Journal of Information Security, 2015, 6, 12-23
Published Online January 2015 in SciRes. http://www.scirp.org/journal/jis
http://dx.doi.org/10.4236/jis.2015.61002

Control Framework for Secure Cloud Computing

Harshit Srivastava[1], Sathish Alampalayam Kumar[2]

[1]Information Technology, Maharaja Agrasen Institute of Technology, New Delhi, India
[2]Computer Science and Information Systems, Coastal Carolina University, Conway, USA
Email: harshit.ndl@gmail.com, skumar@coastal.edu

Received 26 September 2014; revised 25 October 2014; accepted 20 November 2014

Abstract

Cloud computing is touted as the next big thing in the Information Technology (IT) industry, which is going to impact the businesses of any size and yet the security issue continues to pose a big threat on it. The security and privacy issues persisting in cloud computing have proved to be an obstacle for its widespread adoption. In this paper, we look at these issues from a business perspective and how they are damaging the reputation of big companies. There is a literature review on the existing issues in cloud computing and how they are being tackled by the Cloud Service Providers (CSP). We propose a governing body framework which aims at solving these issues by establishing relationship amongst the CSPs in which the data about possible threats can be generated based on the previous attacks on other CSPs. The Governing Body will be responsible for Data Center control, Policy control, legal control, user awareness, performance evaluation, solution architecture and providing motivation for the entities involved.

Keywords

Cloud Computing, Security, Privacy, Organization, Control, Governance, Framework, Cloud Provider

1. Introduction

National Institute of Standards and Technology (NIST) defines cloud computing as a computing model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) [1]. These services can be rapidly provisioned and released with minimal management effort or service provider interaction. NIST also defines that the cloud computing can be achieved through three service models: Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS). Cloud computing can be implemented by the four deployment

How to cite this paper: Srivastava, H. and Kumar, S.A. (2015) Control Framework for Secure Cloud Computing. *Journal of Information Security*, **6**, 12-23. http://dx.doi.org/10.4236/jis.2015.61002

models: Private Cloud, Community Cloud, Public Cloud and Hybrid Cloud. This emerging paradigm allows an organization to reduce costs and develops highly scalable solutions [2]. Cloud promises customers with the benefits of a more convenient way of provisioning IT resources at a faster speed and with a lower cost, compared to traditional IT processes and systems.

Cloud computing has been regarded as the next big thing in the Information Technology (IT) industry. It is predicted that it will have a global impact on how people store and access their data. Apart from storage, it also provides other services which can be utilized from anywhere and at any time. The only concern, however, with cloud computing is the security and privacy issues. As people put their valuable data on the cloud, they are completely dependent on the Cloud Service Provider (CSP) to ensure proper security for their data. Due to large amount of attacks on the data on the cloud, many people have lost their important data and moreover, the confidentiality of their data has been compromised. Therefore, security and privacy are big concern in cloud computing. These issues have been impeding the growth of cloud computing and are proving to be a major obstacle for its widespread adoption.

Cloud service providers try to provide cloud services with built-in security features. They try to build a cloud infrastructure that can withstand any sort of failure whether it is technical, logical or physical. However, there are many factors that can harm the security and reliability of the Cloud infrastructure despite of taking all the necessary steps.

They are generally categorized in the following three layers, in which an organization takes control of the security. These are as follows:

- Physical Layer: The physical layer of security encompasses many factors.

1) Data Center: This deals with the geographical location of the data center. Locations are chosen in such a way that they are not prone to natural or man-made disasters. No data center will be successful in withstanding severe earthquakes, cyclones, volcanic eruptions etc. and it is best to keep the data center in a place that is less vulnerable to be affected by these factors. Also, location of data centers is kept confidential so that it does not fall prey to external attacks.

2) Biometric Scanning: There are methods such as finger-print scan or retina-scan which allow only selected employees to enter the data center. There are usually very few people that are allowed physical entry inside the area where the data are actually stored.

3) Building: The buildings are generally designed to be a data center from the start. They are built in such a way that they can withstand fires. There are cameras all around the place and alarms that go off in case of emergency. Employees and security guards are present in the data center 24 × 7.

- Logical Layer: Logical Layer of security deals with the design of the network that is used for providing cloud services. The network is kept secured with the help of firewalls, anti-virus and intrusion detection systems. Companies that provide cloud services do not want to compromise with the quality of the software used, since it would harm their reputation and affect their business. The hypervisors are generally of high standards and these systems are centrally managed and protected.
- Methodology Layer: This concerns with the security method used at local level in a cloud service provider and it may differ from one organization to another. The main concept of this layer is to assure that various other aspects of security is taken care of. The password that every employee has is made to be very secure and difficult to crack as opposed to some preposterous passwords like "1234" which do not really help in making the system secure. The environment inside a data center is generally very secure and only a few trusted staff members are allowed to make significant changes in the system. The cloud service providers try to give the tasks to trusted staff members instead of outsourcing the tasks.

Organizations are playing a vital role in determining the course of Cloud Computing. If the security and privacy issues continue to remain, then future of Cloud Computing might be in danger. We have to find solutions and controls to the security, privacy and reliability problems in order to make cloud computing a trustworthy paradigm.

2. Companies Involved in Cloud Computing

As cloud computing offers exciting new opportunities to the companies to expand their Infrastructure, some companies took it to the next level and started providing cloud services. The big names in cloud service providing industry are Amazon, Google and of late, IBM and Microsoft. Oracle/Sun and HP are also not far behind. Google has built the largest Cloud Computing infrastructure with Data Centers existing in Taiwan, Singapore, Finland, Belgium and Ireland apart from various US states. Amazon, besides being a huge online shopping site, is also a big mover in cloud computing revolution. With Microsoft Azure, Microsoft has also entered the Cloud Computing industry. Oracle/Sun, IBM and Rack Space have also tied their future to Cloud Computing. However, the security issues existing in cloud computing also reflects upon the security breaches and attacks to the Data Centers of these companies.

