangible costs are readily to be accounted for in monetary terms. There are also some intangible costs. For example, it has been digital documented that implementing a strict security mechanism will reduce the efficiency of the organization [11]. One of the impacts of information security technologies on staff productivity is quantified in terms of non-productive time [11].

In our study, the tangible costs of a cloud computing system include: purchase of security technologies/policies and any associated costs to upgrade hardware and software, the cost of the data stored in the clouds, the cost of CUP consumed in the execution of services, and data transfer costs [6].

The intangible costs of a cloud computing system include: employee non-productive loss, administrator costs, and training employees.

Non-productive time [11] incurred as the result of the reduction in organization efficiency after the implementation of cloud computing security technologies and policies. The more services and security technologies are deployed on a system, the more complex the system will be. In general, increasing the complexity of services in the system will increase the rate of failure. System failure will affect the productivity of the organization. For many projects, this is a conservative estimate, because of high daily operational rates. For example, the daily rates of drilling rigs in oil and gas industry.

Administrators have to be hired to handle the cloud computing systems and the requests in the organization.

Cost of training and education of employees. It has been reported that most security incidents are caused by human errors instead of technology failures, although security incidents can result from nature disasters, technical issues and human acts. Therefore, the organization should provide information security training to employees.

5 Quantitative Evaluation Methodologies

We consider that Petri nets and the associated verification techniques can be used to analyze the cloud computing security.

Petri nets are a graphical modelling tool for a formal description of systems whose dynamics are characterized by concurrency, synchronization, mutual exclusion and conflict [12]. In particular, they have been widely used for structural modelling of workflows and have been applied in a wide range of qualitative and quantitative analysis [12, 13].

A basic Petri net consists of places, transitions, a set of arcs and the initial marking. Places represent possible states of the system, transitions are events or actions which cause the change of state, and every arc simply connects a place with a transition or a transition with a place. A change of state is denoted by consuming/producing tokens (black dots) from places to places, and is caused by the firing of a transition. The firing represents an occurrence of the event or an action taken. The firing is subject to the input conditions, denoted by token availability. A transition is firable or enabled when there are sufficient tokens in its input places. After firing, tokens will be consumed from the input places, and be produced to the output places. For example: in [7], Petri nets are introduced to diagnose the possible malicious behaviour in the cloud computing systems. In [9, 10], Petri nets are used to capture the invisible workflow in cloud computing systems.

Coloured Petri nets allow the modeler to use a number of different colour sets, making it possible to represent data values in a more intuitive way instead of having to encode all data into a single shared set [14]. Coloured Petri nets introduce a set of coloured tokens that can be distinguished from one another, unlike the indistinguishable black tokens in the basic Petri nets, and use arc

expressions to define how transitions can occur in different ways depending on the colours of input and output tokens. Coloured Petri nets can be used to capture the security policies in cloud computing systems. In [7], coloured Petri nets are used to capture the Bell-LaPadula rules and cloud security rules. The security policies for services migration and data migration can be captured by the functions associated with transitions.

Stochastic Petri nets are an extension of classic Petri nets [15], and Stochastic Activity Networks are a class of stochastic Petri nets [16]. One can associate a firing delay with each transition of a Petri net; such a delay specifies the time that the transition has to be enabled before it can actually fire. If the delays are given by a random distribution function, we obtain a stochastic Petri net. A stochastic Petri net model includes a set of ordered activities to be undertaken by humans or other resources of the organization or a system. A stochastic Petri net model is a structure for actions and implies on how work is done within an organization or a system. These actions are work activities across time and space, with a beginning and an ending. In [11], non-productive time associated with information security technologies are captured by the firing delay of the transitions, and the system failure rate can be captured by the probability associated with the transitions.

References

1. B., Gates.: The Internet Tidal Wave, http://www.lettersofnote.com/2011/07/internet-tidal-wave.html. Last accessed 1 Jun 2018
2. J., Ma.: Top 10 security concerns for cloud-based services, https://www.incapsula.com/blog/top-10-cloud-security-concerns.html. Last accessed 1 Jun 2018
3. Microsoft.: Microsoft Azure, https://www.microsoft.com/en-us/trustcenter/security/azure-security. Last accessed 1 Jun 2018
4. IBM.: Security in the IBM Cloud, https://www.ibm.com/cloud/security. Last accessed 1 Jun 2018
5. Google.: Trust & Security, https://cloud.google.com/security/. Last accessed 1 Jun 2018
6. Watson, P.: A Multi-Level Security Model for Partitioning Workflows Over Federated Clouds. Journal of Cloud Computing **1**(1), 15 (2012)
7. Zeng, W., Koutny, M., Watson, P., Germanos, V.: Formal Verification of Secure Information Flow in Cloud Computing. Journal of Information Security and Applications **27-28**, (2016)
8. Humphreys, E.: Information Security Risk Management. British Standards Institution, (2010)
9. Bryans, J., Koutny, M., Mazare, L., Ryan, P.: Opacity Generalised to Transition Systems. International Journal of Information Security **7**(6), 421–435, (2008)
10. Zeng, W., Koutny, M., Watson, P.: Opacity in Internet of Things with Cloud Computing. In: 8th IEEE International Conference on Service-Oriented Computing and Application, pp. 201–2017, Rome, Italy, (2015)
11. Zeng, W., van Moorsel, A.: Quantitative Evaluation of Enterprise DRM Technology. In: Electronic Notes in Theoretical Computer Science, (2011)
12. Murata, T.: Petri nets: Properties, analysis and applications. Proceedings of the IEEE **77**(4), 541–580 (1989)

13. v. d. Aalst, W.: The application of Petri Nets to Workflow Management. Journal of Circuits, Systems and Computers **8**(1) 21–66 (1998)
14. Jensen, K.: Coloured Petri Nets: Basic Concepts, Analysis Methods and Practical Use. 2 edn. Springer-Verlag Berlin Heidelberg (1996)
15. Marsan, M. A., Balbo, G., Conte G., Donatelli, S., Franceschinis, G.: Modelling with Generalized Stochastic Petri Nets. 1st edn. John Wiley & Sons, Inc., New York (1994)
16. Sander, W.: Construction and Solution of Performability Models Based On Stochastic Activity Networks. Ph.D. Thesis, The University of Michigan (1998)
17. Germanos, V., Haar, S., Khomenko, V., Schwoon, S.: Diagnosability under Weak Fairness. ACM Trans. Embed. Comput. Syst. **14**(4) 1–19 (2015)
18. Bérard, B., Haar, S., Schmitz, S., Schwoon, S.: The Complexity of Diagnosability and Opacity Verification for Petri Nets. In: van der Aalst, W., Best, E. Application and Theory of Petri Nets and Concurrency - 38th International Conference, PETRI NETS, vol. 10258, pp. 200-220. Springer (2017)