Towards Validating Cloud Service Providers Using Business Process Modelling and Simulation

Muthu Ramachandran, Victor Chang

School of Computing, Creative Technologies and Engineering, Leeds Beckett University, Leeds, UK

Abstract

Today's data is sensitive that requires privacy and security both from the cloud service providers (CSP) as well as from users in its all the form of data states: data at rest, while transferring data, enquiring data, and processing the data. Cloud computing has been applied in the health sector, national security services, banking and other business and companies that store confidential data into the cloud as we have seen in recent years. Therefore, information and data security is a crucial issue that needs to be addressed thoroughly in the cloud computing business. This research deals with the performance analysis of recent cloud data security models. This paper proposes cloud data security models based on Business Process Modeling Notations (BPMN) and simulation results can reveal performances issues related to data security as part of any organizations initiative on Business process management (BPM).

Keywords: Cloud service provider (CSP); Business process management (BPM); Business process modeling (BPMN); Cloud computing; Data security

Introduction

Cloud computing has become the influencing IT landscape and gained amplified attention in the virtual world (Opitz et al., 2012; Repschläger et al., 2012). The US spending on cloud computing for the last five years was estimated to grow at annual growth rate of 40% and was expected to reach $7 billion by the end of the year (Kaufman, 2009). It was reported that this speeding on cloud computing was expected to pass $95 billion in 2018 (Subashini and Kavitha, 2011). Moreover, it was estimated that 12% of the software market would shift towards the cloud (AlZain et al., 2013). But based on the current growth rate of the cloud business and the trend of software market, it looks like that the software market in the cloud has already surpassed 12%.

Among the variety of definitions of cloud computing, the most popular and commonly used definition that encapsulates the main constituents of cloud computing is the one by the National Institute of Standards and Technology (NIST) (Mell and Grance, 2011). Accordingly, cloud computing is an IT model for using on-demand, shared, measured and self adjustable computing resources, both software and hardware, conveniently via the Internet without the hassle of heavy management requirements and interaction between the client and the provider. There are five core components in the definition of cloud computing; network access, on-demand self-service, resource pooling, measured service and rapid elasticity (Rountree and Castrillo, 2014). NIST definition also includes generally three service models; IaaS (Infrastructure as a Service), PaaS (Platform as a Service) and SaaS (Software as a Service) and four deployment models (private, public, community and hybrid) of cloud computing.

With SaaS the user accesses software and applications through browsers or programming interfaces without direct control over the infrastructure. PaaS provides platform infrastructure such as operating system (OS)

where the user can run and configure software and applications but the user does not have control over the hardware. In IaaS, the user is provided with a hardware and network infrastructure where the user does not have physical access but can use for running OS and applications independently.

According to NIST, in private cloud deployment model the cloud service provider (CSP) provides one of the service models for an organization managed by the organization itself or by the CSP or by a third party. While the community deployment model provides cloud service to a certain classified group of users, the public model provides service to the general public. The fourth service model, the hybrid, is a combination of two or more of the previous deployment models.

The three functional components that the cloud computing model, be it the service or delivery, rotates around are cloud service provider (CSP), client also called owner and user (Sood, 2012). The CSP manages the cloud playing a significant role in providing storage space and computational resource. The client or the owner is individual or organization that rents or buys cloud-computing service for storing data and/or for computation. The user is the individual that utilizes the cloud service as a registered individual or registered through a customer organization.

Some of the advantages of adapting cloud computing include, but are not limited to, reducing initial capital expenditure (Creeger, 2009), minimal management (Pröhl et al., 2012), optimized resource utilization (elasticity) (Armbrust et al., 2010; Cusumano, 2010) and energy efficiency (Katz, 2009). Iyer and Henderson (2010) summarize a number of potentials of cloud computing: virtual business environment, controlled interfaces, ubiquitous access, location independence, rapid elasticity, sourcing independence, addressability and traceability. Hoberg et al. (2012) identified other aspects of cloud computing: increased scalability, increased agility, reduction of IT infrastructure complexity, cost reduction and improved alignment of business and IT.

However, cloud computing is not without a challenge. According to Armbrust et al. (2010) cloud computing has a number of challenges. Some of them are related to data such as lock-in, auditability, confidentiality and transfer problems. The rest include business continuity/availability, performance, unpredictability, storage scalability, bugs in big distributed systems and software licensing. Risks of adopting cloud computing as identified by Fogarty (2009) include compatibility, privacy and interoperability. Compatibility is related to the fact that data in one CSP may not be compatible in other CSP. The owner organization cannot control over the privacy of its data. Alzain et al. (2011) also identified the issue of privacy and security related to the risks on data integrity, data intrusion and service availability.

Most of the drawbacks of cloud computing as mentioned by most of the authors as discussed above and others are related to privacy and security of data. Today's data is sensitive that requires privacy and security both from the CSP side and from the user side at its state of rest, transfer and processing. Cloud computing is applied in the health sector, national security services, banking and other business and companies that store confidential data into the cloud (e.g. Flinders, 2014; Gill, 2013; Toxen, 2014). Therefore, information and data security is a crucial issue that needs to be addressed thoroughly in the cloud computing business. This research deals with the performance analysis of recent cloud data security models.

Background

To date cloud computing can be defined based on resource sharing (multi-tenancy), elasticity, scalability, self-provisioning and pay when you use (e.g. Mell and Grance, 2011; Winkler, 2011). One of the modern cloud computing features is its business model where same resource is shared between multiple users at network, host and application level. Elasticity refers to the fact that cloud users can change their computing needs and provide resources to others when they do not need them any more. The current technology in cloud

computing provides the customers to scale systems, bandwidth and storage size due to the scalability feature of cloud computing. Another important attribute in cloud computing is self-provisioned by the user for computing capacity, software and disc space and network. Most cloud computing service providers charge the users only for the time and resource used, this is referred as pay as use.

The most common cloud computing services have three delivery models (SaaS, PaaS and IaaS), four deployment models (private, public, community and hybrid), and several application domains (computing, storage, finance, web and many others.

According to IDC forecast in 2009, cloud computing services were estimated to grow annually at a rate of 27% with investment of 42 billion by 2012 compared to the traditional IT services estimated to grow at a rate of 5% annually (Mather et al., 2009). The fast growth of cloud computing is attributed to technological advancements in software such as browsers, processors, storage devices, virtualization technology, broadband Internet technology, servers, application programing interface (API) and others (Winkler, 2011). Currently, cloud computing services are on the tip of our finger accessed using PCs, smart phones, tablets, devices in refrigerators, cares and even smart watches.