There have been many instances where the Data Centers of the Cloud Service Providers have slowed down or have stopped working altogether. In June 2012, a big storm in North Virginia affected the Amazon's Data Center. As a result, websites like Netflix, Instagram, Pinterest, and Heroku were down for few hours because they relied on Amazon's cloud service [3]. In another incident, a flawed storage software update over Google triggered an unexpected bug In March 2011. Around 150,000 Gmail accounts were affected and all their messages were deleted in the wake of that software bug [4].

To overcome such security threats, cloud providers try to minimize the risk of attacks by various ways. The whole process of deployment of security is also governed by how they deploy the technology of cloud computing in the first place. The way each cloud service provider deploys the cloud is different from one to another. Therefore, the techniques followed by them are significantly different. For example, as per Cloud Security Alliance Guide [5], Amazon's AWS EC2 infrastructure, as an example, includes vendor responsibility with respect to security and privacy lies only at the physical security, environmental security, and virtualization security level. The user is responsible for security controls at the operating system, applications, and data level. As an example of how the cloud service providers differ from one another, Salesforce.com's Customer Relationship management (CRM) is a SaaS offering and provides entire service to the user. Hence the provider is not only responsible for the physical and environmental security controls, but it must also address the security controls on the infrastructure, the applications, and the data.

According to a recent survey [6], the total number of records containing sensitive personal information involved in security breaches in the United States is more than 600 million records in about 4000 data breaches since January 2005. Recent surveys reveal that human errors and systems glitches caused nearly two-thirds of data breaches globally in 2012, while malicious or criminal attacks are the most costly everywhere at an average of $157 per compromised record.

Some surveys show that malicious attacks (defined as a combination of hacking and insider theft) accounted for nearly 47 percent of the recorded breaches in 2012 in the United States. Hacking attacks were responsible for more than one-third (33.8 percent) of the data breaches recorded [6].

According to a survey by Open Security Foundation [7], there were more than 2000 cloud related data breach incidents globally since 2012. Surveys done on some randomly selected companies show that 82% of those companies saved money moving to cloud while only 14% downsized their IT after cloud adoption.

3. Literature Review

As we discussed earlier, the main concern in cloud computing is of security and the security issues in cloud computing remain the chief obstacle that may prevent its widespread adoption. As more and more data is being migrated to the cloud, there have been more attacks, such as Denial of Service and Authentication attacks. For example, the increase of Internet-capable devices creates opportunities for remote hacking and data leakage. More cloud adopters have been at the receiving end of cloud infrastructure security incidents as compared to traditional IT infrastructure security events. These security incidents and data breaches can have financial consequences on a corporate organization [8]. Despite the decrease in the cost of data breaches in the last year, data breaches are still reported to have cost British and German organizations on average between $2.7 million and $4.4 million [8]. In addition to the economic and financial troubles, security breaches and threats can lead to damaged reputations, loss of customers, delayed software releases and a reduction in investor confidence [9].

3.1. Cloud Computing vs. Outsourcing

In traditional outsourcing, service providers are commissioned to handle data, system and process actively for the user according to the organization's mandate. However, cloud computing has a self-service nature, where users pay for pre-packaged IT resources made available by the cloud providers, using which they process data or other jobs on their own in a self-service fashion. In such cases, the users use infrastructure/resources supplied by the provider, and don't need to own them. Unlike outsourcing, service providers who act actively, cloud providers can be considered as agents who help users to process data and perform other jobs. Cloud providers can, at most, store data passively that the users decide to store on the provider's infrastructure, which is readily retrieval as and when needed.

Shared infrastructure/environments and economies of scale are what drive the public cloud computing providers instead of tailor-made infrastructure to fit the needs of every customer. Though customization of the service is possible in some cases, it would cost additional time and money.

The organization exercises better control over the service provider in traditional outsourcing due to the body of knowledge related to process and systems. Due to one size fit all nature and type of service in the cloud, it's often seen that organization lose control on the cloud providers and struggle with the use of resources on the cloud.

Although, a substantial number of studies already exist on Cloud Computing, it is still unclear how or whether CC differs from the traditional concept of Information Technology Outsourcing. The risks that persisted in IT Outsourcing has just been transferred to Cloud Computing. Security is a prime concern while outsourcing the IT resources of a company and the third party organization that provides outsourcing cannot be trusted blindly with confidential data. Although many service providers are scrupulous about securing their facilities but there may still be risks persisting. The facility has to be secured both on the physical as well as the logical level. All these security risks and privacy concerns can be associated with the issues persisting in cloud computing.

Eric and Yuanyuan [10] believe that contracting to cloud computing include the standard risks of Outsourcing of any kind with 3 major issues being

- Vendor Lock-in: The risk of interoperability persists in cloud computing. Client find themselves locked-in to a specific cloud provider, unable to transition from one provider to another, or finding a lack of interoperability between their existing in-house infrastructure and cloud based services.
- Security and privacy of data: The data that is stored on the client's servers, the client retains control over the security of the servers. But where client data is given to the cloud provider to store, it is stored by the cloud provider in multiple data centres across multiple jurisdictions. Google, for example, has data centres in the US, Europe, Russia, South America and across Asia. Whilst storage across multiple locations may distribute the risk of a single point of failure, it also creates multiple possible points for intrusion.
- Undermining of the confidential data: Concerns regarding security, privacy and integrity of data are further exacerbated by little and/or inconsistent regulatory framework regarding the privacy and security of data. In some countries laws give government agencies a right to inspect data held there and privacy law safeguards are unknown. This clearly undermines the confidentiality of the data stored in the cloud.

