Aligning Cloud Computing Security with Business Strategy

Hany Mohamed Hassan El-Hoby [1], Mohammed A. F. Salah [2],
Prof. Dr. Mohd Adam Suhaimi[3]
[1](Information System,, ICT/ IIUM, Malaysia),
[2](IS, ICT/ IIUM, Malaysia),
[3](IS, ICT/ IIUM, Malaysia)

ABSTRACT : *These days, the technological growth in the IT sector is rapid. Cloud computing is also one of the new technologies that have both benefits and limitations. This paper gives an overview of how cloud computing can be helpful for an enterprise. It emphasizes on how cloud computing can be adopted in the IT sector. The paper also discusses the security issues of cloud computing. This article also highlights the issue of data leakage in this technology which face the cloud computing clients. The authors have designed a model to solve this issue through data isolation. A business value will be achieved through the proposed model by aligning the cloud computing security with the business strategy and increase the security procedures to verify the authenticated users through the virtual system.*

Keywords -: *Aligning Business/ IT goal, cloud computing, security, Privacy.*

1. introduction

Because of serious market competition and a considerably modifying company environment, cloud computing is considered as an important area for IT. The goal of the practice of computing and that is to make better use of information technology resources, and combine them together to achieve the increase in production and be able to deal with various issues calculation [1]

From a business perspective, companies are progressively trying to move the business processes and to integrate them with the current information system (IS) programs and construct an application based on the internet technologies to exchange with trading associates. [2]

The provider must ensure that customers can continue to have the same protection and privacy management over their applications and services to ensure that their organization and customers are protected and they can meet their service-level agreements, and show how they can prove compliance to their auditors.

The authentication system seeks to increase the confidentiality of security providers. The Virtualization refers to virtual process that are used to simulate physical resources. Thus great benefit can be derived from cloud computing systems.

Cloud computing is a growing technology that can provide customers with all kinds of accessible alternatives, such as channels, tools, and applications.

This paper proposes a Trusted Platform to ensure accuracy and confidentially in Cloud Computing Security Platform (CCSP) aligned with business strategy.

1. Background

1.1. Cloud computing concept

The cloud computing is a kind of service provider that offers all of the application delivered as a service through the Internet and the hardware and software that may be located in the data center. Cloud computing is a new model that provides computing resources with services and applications soft distributed systems and data storage [1].

1.2. Business Factors in Cloud Computing:

The potency factors of cloud computing ensure a competitive advantage and system agility in business [3].

A business value will be gained from the following factors which will be achieved through the cloud computing service provider.

1.2.1. The business factors of cloud computing:

a- Agility and Competitive Edge:

Level to which enhanced agility in working with competitive markets and customer requirements allowed alignment with cloud.

b- Cost-Benefits:

Level to which financial concerns allowed alignment with cloud.

c- Executive Involvement of Business Organization(s):

Level to which contribution of senior managers from business enterprise allowed alignment with cloud.

d- Executive Involvement of Information Systems Organization:

Extent to which contribution of senior managers from internal information systems of the organization allowed alignment with cloud.

e- Organizational Change Management:

To which extent business change management procedures allowed alignment with cloud.

f- Participation of Client Organizations:

Level to which government or industry regulating requirements allowed alignment with cloud

g- Regulatory Requirements:

To which level government or industry regulating requirements allowed alignment with cloud.

h- Strategic Planning:

To which level business planning allowed alignment with cloud. [4].

1.3. Threats, Vulnerabilities and Risks in Cloud Computing:

Bisong mentioned the risks related with the cloud processing systems, which may appear as listed below [5]:

1- Cloud computing resources and components can be used through the unauthorized access
2- Malicious attacks which may appear from internally
3- The risk which related with shared information technology systems and IT resources
4- Data can face some trouble such as data loss, leakage and manipulation
5- Data manipulation, leakage and loss.
6- User account hijacking

2. Literature review

2.1. Issues to Clarify Before Adopting Cloud Computing:

Before adopting cloud computing there are some issue should be considered:

2.1.1. User Access:

Administrators who have privileges to control the information in the cloud computing environment should follow the companies hiring rules and policies.