Some of the main features that are driving the adoption of cloud computing are small initial investment and low running cost, reliability and sustainability, repeated pattern, resource elasticity, location independence, resources sharing at enormous scale, better automation, on-demand access, computational efficiency, and technology transparency (e.g. Mather et al., 2009; Winkler, 2011; Modi et al., 2013). To ensure better automation, reliability and efficiency, a cloud is designed based on repeating pattern. When a computing service is delivered by abstracting the technology through an interface, it makes the technology transparent. Transparency lowers the cost of the cloud provider that makes it beneficiary in terms of operation and competitiveness. On demand access and self-service enables the providers to deliver the cloud service to the customers with cost effectiveness and agility. All these features to be true, they need more abstraction, which brings more complexity. That is the trade-off of all the good features in cloud computing. Since complexity makes the attack surface wider, it makes security in cloud computing challenging.

Thus the growth of cloud computing is with barriers that include security, privacy, connectivity and open access, reliability, interoperability, independence from CSPs, economic value, IT governance and changes in IT organization. The cloud will not be efficient, reliable and cost-effective without reliable and fast network connectivity. A few minutes disruption of connection and lagging network may mean costly to the customer. Availability and reliability are interconnected in terms of security. The most useful features of cloud computing to be cost-effective and agile are connectivity and security. Security issue in the cloud mainly data security will be addressed in the next section.

Cloud computing particularly refers to transferring, manipulating, computing and storage of data via a network to an offsite computing infrastructure managed and maintained by a third party. The computing resources are configured to run applications simultaneously to multiple users or multiple tenants. Under such computing environment, CSP should be able to ensure the security of the client data through the security principles such as firewall, virtual private network (VPN) and user authentication, private and public keys, encryption and other security policies. Due to the concept of resource pooling with other clouds, the clients' data is available both to third party cloud and the cloud in use (Julisch and Hall, 2010). Thus, security is a critical component in cloud computing business to ensure data is available and access is permitted only to authorized users (Overby et al., 2006).

Security for Cloud Computing

Cloud security in general includes physical security, disaster recovery and infrastructure security at hypervisor/host and network level (Chang, 2015), platform security both at root and guest OS level,as well as software security that includes user security, data and information security and application security. Firewall, security monitoring, load balancer, BGP at hypervisor and network level secure the infrastructure. In addition to the security layers for the infrastructure, NoSQL, API, Message queues, storage and hardening is used to secure the cloud at the platform level. Identity and access management, system and network auditing are related to user security and monitoring. Encryption is the main security layer in the security architecture of SaaS (Chang et al., 2016).

Several issues and problems related to cloud security are reviewed and addressed (Daniel and Wilson, 2003; Dikaiakos et al., 2009; Subashini and Kavitha, 2011; AlZain et al,. 2013; Modi et al., 2013). Due to the outsourcing feature of cloud computing, architectural security issues are also other security concerns. Such issues include external attack from unauthorized person accessing critical client data and security breach from the provider (Sood, 2012). Thus, any security and privacy violation in the cloud can cause significant and expensive consequences to the provider and the client and to the cloud computing sector in general. Putting in position stricter governance and regulations as well as organized cloud security systems will increase the confidence of organizations and business owners to go for cloud computing.

Modi et al. (2013) classified cloud security issues as attacks, threats and Vulnerability. Attack from a cloud computing context is defined as the act of harming the cloud computing resources. Threat refers to an event that may potentially compromise the cloud resource or can be incidental and malicious to affect the cloud including failure to cloud data storage. Vulnerability in cloud security refers to the ambiguity that exists in the cloud security system that can lead an intruder to get access to the cloud system using sophisticated methods. The key and thoroughly listed security elements in the cloud as discussed by Subashini and Kavitha (2011) are network security, authentication and authorization, identity management and sign-on process, web application security, virtualization vulnerability, availability, backup, data security, data locality, data integrity, data segregation, data access, data confidentiality and data breaches. As indicated by the authors most of the cloud security elements are related to data security.

Network security is related to weak Internet traffic that can lead to leakage of sensitive information and data to malicious users while the data or information is in transit by sniffing to network packets. The network can be secured using SSL (Secure Socket Layer), TLS (Transport Layer Security) and data and information encryption. Strong network traffic can protect the cloud from network security problems such as IP spoofing, Man-In-The-Middle (MITM), port scanning, packet sniffing, port scanning and others. Security breaches associated with authentication and authorization is when a company's employee information is stored in Lightweight Directory Access Protocol (LDAP) servers instead of Active Directory and when user credentials are stored in CSP's database outside the corporate IT infrastructure or when the information and credentials of an employee remains active and in the cloud database after the employee has left the company. Sign-on process and identity management is an IT administration that handles the identification of users in a system by their country, network or IP address or organization to control access to the resources of an organization IT by putting established boundaries around the system. It can include creating, managing and removing user identities, control access using smart systems such as chipped cards to access a service and assigning roles. Mismanagement and misuse of identity and log-on process may lead to catastrophic security damages to the cloud and to the client.

A SaaS is provided using web applications running on a web browser. Security patches in the web application can cause vulnerability to software and applications provided by SaaS. Vulnerabilities related to web applications with security holes cannot be sufficiently addressed with network firewall, IDS and IPS. This is because web applications give way to new security dangers that do not need application level defence and

cannot be efficiently tackled at the network level (Subashini and Kavitha, 2011). Verizon reported on its data breach in 2008 that 59% of the security breach comes from hacking web applications, of which 39% from application or service layer, 23% from OS or platform, 18% from exploiting known vulnerability, 5% from exploiting unknown vulnerability and 5% from use of back door (Wade et al., 2008). A CSP must be available 24/7 to provide services to enterprises around the clock. This can be achieved by continuously changing the architecture at various levels (application, platform or infrastructure) to increase scalability and availability. However, denial of service attack and hardware or software failure happen in the cloud all the time. The other security listing by Subashini and Kavitha (2011) is backup. CSPs should provide backup service to all sensitive data to enable quick recovery at the time of disaster. To avoid unauthorized access to backed up data, the data must be encrypted. Backed up data can cause a potential security problem if it not properly handled, especially, at the time of deletion and when a customer stops its subscription to a cloud provider.