3.2. Deployment of Security in Cloud Environment

Compared to traditional IT environment, security deployed at every level in the cloud environment must be different while considering the security needs for each level. Chow *et al.*, [11] think that traditional in-house authorization and authentication framework that were employed previously cannot be extended to the cloud environment and would probably need some modification to be compatible to the services of cloud computing. Subashini and Kavitha [12] highlighted security issues applicable to various layers of the cloud computing environment while noting that security needs will vary for each delivery model. The biggest threat to the cloud environment that exists today is of unauthorized access. The users put their confidential data on the cloud hoping that their data will remain safe but due to unauthorized access, the confidentiality of the data is undermined. As a result, users are reluctant to migrate their data to the cloud.

3.3. Security Issues in Cloud Environment

Per our literature review, common security issues that arise in cloud computing can be classified broadly into six areas:

- Infrastructure: This concern is mainly related to the physical security provided by the cloud service provider. Cohen [13] states that from physical security perspective, the security issues might be more vulnerable in cloud computing as compared to traditional in-house security techniques. Security of the data centers provisioned by the cloud service providers would fall under infrastructure area. This concerns the amount of surveillance that exists inside the data center. There must be enough security guards and cameras present so as to reduce the risk of external intrusion or attacks. Moreover, this security control must be consistent across all the cloud providers. Cloud provider should ensure that the data center security is well-planned out and this might just alleviate the security risks which are larger as it is.

- Data: The 2011 Ernst and Young Global Information Security Survey [14] reported that 36% of respondents were currently using cloud computing services or deploying applications and storing data in cloud environments, as compared to 23% from the previous year. Furthermore, this report goes on to state that 25% of respondents are currently evaluating or investigating the use of cloud services in the subsequent year. Cloud computing services are also being utilized by governments in order to reduce costs and improve the efficiency of IT solutions within their agencies [15]. With more and more organizations moving to cloud and storing their data in the cloud, there is more data available than there ever has been before. Therefore the surface area of the attacks is also larger. As a result, unauthorized data accesses are common attacks that occur. These attacks weaken the trust of the users and they feel that their data is insecure. Users also raise other issues that might be possible with the type of data security provided by cloud providers. These include the security of Application Program Interfaces (API) provided by them. Users would want to know whether the software used and the machines present are reliable and the way in which they are used, such that it is sufficient to ensure data security. Cloud Providers are reluctant to provide this kind of information as giving all the details about security they will make themselves vulnerable to more attacks. This creates a lack of transparency between the users and the Cloud Providers.
- Access: Jansen and Grance [16] stated that one of the biggest concerns for an organization, considering the adoption of cloud computing, is preventing unauthorized access to resources. It has been demonstrated that the unauthorized access of data compromises the confidentiality of the data stored access [16]. Cloud computing promises availability *i.e.* users can access the same data from any device. Question is if this would impact security? If there would be any unauthorized access of someone's data, it will not be from the same device that the user uses to access it but from a remote location and obviously from a different device. In that case, it is essential to ensure that the user is genuine. Therefore, a default device should be assigned to a user by the cloud provider and if the user tries to access the data from another device, one would need to give proper verification and authentication in order to prove his identity. Google follows the location based access technique but not all the cloud providers follow this [15]. Hence an organization should ensure that all the providers consistently follow these controls.
- Availability: To ensure availability to all the users, that try to access their account or data, the cloud service must scale itself according to the number of users. The number of servers increase or decrease to keep up with the traffic. This scalability feature is performed either automatically by the cloud providers' servers through knowledge learning or manually by prompting the administrator to do this. This however, will not ensure that a cloud can handle any amount of traffic that comes its way. SAP's CEO, Leo Apotheker stated: "There are certain things that you cannot run in the cloud because the cloud would collapse. Don't believe that any utility company is going to run its billing for 50 million consumers in the cloud." This raises another issue that in case of huge traffic caused by DoS attacks, the cloud might just collapse and for that time the users will not be able to access their data.
- Compliance: Several organizations such as SAS 70 and ISO 27001 put forth regulations from the security audits, operation traceability and data location perspective. Cloud providers are supposed to follow these rules & regulations in order to ensure security of the cloud. Users need to be completely aware of what all rules and regulations are followed by their cloud provider. There have been many instances such as the case of Google Docs in March 2009, where full security and data safety audit reports were not made public and data integrity was allegedly compromised by improper access [17].
- Role of Users: The customers also play an important role in determining the course of cloud computing. Cloud adopters need to trust the cloud providers and understand that until the technology is fully matured, that cloud computing customers will need to make every effort to protect the information consciously. Reed and Bennett [18] provide key guidelines on how to make best use of secure cloud services and a concise guide to cloud computing. The key points of their discussion are:

1) The biggest risk that the technology faces today is Users.

2) Shadow IT is an on-going risk and generally introduced by such employees who have no concerns beyond their own role in considering the risks involved in the solution provided.

3) Experienced teams often roll out new technologies, but there still exists the risk when traditional security practices are ignored or adapted to the new environment.

4) Attackers will always go after the valuable things and it may not be money itself.

5) A single security standard is unlikely to save you.

- Related Solutions Proposed in Literature: There are few organizational control perspective solutions proposed in the literature to address the issues discussed earlier. Organizational control will help to manage the overall services of the cloud service provider and in return, reduce the security and reliability issues of cloud computing. The cloud computing governance model by Guo, Song and Song [19] addresses requirements and objectives of service, policy, security, risk and compliance management in cloud computing and supplements detailed descriptions and important information on the required system design. Their main contribution lies in the development of an architecture for Risk and Compliance Management (RCM), which focuses on controlling of services and policies (compliance regulations) by means of monitoring cloud computing Services. An overview of RCM in Cloud Computing is provided by Chaput and Ringwood [20]. They discuss different types of RCM regulations like laws and industry regulations affecting the adoption of Cloud Computing. Four key features discussed are security methods like data classification, access control, authentication and authorization, risk management methods like business impact analysis and business continuity, certifications and auditing standards.

In the territory of compliance management, Matthews *et al.* [21] propose virtual machine contracts, which extend the open virtual machine format. These electronic contracts describe and formalize technical requirements such as firewall rules, transport protocols, source and destination addresses as well as source and destination ports, to configure the virtual machines for a particular network segment. Kamara and Lauter [22] present methods and architectures for the encryption of cloud storage. One objective is to secure storage services for regulatory compliance by encrypting the data on-premise to avoid access to the data by a third party. They argue that this approach reduces the legal exposure and in return reduces the risk factors. Brandic *et al.* [23] provides an extension of Service Level Agreements (SLA) with regard to compliance issues. They introduce Compliance Level Agreements (CLA) and develop a detailed architecture for compliance management in Cloud Computing.

The security risks in cloud computing can be reduced by specifically outlining the attacks and threats which may be considered as malicious. Ristenpart *et al.* [24] believes that security guidelines are also needed to address and mitigate risks associated with hypervisor-level attacks including cross-virtualization attacks. An insecure hypervisor can allow a malicious user to gain access to data stored in virtual machines hosted on a vulnerable hypervisor. Standards and guidelines can specify how the organization accomplishes a Virtual Machine Image (VMI) [25]. Wei *et al.* [26] suggest that a framework is developed to manage VMI creation, storage and destruction procedures. This framework is likely to contain controls such as filters to remove sensitive information from an image prior to publishing and a mechanism to track changes performed on a specific image to mitigate malicious image modification.

Another organizational control is punishment, which is carried out to reduce the undesirable behavior of employees such as non-compliance to the safety regulations and rules. Punishment is generally considered as a very effective way to produce behavior change. As a management tool within organizations, punishment is defined as "the application of a negative consequence to, or the withdrawal of a positive consequence from, an employee" [27]. Mohammad I. Merhi & Punit Ahluwalia [28] state that some employees in general tend to repeat actions that do not produce negative outcomes and prefer to avoid those actions that lead to negative actions; thus reducing likelihood of punishment. The rationale behind this argument is that punishment creates an anxiety in minds of employees which forces them to change their behaviors towards organizational policies.

All the solutions mentioned above are very limited and specific to some particular areas of the cloud computing industry. Acting on these specific details from outside will be very painstaking and time consuming. Therefore, we need to come up with such a solution that integrates all these methods and binds them into a unit that will control all the proceeding in the cloud environment. We will call it the Governing Body. This will help to bring some kind of Organizational Control in the cloud environment and reduce the security and reliability issues persisting in cloud computing.

4. Governing Body

There is a need for the cloud providers to hide some security related information, as they need to keep all the information about the security procedures confidential in order to minimize any security breaches. Do we have any reference to substantiate this claim This lack of transparency results in the cloud customers losing trust on the cloud providers. As a result, customers are reluctant to store their valuable data on the cloud, which undermines the potential of cloud computing. Our framework approach to solve these issues is by the formation of a governing body which will act as an interface between the cloud providers and cloud end users and provide organizational control. The governing body in our framework is unique compared to the existing infrastructure due to the following reasons: This governing body will be an independent unit and will not be influenced by any of the two entities involved. It will be responsible for any and every actions that take place inside the cloud environment. Various cloud providers will need to register themselves to the governing body and then that body will assess all the procedures and methodologies involved in the technology.

In general, this Governing Body will be responsible for risk assessment & management, security performance evaluation, policy, audit and compliance with respect to the deployment of cloud layer. The Governing Body is different from the existing infrastructure as it will not be limited to just assessing the conditions. In addition, it will also provide solutions and alternatives to the customers in case of any issues that takes place in the cloud environment whether it is due to technology failure or any external factors.

As shown in **Figure 1**, the governing body is an interface that provides formal control and governance between cloud provider and customer, to ensure that there is a smooth working and a well-coordinated system. The governing body will be responsible for the following functionalities, which the cloud provider cannot provide on their own.

4.1. Data Center Control

Governing body will be responsible for the operations inside the cloud environment. By migrating applications to the cloud, the risk factors increase. The traditional data control methods need to be modified in order to cope with the security and privacy challenges associated with the cloud environment. The entity that is at most risk inside the cloud environment is data center. The data center is a centralized location, where the entire customer's data are stored. Hence, cloud providers need to ensure that no security breaches take place inside the data center. To achieve this, the governing body should continuously monitor the possible security related threats and the products/solutions available to counter those threats, procure and implement them. For instance, some of the solutions include data replication facilities with hot site disaster recovery service. The governing body would need to ensure that the data centers are safe and secure and that all the data that resides inside it, must be backed up to ensure the business continuity in case of disaster. Disaster recovery and business continuity is one thing that every cloud provider promises. However, to ensure it gets implemented and operates in a right manner, there needs to be a centralized authority to get them implemented.