Network, data and information security in cloud computing are emerging sectors of IT. In the cloud it is known as Security as a Service (Linthicum, 2009; Stieninger and Nedbal, 2014). It is classified into features such as identification, authentication, authorization, privacy, integrity and durability (Winkler, 2011; Armbrust et al., 2010). It refers to protection of data, applications, platform, service and the infrastructure in general with a set of policies, technologies and controls. The state of data in the cloud can be generally classified as data in rest, data in use or data in motion. Data security should address most of the cloud computing security challenges (Ackermann, 2013) at all states of data. Although Cloud computing has a number of technical and economic benefits, security remains to be a major challenge in its adoption for both the service providers and customers (e.g. Mell and Grance, 2010; Mather et al., 2009).

Data Security

This section provides key issues associated with data security in the cloud as it is the main focus on this paper to apply big data analytics to study the performance of data security in the cloud.

Data security covers the majority of cloud security challenges in general from both architectural and technological points of view (Change and Ramachandran, 2016). Data security, as identifies by Oracle in 2012, are related to data tampering (unauthorized modification of data), eavesdropping and stealing (theft on personal data, such as credit cards), identity theft (falsifying personal identity), stealing passwords, unauthorized access to database, irresponsible system administration, poor user management, providing multiple services and application layers that makes managing cloud security complex. Despite its several advantages, cloud computing remains in greater challenge due to the uncertainty attributed to data, information, host and network security (Mather et al., 2009). This uncertainly makes cloud adopters to assume security, especially on data security, to be the primary concern with the cloud. Thus, one of the key factors hindering cloud adoption is related to storing and computing sensitive data in the cloud, especially in community, hybrid or public cloud. Data security concerns in the cloud are two fold; limited control of the data by the data owner due to the fact that data is not stored in the owners' premises, and multi-tenancy feature of the cloud increases the risk to sensitive data. Data security is mainly an issue when it is at rest or stored in the data storage, when data is in motion (transferring data to and from the cloud) and when data is in use. Data security concerns are mainly related to confidentiality, integrity and availability at its different states including data in computation or use.

Data at rest is data stored in a hard disk on user computers, servers and backup storage devices. If corporate data is stored in the cloud, its security risk is similar to data at other states as the owner is not in total control of this data. Winkler (2011) reported that there are two requirements for an organization to choose cloud storage to sensitive data; risk exposure is acceptable which varies depending on the delivery and the deployment model, make sure that CSP is a responsible guardian to your data by following industry standard best practices, uses security technology relevant to the type of data stored.

Data in motion is data that is in transfer between one storage to an other such as to and from organization storage and the cloud storage. Data is said to be in motion or in transit when the user uploads and downloads data to and from the cloud. Username and password that help to authenticate a user to a cloud service are considered as sensitive data in motion as it is not stored encrypted (Subashini and Kavitha, 2011; Winkler, 2011; Modi et al., 2013). The security concerns associated to data in motion is protecting it from data tampering, ensuring the confidentiality of the data and preventing the data being observed by third party while the data is in transit. Encrypting the data in motion is probably the only security technique for data in motion.

Data in use is data, which is actually being on the process of computing by the user in the cloud. It can be the data open for processing, generated from a model running in the cloud or intermediate data accessed by software as an input for computation and so on. There is no known security technique for data in use as it is not possible to encrypt such data. The only security for such data is to use the data in a secured environment such as using access control and firewall.

Sood (2012) summarizes the common data security techniques available in cloud computing and proposed a new data security design and analysed its performance. Prasad et al. (2011) provided a three-dimensional authentication technique where availability of data is provided by overcoming problems such as denial of service and data leakage. The proposed technique does not require encryption. As a result, if the username and password are compromised unauthorized user can easily access the data in the cloud.

Kamara and Lauter (2010) reported a security model that uses the concept of index encryption suitable for preserving integrity using cryptography. In this method, when data is transferred from the user system to the cloud or other systems, a master encryption key is generated to encrypt the data and a secret decryption key is stored on the receiver side to decrypt it for authorized user. The drawback of this method is the fact that searching encrypted data is complex and inefficient. An alternative symmetric searchable data encryption security model was proposed by Wang et al. (2010). However the drawback of using such encryption method in the cloud is that the user needs to have a prior knowledge about the encrypted data. In addition, it does not show any evidence about confidentiality, integrity and security attacks. In fact, the model is premature to be considered as suitable for securing the cloud. Popa et al. (2010) reported what is called cloud proof storage security model. This method uses encryption and other engineering tools to create an efficient and scalable security model that enables users to detect confidentiality, integrity, write serial ability and freshness and cloud misbehaviour.

Sood (2012) claimed a security technique that protects, authenticates and maintains the integrity of the data implemented using the best available methods. The proposed security design includes dividing the data into different sections, 128-bit SSL encryption, index builder, verification of the message owner and authentication of data user at two check points (by the owner and by the cloud).

In our approach, the method based on Business Process Modelling (BPMN) provides data security at two phases: (1) while the data is in motion (i.e. when transferred to the cloud) and at rest (i.e. when it is stored in the cloud) and (2) while accessing the data from the cloud. At the second phase the method provides accesses to the data for users if they pass all the security gates provided by the method as indicated above.

Business Process Modelling (BPM)

Business Process Modeling Notation (BPMN) has been effective to provide system design. It can be used in security engineering to calculate the required time and resources needed to gain back control when the Data Center has been compromised. Chang and Ramanchandran (2016) demonstrate the use of BPMN and have worked out 125 hours of data recovery and take back control from a compromised Data Center has been critical for all the service providers and users. They have performed large scale penetration testing to test

robustness of their security system and service. Similarly, BPMN can be used to provide resilient system and software design for security before the actual implementation. BPMN can also be used to work out the business processes which can be suited for each organisations. To demonstrate how BPMN can be used effectively for Cloud security, Bonita Soft BPM can be used to conduct virtual simulation experiments. Bonita is a software environment for business process management (BPM) modelling and simulation software development process.

BPMN is used to simulate data security models of three-cloud service providers (CSP) (CSP-1, CSP-2 and CSP-3). The three cloud service providers are selected for this work because it was possible to get their data security design partially from the provider and partially by subscribing for their cloud service and understanding how data security is handled in these CSPs. Information from CSP-2 is disclosed since they do not disseminate their information for academic publishing. After accepting ethical approval and agreement from the other two cloud service providers, both will remain anonymous as **CSP-1 and CSP-3** for the rest of the text in this paper.