4.2. Policy Creation and Control

The security features that are included in the cloud environment are very important to determine the level of security present in the cloud. The security policy that will be drafted by the governing body will be responsible for all the layers of the security features that will be included in the cloud. For example, the security policy shall specify the use of firewalls, anti-virus, type of virtualization and the hyper-visor used to achieve the secure cloud

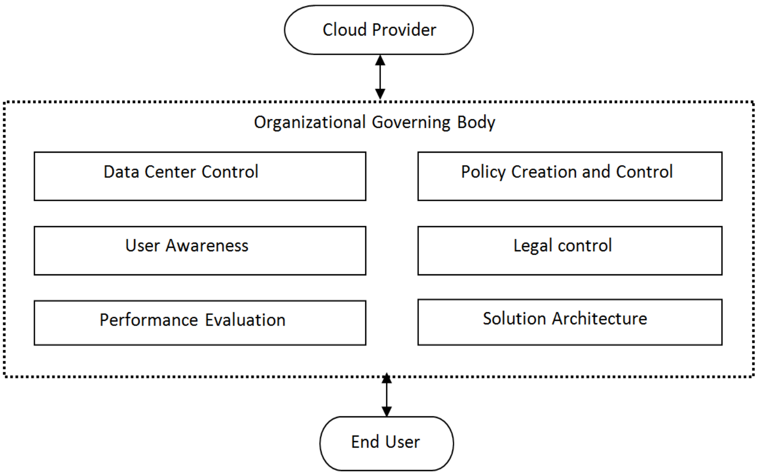


Figure 1. Organizational control through governing body.

functionality. It is to be noted that the above features may vary depending upon the budget of the cloud provider, which in turn will reflect in the use and adoption of that cloud. We suggest that the governing board and the cloud provider would jointly determine the security features to be included. Only an outline of the features will be discussed between the two and once the cloud is deployed, the governing body would validate to see if all the features discussed before have been implemented.

4.3. User Awareness

The governing body will need to specify all the procedures and methods that a cloud provider and user follow to ensure the security and privacy of the cloud. The governing body needs to filter and provide information to users in such a way that the users are aware of the security features and at the same time, no confidential information is leaked. Our automated control framework described in next section, ensures that based on triggers, central body convey right information at right time to right parties involved in the environment in an automated fashion. This will ensure removal of the lack of transparency in communicating security features, such that users are able to trust the cloud providers.

4.4. Legal Control

There are a number of jurisdictions and laws that apply to cloud computing. Laws vary from place to place and generally the data centers of a cloud provider are located in different countries or may be different continents. To gain knowledge and abide by all the laws of different location can be very difficult to cope with. For example US Patriot Act can be applied to foreign organizations that use U.S based cloud provider. Per US Patriot Act the Governmental authorities only may access cloud data pursuant to the Patriot Act to 1) "obtain foreign intelligence information not concerning a United States person" or 2) "protect against international terrorism or clandestine intelligence activities". Even a single law broken may affect the organization in many different ways. These laws and jurisdiction vary from geographical locations to the methods involved in the cloud computing and allowing the personnel to enter or work in the facility. Complying with all the jurisdiction and laws is a very time consuming job and may reflect in the efficiency of the cloud. Therefore, by outsourcing and letting the governing body take care of all the legal matters, the cloud provider can redirect the resources to ensure their cloud services are safe, secure and efficient and at the same time ensure all the jurisdictions and laws are followed.

4.5. Performance Evaluation

One of the parameters to evaluate the performance of the cloud is the number of security breaches and attacks to determine the performance of the cloud. Governing body should assess the performance of the cloud environment based on the security parameters and draft a report that will determine the efficiency of the cloud. This will help users in determining what all security features are being ignored by the cloud provider and help them make decisions by providing the right choices. The performance evaluation of the providers would motivate the good providers to increase their trust score with the governing body, compared to those providers who can try to negatively affect the organization. This will also help the governing body to rank the providers based on the provider's trust score. The cloud providers will also benefit from this evaluation, as they will get to know the limitations and the disadvantages in their implementation of security controls in the cloud computing environment and redirect the resources where the attention is needed. With the help of the performance evaluation functionality, the factors that caused attacks and threats can be identified and response strategies cab be applied to remove those threats and attacks, to ensure the cloud is safe and reliable.

4.6. Solution Architecture

The governing body shall not only be responsible for the policy, monitoring, evaluation and legal controls but also responsible for providing solutions to the customers: providers and end users. For example, following are some of the problem samples that the governing body shall be responsible for providing solutions: 1) Customers lost their data or are unable to access their data due to the occurrence of mishap in the cloud environment. 2) If a Cloud Provider goes bankrupt or due to some other factors and decides to shut down some of the data centers, many users' data will be at risk. At that point of time, the governing body will be responsible for providing alternative solutions to the users. The solution might range from migration of data to some other cloud provider or giving all the data back to the user so that they can manage it themselves in their internal IT environment. This results in tighter organizational control for the resources, which is the governing body's mandate.

In a large organization that caters to the needs of millions of customers, there could be many unsatisfied customers, who often file legal complaints or threaten to damage the reputation of the organization in some way or the other. Disputes and conflicts may also arise between two or more cloud providers, due to the disagreement over the issues. Disputes in IT industry are very common and there have been a number of incidents where some company adopted someone else's ideas to develop their own product. For instance, recently Microsoft sued Salesforce.com for the cloud computing patent infringement. In this case, the governing body will make sure that the conflicts and disputes are solved through our framework. This is done with the help of threat index, which we introduced in our framework. The threat index is computed by the security parameters, of which conflicts and disputes are part of it.

4.7. Motivation for the Entities Involved

The proposed framework ensures that the entities involved: Cloud provider, governing body and the end user are motivated to participate in the operations. The motivation for the governing body is in the satisfaction on its leadership service to control the cloud operation between the cloud provider and the end user successfully in a secure manner. The Governing Body will also hold the power to send a warning or shut-down a cloud provider if the cloud provider fails to comply with most of the regulations set by the Governing Body. The cloud provider can also be warned if its recent methods to secure the cloud are proving to be ineffective or even dangerous. In this case, the cloud providers might be reluctant to support the Governing Body and might even question its existence as it is harming them in one way. On the other hand however, by complying with all the regulations set by the Governing Body, they will ensure quality in their functioning and therefore will attract a large number of customers. In this way, the Governing Body can prove to be a negative factor to those who aren't securing their technology properly and can also prove to be massively beneficial for those who are abiding by all the rules and regulations of the Governing Body.

As a result, the cloud providers who are detrimental to the needs of the user are marginalized and the cloud providers who are sensitive to the secure operations of the cloud become successful in their operations. This also ensures that the provider works collaboratively with the governing body to ensure its success in its existence.

Thus the governing body provides organizational control to the cloud environment by keeping track of all the activities going on and providing solutions as and when required. By establishing a central body, cloud computing will become organized and managed by ensuring right information is conveyed at right time to right parties. Thus, through this governance control framework enabled governing body, which is trusted by both the cloud provider and the end user, we can eliminate the lack of transparency that exists between the user and the cloud provider. As the end users perceive security and transparency in the communications, with minimal conflicts and disputes, they would be motivated to participate in the clouds computing activities (**Table 1**).

5. Organization Control Framework

The functionalities that were discussed earlier can be achieved by our framework, as shown in **Figure 2**. Security parameters indicated in **Figure 2** include technical, legal and policy parameters. In this framework, Threat Index (TI) calculates the vulnerability of a cloud environment based data center to threats and attacks. This threat index is calculated based on the parameters from cloud based data center security control, legal control, policy control perspectives. By calculating the threat index, performance trend of a cloud provider can be identified and communicated to the user. Threat Index can be calculated over a specified period of time and that can be compared with the benchmark index thresholds obtained with the help of historical training [29]-[32]. Historical training is done by collection of data, with and without attacks, with and without legal control, with and without policy control over a long period of time. The comparison of the index threshold with the threat index helps the organization to gain knowledge of the current security, policy and legal trends. This will help the organization and the cloud provider to increase or decrease the controls from technical, legal and policy perspective with the help of solution architecture framework. It will also help them pointing out the methodologies that are flawed, if any, and help them improve it in order to increase the reliability of the cloud.

Table 1. Proposed methods to handle security challenges.

Security Challenges	Method(s)
Data Centre	1. Design a basic layout for the Data Centre such that secure cloud services are provided by cloud provider to the user 2. Continuously monitor security related threats and provide solutions such as data replication and hot-site recovery service, if the need arises
Policy Creation and Control	1. Security policy will be drafted by Governing Body to ensure the security at all layers 2. Cloud Provider and Governing Body will collaborate to implement and control the features in the security policy.
User Awareness	1. The governing body will need to specify all the procedures and methods that a cloud provider and user need to follow 2. Filter the information and make the users aware of the security features without leaking any confidential information. 3. central body convey right information at right time to right parties involved in the environment in an automated fashion
Legal Control	1. Governing body would acquire global laws pertaining to the cloud operation and take care of all the legal matters related to global cloud operations so that the Cloud Provider can focus its resources on making the cloud safe, secure and efficient.
Performance Evaluation	1. Assess the performance of the cloud provider based on the security parameters and estimate the efficiency and the threat index of the provider's operations. 2. Governing Body will then rank all the cloud providers based on their efficiency.
Conflict and Dispute Resolution	1. This will be done with the help of threat index that computes security parameters of which, conflicts are a part. 2. If the cloud provider is found guilty in a dispute, its license will be revoked.

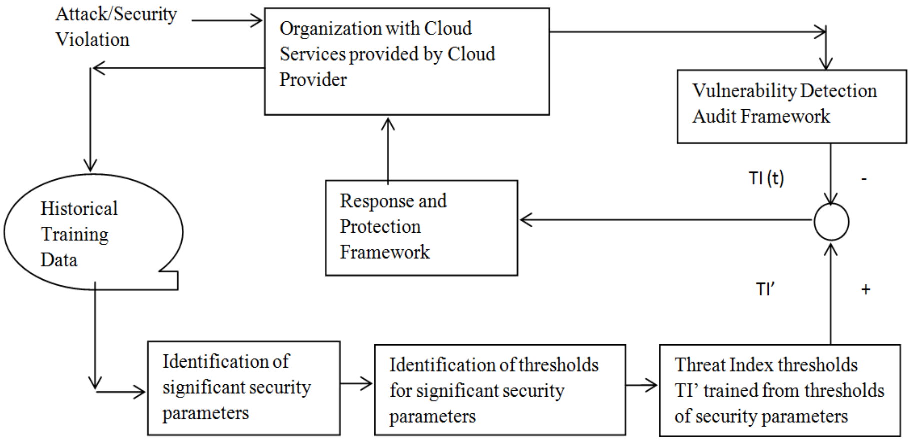

Attack/Security Violation
Organization with Cloud Services provided by Cloud Provider
Vulnerability Detection Audit Framework
TI (t)
-
Historical Training Data
Response and Protection Framework
TI'
+
Identification of significant security parameters
Identification of thresholds for significant security parameters
Threat Index thresholds TI' trained from thresholds of security parameters

Figure 2. Organization control framework for cloud services.

6. Summary and Conclusion

Cloud computing is purported to be the future of the IT industry. Cloud computing marks a true paradigm shift in how the computing would happen in the future and cloud computing is likely to have the same impact on IT industry that foundries have had on the manufacturing industry. However, one thing that proves to be the biggest obstacle in its course is security issue.

Security issues vary from physical and legal level involving data centers and geographical locations to methodological level involving the policy and logic used in deploying the cloud to technical level involving the technology involved in implementing the cloud. This has prevented cloud computing from its widespread adoption.