Cloud Service Provider 1 (CSP-1) Review by BPMN

CSP-1 claims that it delivers secure and high level services such as infrastructure, computing, storage, networking, database services. CSP-1 believes information security is vital and it is a fundamental requirement of the service in order to protect confidential and critical information from intentional and unintentional deletion, leakage, compromised data integrity and theft. The cloud data security model of CSP-1 is based on a shared responsibility between the provider and the client. CSP-1 customers are responsible for protecting the confidentiality, integrity and availability of their data in the cloud and need to meet certain requirements for information protections as signed in the SLA. The document in the SLA includes best practices (but not how to), that can help a client to leverage and apply Information Security Management Systems (ISMS) that describes a couple of cloud security strategies and procedures for the data in CSP-1 that belongs to the customer.

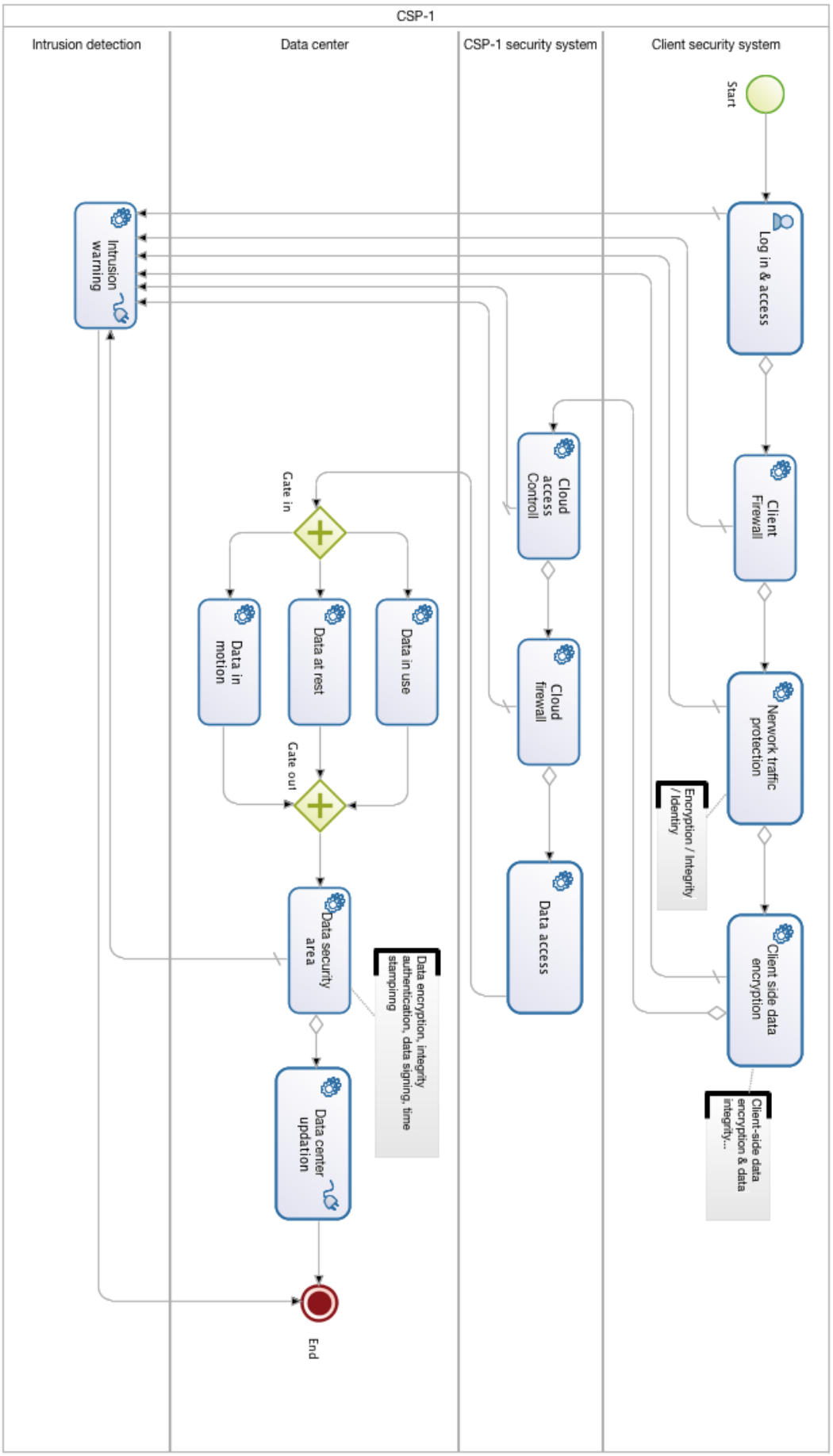

Figure 1: CSP-1 data security model as modelled in Bonita.

In the shared responsibility security feature of CSP-1, the majority of the responsibility to secure the data in CSP-1 falls to the client as shown in Figure 1 on client security system lane. The service provider allows the customer to design its security model using CSP-1's security architecture and features as a foundation. The main responsibility of this provider is to secure the infrastructure and services. It provides security of facilities, hardware, network infrastructure and virtualization infrastructure. For instance, it is the responsibility of the customer to secure the cloud provider's machine images, operating systems, applications and data, credentials and configurations and others. For CSP-1 storage services, the customer has full responsibility for the data security and setup its own firewall rules and access control to access the services.

As shown in **Figure 1** CSP-1 uses Identity and Access Management (IAM) in its security model to manage users, credentials (password, access keys and permissions for a particular services in the cloud). A user who has access to the client system can sign up for CSP-1 to create an account with a user name and password. This user must first login to the client system (*log in and access* in the client security system) and pass through a series of securities (client firewall, network traffic protection and client side data encryption) before entering to the cloud access control. In the cloud access control, the user can use the cloud user name and password to access the cloud and to use its resources using a browser-based management console. The client can also create access key for each user to allow the users access CSP-1 on a command line interface. Thus, the client can create CSP-1 accounts using IAM for each user with separate user name, password and access keys. This lets the users to log into the cloud console through a specific URL assigned to each account.

Once the user is in the cloud passing through the cloud access control (cloud security system in **Figure 1**), it is possible to access the data but for read and write access the user should pass through extra security checks such as using encryption key to encrypt the data for transfer and store and decrypt to use it. The data center and intrusion detection sections are the same for all models and it is discussed elsewhere in this chapter.