From an organizational control perspective, we provided an automated control framework comprised of independent governing body that will mediate between the cloud provider and the user. Governing body will be responsible for ensuring the security of cloud based data center, implementation of a secure policy & control, increase the user awareness about security methods deployed, handling the legal matters, resolution of disputes, evaluation of performance and providing solutions for the end user. We have described a framework, which computes threat index based on the security parameters, that the governing body could apply to fulfill their responsibilities and use in the planning the implementation of the security policy to keep the organization in control from the cloud computing security and privacy issues.

References

[1] Mell, P. and Grance, T. (2011) The NIST Definition of Cloud Computing. NIST Special Publication 800-145, National Institute of Standards and Technology, Gaithersburg.

[2] Armbrust, M., Fox, A., Griffith, R., Joseph, A.D., Katz, R., Konwinski, A., Lee, G., Patterson, D., Rabkin, A., Stoica, I. and Zaharia, M. (2009) Above the Clouds: A Berkeley View of Cloud Computing. Technical Report No. UCB/EECS-2009-28, University of California, Berkeley.

[3] Morgan, T.P. (2014) Amazon Cloud Knocked out by Violent Storms in Virginia. http://www.theregister.co.uk/2012/06/30/amazon_cloud_storm_outage/

[4] Mah, P. (2014) The Big Gmail Crash and the Lesson for Email Administrators. http://www.theemailadmin.com/2011/03/the-big-gmail-crash-and-the-lesson-for-email-administrators

[5] Cloud Security Alliance Guide (2013). https://www.cloudsecurityalliance.org/csaguide.pdf

[6] Symantec (2014). http://www.symantec.com/connect/blogs/data-breach-trends

[7] Open Security Foundation *Dataloss DB* [Data File] (2014). http://www.symantec.com/connect/blogs/data-loss-db-breach-data-breaches-classified-source

[8] Glisson, W.B., McDonald, A. and Welland, R. (2006) Web Engineering Security: A Practitioner's Perspective. *Proceedings of the* 6*th International Conference on Web Engineering*, ACM, Palo Alto.

[9] Ponemon Institute LLC (2011) The 2011 Cost of Data Breach Study: Global. Symantec.

[10] Clemons, E.K. and Chen, Y.Y. (2011) Making the Decision to Contract for Cloud Services: Managing the Risk of an Extreme Form of IT Outsourcing. 44*th Hawaii International Conference on System Sciences* (*HICSS*), Kauai, 4-7 January 2011, 1-10, http://dx.doi.org/10.1109/HICSS.2011.292

[11] Chow, R., Golle, P., Jakobsson, M., Shi, E., Staddon, J., Masuoka, R. and Molina, J. (2009) Controlling Data in the Cloud: Outsourcing Computation without Outsourcing Control. *Proceedings of the* 2009 *ACM Workshop on Cloud Computing Security*, Chicago, 13 November 2009, 85-90.

[12] Subashini, S. and Kavitha, V.A. (2011) Survey on Security Issues in Service Delivery Models of Cloud Computing. *Journal of Network and Computer Applications*, **34**, 1-11. http://dx.doi.org/10.1016/j.jnca.2010.07.006

[13] Cohen, M. (2012) Forecasting the First Steps of Cloud Adoption. *eWEEK*, **14**, 1-3.

[14] Ernst & Young Advisory Services (2011) Into the Cloud, out of The Fog—The 2011 Global Information Security Survey. Ernst & Young, Zimbabwe.

[15] Willcocks, L., Venters, W., Whitley, E. and Hindle, J. (2012) Cloud on the Landscape: Problems and Challenges. The New IT Outsourcing Landscape: From Innovation to Cloud Services. Palgrave Macmillan, Basingstoke.

[16] Jansen, W. and Grance, T. (2011) Guidelines on Security and Privacy in Public Cloud Computing. NIST Technical Report-SP-800-144.

[17] Vascellaro, J.E. (2013) Wall Street Journal Article. http://blogs.wsj.com/digits/2009/03/08/1214/

[18] Bennett, R.G. (2010) Silver Clouds, Dark Linings: A Concise Guide to Cloud Computing. Prentice Hall, Upper Saddle River.

[19] Guo, Z., Song, M. and Song, J. (2010) A Governance Model for Cloud Computing. *IEEE Proceedings of the International Conference on Management and Service Science*, Wuhan, 24-26 August 2010, 3759-3764.

[20] Chaput, S.R. and Ringwood, K. (2010) Cloud Compliance: A Framework for Using Cloud Computing in a Regulated World. In: Antonopoulos, N. and Gillam, L., Eds., *Cloud Computing Principles Systems and Applications*, Springer, Heidelberg, 241-255.

[21] Matthews, J., Garfinkel, T., Hoff, C. and Wheeler, J. (2009) Virtual Machine Contracts for Datacenter and Cloud Computing Environments. *ACDC*'09 *Proceedings of the* 1*st Workshop on Automated Control for Datacenters and Clouds*, Barcelona, 19 June 2009, 25-30. http://dx.doi.org/10.1145/1555271.1555278

[22] Kamara, S. and Lauter, K. (2010) Cryptographic Cloud Storage. *Proceedings of the* 1*st Workshop on Real Life Cryptographic Protocols and Standardization*, Canary Islands, 28 January 2010, 1-14.

[23] Brandic, I., Dustdar, S., Anstett, T., Schumm, D., Leymann, F. and Konrad, R. (2010) Compliant Cloud Computing (C3): Architecture and Language Support for User-Driven Compliance Management in Clouds. *IEEE Proceedings of*

the 3*rd International Conference on Cloud Computing*, Miami, 5-10 July 2010, 244-251.