A new CSP-1 instance can be started and accessed through secure remote system access protocols, like secure shell (SSH) or remote desktop protocol (RDP). Before accessing and configuring the instance remotely, it has to be authenticated at platform level and then authentication mechanisms can be setup. For authentication, CSP-1 provides industry standard RSA asymmetric key pairs (private and public keys) in which each user can have multiple key pairs to start new instances with different key pairs. The public and private keys can be generated in a secure environment by the user using standard tools such as OpenSSL. It is the responsibility of the client to generate and manage the keys, especially the private keys. But the keys can be generated in the cloud environment by the CSP-1 and provided to the user when first an instance is created. In such a case the keys must be downloaded and saved by the user. If the keys are lost, they must be regenerated by the user. These key pairs are not associated to the cloud or client user credentials but are used to allow the user to a particular instance. In the model these are included and modeled with in the access control (**Figure 1**).

In the shared security responsibility agreement, CSP-1 provides data backup and recovery tools but the client must use the right tools and configuration for disaster recovery policy.

CSP-3 Data Security Model

CSP-3 security strategy offers security at several stages of data storage, access and transfer using its corporate security policies, company structural security, data management, access control, personnel security, physical and environmental and infrastructure security, systems and software development and maintenance and disaster recovery and business continuity. In this subsection, the security entities that are relevant to data security of CSP-3 as shown in **Figure 2** are discussed.

Generally, security in CSP-3 includes several topics covering security policies that apply to every employ at different security levels to comply with accounts, data and physical security and policies that employs need to follow when using integral applications and systems. CSP-3 personnel dealing with client data need to comply with company policies on the proper use of data related to business processes and outcomes of violating the code of conduct. Security policies are revised at a regular time interval and employees are given routine and formal training on security. The security system in CSP-3 is organized into several security teams, such as physical security, data security, information security, personnel security and so on, each of which have team of staff to handle security issues in their respective departments. CSP-3 customer and end user data assets and information are governed by these security policies and methods.

Each customer's data, structured or unstructured, in CSP-3 are distributed over a shared homogeneous multiple hardware. CSP-3 data storage requires authentication and authorization to be accessed by other components. Service to service authentication is based on a security procedure which depends on authentication infrastructure. As illustrated on the CSP-3 security model on cloud security lane on **Figure 2**, a user logged into the cloud domain has to login again for the cloud service. Once logged in for a cloud service a user can make user authenticated data request via an application front-end. The same front-end application makes a virtual system call to application back-end to process the request. The back-end authenticates the system call only if the caller is from authenticated user front-end application. If the caller is authorized, the application back-end makes a system call to the storage layer to get the requested data. The request is then authenticated and authenticated by the storage layer and the request is processed if the requester back-end is from authenticated and authorized back-end to access the requested data in the data store.

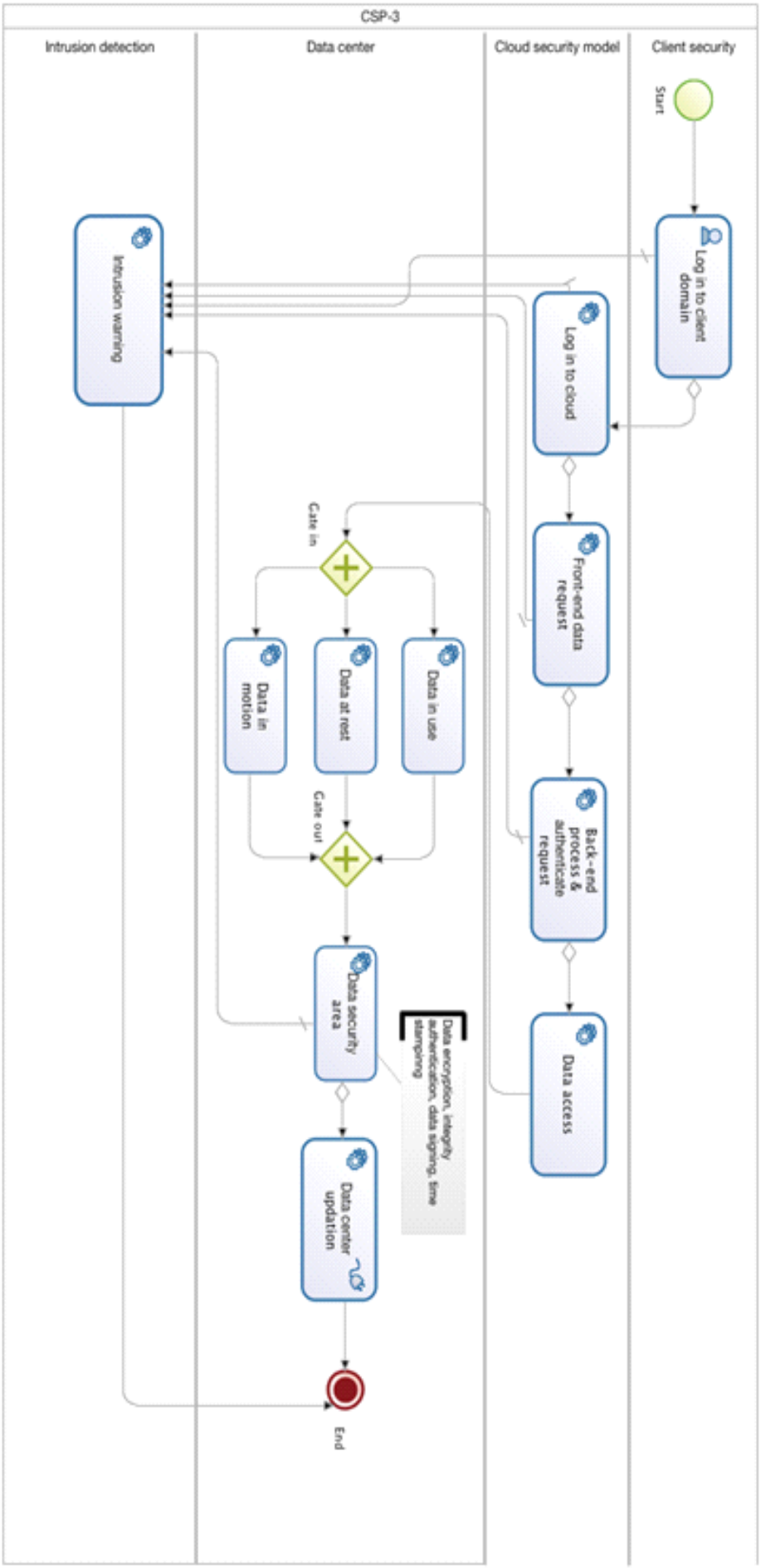
CSP-3
Intrusion detection
Data center
Cloud security model
Client security
Start
Log in to client domain
Intrusion warning
Log in to cloud
Front-end data request
Gate in
Data in motion
Data at rest
Data in use
Gate out
Back-end process & authenticate request
Data security area
Data encryption, integrity authentication, data signing, time stamping
Data access
Data center updation
End

Figure 2: CSP-3 data security model.

CSP-3 data is protected against unauthorized access using a number of access controls (authentication and authorization) that are implemented to the security system. One of these access controls is using a unique user ID and password. The user ID helps CSP-3 to supervise users activity on the cloud, such as activity on the cloud network, access to the cloud or customer data and information. Password and passphrases that are required to be change periodically are used for authenticating a user to access application front-end. The cloud system enforces users to change passwords and passphrases during expiration, restrict on their reuse and follow certain rules on creating them to ensure their strength. CSP-3 uses two-step authentication techniques, including certificates and password generators. Two-step authentication is needed for access to the cloud service, resources and on using third party application that use the cloud App.

Authorization control is based on the role of the user in the cloud or in the client. To get additional access right to a data, a user must request additional authentication for access approved by a data system owner, manager or executives.

BPMN Simulations for Security

This section discusses about the simulation of cloud data security models using BPMN. BPMN is a graphical language used to define processes and identify process requirements and specifications to evaluate the performance of a system. Simulating a process helps to understand business performance for expected and unexpected external events in that process. Thus, using BPMN simulation in cloud security models helps to evaluate the behavior and performance of different processes and tasks in the model for both expected and unexpected scenarios (Chang and Ramachandran 2016; Chang et al., 2016). As discussed in Section 2, the reason why BPMN is selected for simulating the security models is that it can provide the execution time of securing and protecting the data center. In addition, another important point worth mentioning about business process modeling (BPM) is that it helps to identify business process that potentially have influence to the system in general and on stakeholders in particular. It allows business analysts to prioritize the most critical business processes.

As discussed in the previous sections, all cloud data security architectural models have the following stakeholders:

- The client (customer using cloud service) who has registered users of the cloud
- The cloud service provider that has sections such as
    - Cloud security system/cloud management team
    - Data center and security pool
    - Attack detection and intrusion rejection process

The cloud computing client can have computers and applications designed particularly to access and use the cloud computing services. Such computers give interface for the user via web browsers and terminals. CSP is the party that provides cloud services using service delivery models via the Internet.

How BPMN can be useful for enterprise security

This section explains how the use of BPMN can be useful and contributing to security for businesses. In this paper, the user accesses the cloud data storage service by logging into the client domain and using the cloud credentials provided by the client. CSP-1 and CSP-3 security models are classed in this type. In the first case,

once the request is sent to the cloud, it passes through a number of management and security checks. In the second case, there is no sending for data request but there is only logging into the client system and access the cloud using the client credentials. Once the data request in the first case or the user in the second case is in the cloud system, it goes through a number of security checks including the cloud management team in the cloud security system, security pools in the data center. If the request or a credential does not pass one of the security layers in any of the cloud data security system, it passes to attack detection and intrusion rejection system.

The data center is an important part of CSPs, especially those providing Storage as a Service. The data center is connected to servers, data storage services and all applications in the cloud. The efficiency of cloud business depends on the data center, its supports and operations. Since the data center plays a vital role in the cloud business, it is important to make sure it is managed efficiently, its service carefully planned to meet the ever growing performance and application requirements. The data center in all the security architectures starts with a decision on the status of data (in use, in motion and at rest). Once the user passes through the status gate, he/she is put to the data, which is at one state. Before fully revealing the data and going to the data access end, it has to pass through the security pool, which can include encryption and data center update).

The intrusion detection part alarms the cloud security team, data centers and clients and/or users about the intrusion. If any intrusion attempts occur, the system should be set to compose and send email to respective parties.

In all security architectures to be analyzed, the key components in the cloud computing architecture that are relevant to this work include cloud clients, users, CSP (Security management team, data state, security pool and data updating in the data center and intrusion detection) and intruders where intrusion detection process needs to be carried out. Processes that need to be simulated using BPMN briefly include:

1. The *user* who can also be staff member of a client is sending a request message to the CSP through the client Internet domain or outside. In Bonita BPMN, this is an actor that starts the simulation process by sending a message of data request to either directly to the cloud or via the client system that takes action on the request and sends the request message to the cloud on the behalf of the user. An actor in Bonita is a placeholder for the user who performs tasks in a process.

2. The data request message entering into the *cloud* system passes through a number of security checks depending on the security model of that particular cloud provider. e.g.

    - The sender's identity is checked by access control mechanism and firewall. The identity management is enforced to ensure that right level of access is only granted to the right person.

    - Intrusion identification and rejection process takes place by detecting attacks, intrusion and penetration by providing up-to-date technologies to prevent attacks such as DoS, anti-spoofing, port scanning, known vulnerabilities, pattern-based attacks, parameter tampering, cross site scripting, SQL injection and cookie poisoning.

    - It passes through the encryption process. Encryption screens and offers early warning as soon as the behavior of the entity behaves abnormally.

    - Updates the status on the data access at the data center.

    - If intrusion occurs in any of the layers a message should be sent to screening for identifying which security attack it was and a warning message is sent to the CSP and to the client and/user as quickly as possible.

3. At the cloud *data center*, the data in all the selected security models passes through data status and other security pools. In this case the detailed steps are as follows:

   - The data passes through data status decision that allows the simulation process to go through different states depending on the state of the data in the cloud (in use, at rest or in motion).
   - The data has to pass through other securities that are separate actions in the data center with dedicated security processes (data security area and data centre update) that helps to study security controls in place before it ends.
   - Finally the data access is updated depending on the identity of the actor who initiated the process.