[24] Ristenpart, T., Tromer, E., Shacham, H. and Savage, S. (2009) Hey, You, Get off of My Cloud: Exploring Information Leakage in Third-Party Compute Clouds. *Proceedings of the* 16*th ACM Conference on Computer and Communications Security*, Chicago, 9-13 November 2009, 199-212.

[25] PCI Security Standards Council (2011) Information Supplement: PCI DSS Virtualization Guidelines.

[26] Wei, J., Zhang, X., Ammons, G., Bala, V. and Ning, P. (2009) Managing Security of Virtual Machine Images in a Cloud Environment. In: Oprea, A., Ed., *ACM Workshop on Cloud Computing Security*, ACM, New York.

[27] Trevino, L.K. (1992) The Social Effects of Punishment in Organizations: A Justice Perspective. *Academy of Management Review*, **17**, 647-676.

[28] Merhi, M.I. and Ahluwalia, P. (2013) Information Security Policies Compliance: The Role of Organizational Punishment. *Proceedings of the* 19*th Americas Conference on Information Systems*, Chicago, 15-17 August 2013, 1-7.

[29] Alampalayam, S.P. and Kumar, A. (2003) Security Model for Routing Attacks in Mobile Ad Hoc Networks. *Proceedings of IEEE VTC*, Louisville, 6-9 October 2003, 2122-2126.

[30] Alampalayam, S.P. and Kumar, A. (2007) Statistical Based Intrusion Detection Framework Using Six Sigma Technique. *International Journal of Computer Science and Network Security*, **7**, 333-342.

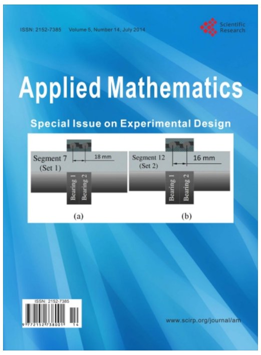
[31] Alampalayam, S.P. and Kumar, A. (2004) Predictive Security Model Using Data Mining. *Proceedings of IEEE Globecom*, Louisville, 29 November-3 December 2004, 2208-2212.

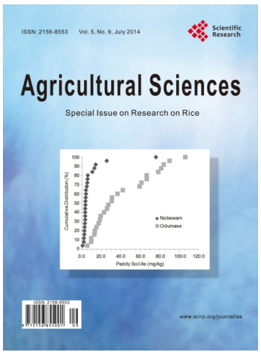
[32] Alampalayam, S.P. and Srinivasan, S. (2009) Intrusion Recovery Framework for Tactical Mobile Ad Hoc Networks. *The International Journal of Computer Science and Network Security*, **9**, 1-10.

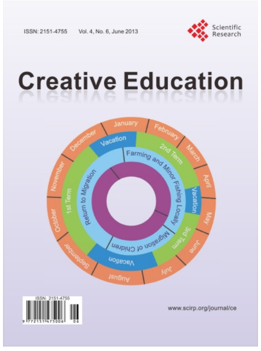
Advances in
Bioscience and Biotechnology

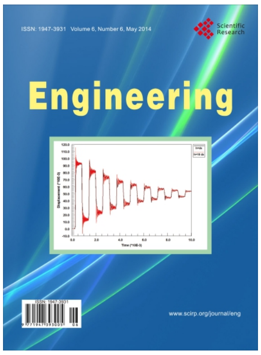
American Journal of
Analytical Chemistry

American Journal of
Plant Sciences
Special Issue on Photosynthesis

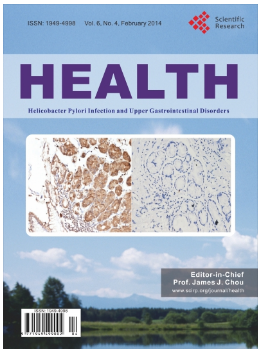

Applied Mathematics
Special Issue on Experimental Design


Agricultural Sciences
Special Issue on Research on Rice


Creative Education

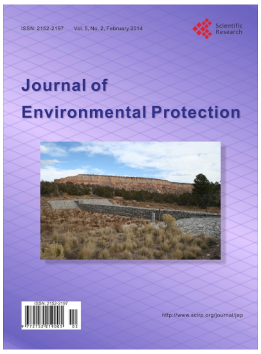

Engineering

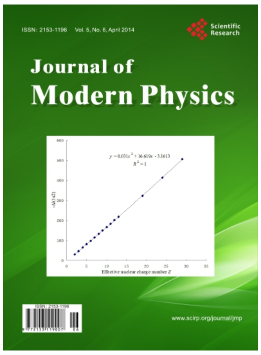
Food and Nutrition Sciences


HEALTH
Helicobacter Pylori Infection and Upper Gastrointestinal Disorders
Editor-in-Chief
Prof. James J. Chou

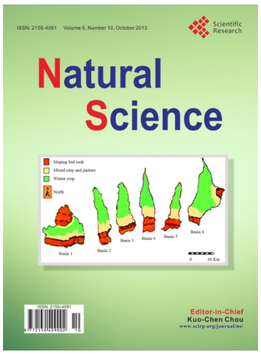
Journal of Computer
and Communications

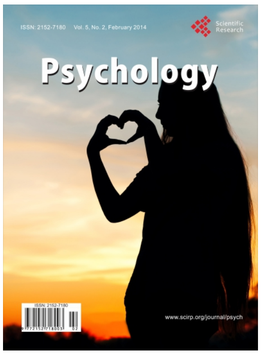
Journal of Cancer Therapy
Special Issue on Bone Tumor Research


Journal of
Environmental Protection


Journal of
Modern Physics

Modern Economy


Natural
Science
Editor-in-Chief
Kuo-Chen Chou


Psychology