4. Another lane of the security models is the intrusion detection part. This section requires the attention of three lanes in the simulation process; the cloud provider security lane, the data centre lane and the client security lane. If any security suspicion is detected in any one of the tasks in the three lanes it raises security alarm and warns both parties as quickly as possible.

Discussion

In summary, BPMN can be useful for businesses as follows. First, they can understand the problems caused by security breach, identify which section of the security service under attack and the time to recover the data in order to resume services back to normal. Second, it provides the incentives for security design and allows the organization to review their current security service, identify limitations imposed by system design and evaluate the proposed areas of improvements. Examples of two service providers in this paper illustrate that BPMN can be effective solution for security design and ensures data security in place.

Security is a complex area that involves with different aspects such as encryption, firewall, access control, identity management, authentication and authorization, data center management and intrusion detection. Different techniques and recommendations are required to ensure a delivery of robust and reliable service that can withstand attacks such as SQL injection, denial of service, viruses and trojans, anti-spoofing, port scanning, cross site scripting, phishing and unauthorized access. Hence a complete and comprehensive approach to integrate different security services is required to allow all the users can be protected against hacking and unauthorized access. One such an approach is by the use of a framework that not only includes the recommendation for security guidelines, training and best practices, but it also includes the security solutions for each key aspect of security as mentioned above. For example, the security demonstration by Cloud Computing Adoption Framework (CCAF) can provide multi-layered and multi-purposed security service. It includes the integration of three major security solution that can can minimize the attacks, as demonstrated by large scale penetration testing and ethical hacking. The use of NoSQL databases can be the least affected by the large scale SQL injection performed by the ethical hacking (Chang et al., 2016). Thus, the use of a framework approach is relevant to the enterprises since their services and all types of data need to be safely protected. The use of BPMN can be further integrated into CCAF Version 2, whereby the BPMN can be used at any time to diagnose the security design and evaluate the performance at any time. The BPMN can simulate the time, the impacts and the weakest links (thus, the likely points of attacks) and report the the system manager the time required to recover the data, rescue services and points to defend attacks when the services are under the unauthorized attacks. BPMN can be fully integrated with CCAF Version 2 to provide a more reliable, resilient and stable security service for enterprises.

Conclusion and Future Work

This paper starts with the general literature in Cloud and data security and evaluates the current practices. The use of BPMN has been explained as the service to provide data security and security design. There are two CSP

examples given in this paper and details of their security design has been presented. Supported by the rationale of the design, all the data can be kept safe. In the event of the security breach, the use of BPMN can identify which sections of the security service under the attack and thus can save time and resources to perform the recovery actions. BPMN can be effectively used to support data security as illustrated by examples of the two service providers. The future work will include the large scale simulations and performance evaluation of the BPMN for these two service providers. Additionally, new security services will be designed to demonstrated a higher level of security that can achieve a good performance to diagnose the problems, perform quarantine actions for infected files and isolate those infected files out of the security services. BPMN will be fully integrated with CCAF Version 2 to provide businesses a more reliable and resilient security service.

References

Ackermann, T. (2013) *IT Security Risk Management: Perceived IT Security Risks in the Context of Cloud Computing.* Springer Gabler.

Aguilar-Saven, R. S. (2004) *Business process modelling: Review and framework.* International Journal of production economics 90, 129 – 149.

Alzain, M. A., Pardede, E., Soh, B. and Thom, J. A. (2011) *Cloud Computing security: From single to multi-clouds.* In Proceedings of the HICSS, 5490 – 5499.

AlZain, M. A., Soh, B and Pardede, E. (2013) *A Survey on Data Security Issues in Cloud Computing: From Single to Multi-Clouds.* Journal Of Software 8, 1068 – 1078.

April, J., Better, M., Glover, F., Kelly, J. P. and Laguna, M. (2005) *Enhancing business process management with simulation optimization.* Available from: <http://beta.bptrends.com/publications/> [Accessed December 12, 2014].

Armbrust, M., Stoica, I., Zaharia, M., Fox, A., Griffith, R., Joseph, A. D., et al. (2010) *A view of cloud computing*. Communications of the ACM 53, 50 – 58.

Bennett, M. (2014) *eBay: How not to handle a security breach.* Available from: <http://www.theinquirer.net/inquirer/opinion/> [Accessed 26 May 2014].

BonitaSoft (2014) *Documentation*. Available from: <http://documentation.bonitasoft.com/> [Accessed 24 May 2014]

BOS (2011) *Bonita Open Solution 5.5 Simulation Guide*. Available from: < http://www.bonitasoft.com/system/files/> [Accessed on October 29, 2014].

Brunette, G., Mogull, R. (2009) *Security Guidance for Critical Areas of Focus in Cloud Computing* V2.1, Prepared by the Cloud Security Alliance.

Chang, V. (2015). Towards a Big Data system disaster recovery in a Private Cloud. Ad Hoc Networks, 35, 65-82.

Chang, V. and Ramachandran,R. (2016) *Towards Cloud Data Security proposed and demonstrated by Cloud Computing Adoption Framework.* IEEE Transactions on Service Computing, 9(1), 138-151.

Chang, V., Kuo, Y. H., & Ramachandran, M. (2016). Cloud computing adoption framework: A security framework for business clouds. Future Generation Computer Systems, 57, 24-41.

Clark, M., Enstone, L. (2006) *L-SIM: simulating BPMN diagrams with a purpose built.* Proceedings of the Winter Simulation Conference 2006, Monterey CA, 591 – 597.

Cousins, J., Stewart, T. (2002) *What is Business Process Design and Why Should I care?* Rivcom LTD Whitepaper.

Creeger, M. (2009) *CTO roundtable.* Communications of the ACM 52, 50.

Cusumano, M. (2010) *Cloud computing and SaaS as new computing platforms*. Communications of the ACM 53, 27 – 29.

Daniel, E. M. and Wilson, H. N. (2003) *The role of dynamic capabilities in e-business transformation.* European Journal of Information Systems 4, 282 – 296.

Davenport, T. H. and Short, J. E. (1990) *The New Industrial Engineering: Information technology and business process redesign*. Center for Information Systems Research, Massachusetts Institute of Technology, June 1990. Available from: <http://dspace.mit.edu/bitstream/ handle/>. [Accessed 25 December 2014].

Dikaiakos, M. D., Katsaros, D., Pallis, G., Vakali, A. and Mehra, P. (2009) *Cloud computing*. IEEE Internet Computing 12, 10 – 13.

DoD 5220.22-M (2006). *National Industrial Security Program Operating Manual*. United States Department of Defense.

Flinders, K. (2014) *Banks could lower costs with cloud computing, but there are risks too.* Available from: <http://www.computerweekly.com> [Accessed 25 May 2014].

Fogarty, K. (2009) *Cloud Computing definitions and solutions*. Available from: <http://www.cio.com/article/print/501814> [Accessed 25 May 2014].

Gill, P. S. (2013) Cloud Computing and Enterprise Systems: Applications in the Auto Industry. The International Journal of Technology, Knowledge, and Society 9, 1832 – 3669.

Hoberg, P., Wollersheim, J. and Krcmar, H. (2012) *The business perspective on Cloud Computing: A literature review of research on Cloud Computing.* In Proceedings of the AMCIS.

Hubr, V. (2011) *Interaction, Simulation, Optimization and Monitoring of Processes in Emergency Management [Master's Thesis]*. Masaryk University.

Iyer, B. and Henderson, J. C. (2010) *Preparing for the future – understanding the seven capabilities of Cloud Computing*. MIS Quarterly Executive, 117 – 131.

Julisch, K. and Hall, M. (2010) *Security and control in the cloud.* Information Security Journal: A Global Perspective 19, 299 – 309.

Kamara, S., Lauter, K. (2010) *Cryptographic cloud storage.* Lecture Notes in Computer Science 6054, 136 – 149.

Katz, R. (2009) *Tech titans building boom*. IEEE Spectrum, 40–54.

Kaufman, L. M. (2009) Data *security in the world of cloud computing.* IEEE Security and Privacy 7, 61 – 64.

Lawrence, P. (1997) *Workflow Handbook: Workflow Management Coalition*. John Wiley and Sons.

Linthicum, D. (2009) *Defining the Cloud Computing framework: Refining the concept.* Available from: <http://cloudcomputing.sys-con.com/node/811519> [Accessed 23 May 2014].

Mather, T., Kumaraswamy, S. and Latif, S. (2009). *Cloud Security and Privacy*. O'Reilly Media, Inc.

Mathew, B., Mansharamani, R. (2012) *Simulating Business Processes – A Review of Tools and Techniques.* International Journal of Modelling and Optimization 2, 417 – 421.

Mell, P. and Grance, T. (2011) *The NIST definition of Cloud Computing*. NIST Special Publication 800 – 145.

Modi, C., Patel, D., Borisaniya, B., Patel, A., Rajarajan, M. (2013) *A survey on security issues and solutions at different layers of Cloud computing.* Journal of Supercomputing 63, 561– 592.

Opitz, N., Langkau, T. F., Schmidt, N. H., and Kolbe, L. M. (2012) *Technology acceptance of Cloud Computing: Empirical evidence from German IT Departments.* In Proceedings of the HICSS, 1593 – 1602.

Overby, E., Bharadwaj, A. and Sambamurthy, V. (2006) *Enterprise agility and the enabling role of information technology.* European Journal of Information Systems 15, 120 – 31.

Popa, R. A., lorch, J. R., Molnar, D., Wang, H. J. and Zhuang, L. (2010) *Enabling security in cloud storage SLAs with cloud proof*. Technical report. Microsoft Research.

Prasad, P., Ojha, B., Shahi, R. R.and Lal, R. (2011) *3-dimensional security in cloud computing.* Computer Research and Development (ICCRD) 3, 198 – 208.

Pröhl, T., Repschläger, J., Erek, K. and Zarnekow, R. (2012) *IT- Service management in Cloud Computing*. HMD—Praxis der Wirtschaftsinformatik 6 – 14.

Repschläger, J., Wind, S., Zarnekow, R., and Turowski, K. (2012) *A reference guide to Cloud Computing dimensions: Infrastructure as a service classification framework*. In Proceedings of the HICSS, pp. 2178 – 2188.

Rich (2011) *Data Security Lifecycle 2.0 and the Cloud: Locations and Access*. Avialable from: <https://securosis.com/blog/> [Accessed December 11, 2014].

Rountree, D. and Castrillo, I. (2014) *The Basics of Cloud Computing: Understanding the Fundamentals of Cloud Computing in Theory and Practice.* 1st Ed. Elsevier Inc.

Schneier, B. (2010) Available from: <http://www.schneier.com/blog/archives/> [Accessed 20 December 2014].

Smaizys, A., Vasilecas, O. (2009) *Business Rules Based Agile ERP Systems Development.* Informatica 20, 439 – 460.

Sood, S. K. (2012) *A combined approach to ensure data security in cloud computing.* Journal of Network and Computer Applications 35, 1831 – 1838.

Stieninger, M. and Nedbal, D. (2014) Characteristics of Cloud Computing in the Business Context: A Systematic Literature Review. Global Journal of Flexible Systems Management 15, 59 – 68.

Subashini, S. and Kavitha V. (2011) *A survey on security issues in service delivery models of cloud computing.* Journal of Network and Computer Applications 34, 1–11.

Subashini, S. and Kavitha, V. (2011) *A survey on security issues in service delivery models of cloud computing*, Journal of Network and Computer Applications, 1-11.

Toxen, b. (2014) *The NSA and Snowden: Securing the All-Seeing Eye.* Communications of the ACM 57, 41 – 55.

van der Aalst, W. M., ter Hofstede, A., and Weske, M. (2003) *Business process management: A survey.* Available from: <http://citeseerx.ist.psu.edu/viewdoc/> [Accessed December 25 2014]

Vasilecas, O., Smaizys, A., Rima, A. (2013) *Business Process Modelling and Simulation: Hybrid Method for Concurrency Aspect Modelling*. Baltic Journal of Modern Computing 1, 228 – 243.

Wade, H.B., Hylender C. D., Valentine J. A. (2008) *Verizon Business 2008 data breach investigation report.* Available from: </http://www.verizonbusiness.com/resources/> [accessed March 20 2014].

Wang, C., Cao, N., Li, J., Ren, K. and Lou, W. (2010) *Secure ranked keyword search over encrypted cloud data.* Journal of the ACM 43, 431 – 73.

White, S. A. (2011) *Introduction to BPMN, IBM Corporation*. Available from: <http://www.zurich.ibm.com/> [accessed December 25 2014].

Winkler, V.J.R. (2011) Securing *the Cloud: Cloud Computer Security Techniques and Tactics.* Elsevier Inc.