2.1.2. Regulatory Compliance:

The organization or the company have to be sure that the security certification and external audits are needed to be submitted by the cloud service provider.

2.1.3. Data location:

Cloud computing service provider need to follow the organization request in storing the data in specific locations and these location have to follow the current state rules.

2.1.4. Isolating the data:

Organization should take care about the data isolation and have to investigate if the encryption methods are applied and work effectively.

2.1.5. Disaster Recovery:

Organization has to be sure that data recovery plan is already active for recovering data and information and how long of time it will take in case of disasters.

2.1.6. Long-term Viability:

Ask potential suppliers how you would get your data back if they were to don't succeed or be obtained, and discover out if the data would be in a structure that you could quickly transfer into an alternative program.

2.2. Cloud Security Requirements:

The security architecture of the cloud is established after the construction of the security policy in the cloud. The creation of the cloud security architecture should be directed by the security policy. Some of the security requirements for the cloud architecture are listed below:[15]

a. Network Time Protocol by synchronizing at the same time helps in the correct working of systems and gives reliable system information records. Clock divergence between system and computers are resulting in errors which may be difficult to identify.

b. The cloud users should be managed and verified in agreement with the lawful requirements and the policies. For example, if the system is compromised in the future, the historical information of the user login can be helpful for further investigations.

c. The access to the cloud infrastructure can be narrow and limited by identifying the user information through the access control action. Thus, accessing the client's data and information by the cloud staff should be limited and restricted.

d. Security staff should deliver the important security alerts on time. So, by identifying, analyzing and investigation these alerts the other related security incident can be controlled. Cloud computing service provider can avoid the critical security incidents by providing specialized systems for intrusion detection. So, by installing these systems in the cloud service it will be applied automatically to the cloud users.

2.3. Security Standards and Policies:

There are a lot of resources are available to help in the enhancement of information security standards and polices. These policies and standards should be analyzed when significant changes happen in the company or in the IT environment [4].

a. Different people should be granted the roles and responsibilities. Also the policy should be granted the techniques on how to execute the investigation reporting.

b. All infrastructure components, servers, switches, software configuration, and network configurations back up have to be taken care of.

c. Initial and regular testing should be documented.

d. To follow the encryption standard an accepted cryptography algorithms with a key needed to be used

e. Quality of acceptable password should meet the Criterions Comply.

2.4. Steps to Cloud Security:

Organizations need to understand the security vulnerability that might be appeared through using the services of cloud computing. By following the steps below enterprises will understand the security paradigm provided by the cloud computing service provider [5],[14]:

a. Understand the cloud

By recognizing how the security of the data received by the cloud can be impacted through the cloud's loose structure. This can be achieved by looking inside the cloud deeply and knowing the way of transferring data and managing data which done by cloud service.

b. Demand Transparency.

By ensure that the cloud computing service provider is ready to provide information by detailed about the security architecture and the cloud provider is prepared to be ready to consent frequent security audit. The frequent protection audit should be conducted by a separate body or government organization.

c. Reinforce Internal Security.

By ensure that internal protection technologies and techniques containing firewalls and user access controls of the cloud computing service provider are powerful and capable with the measurements of cloud security.

d. Consider the Legal Implications:

Understanding how the information transmitted to cloud is going to be impacted by the rules.

e. Pay attention:

Regularly get the new updates in the technology of cloud computing and examine how it will affect and influence the security of the data.

2.5. What is the challenges in security of cloud computing and how to handle it:

The challenges of cloud computing are very big. The cloud architecture faced more threats. Like internal and external threats on cloud environments on cloud providers.

- **Multi-Tenancy**

On one hand, the cloud provider develops its protection to fulfill at a higher risk customer, and all the customers of low risk and then get better protection than they would have. On the other hand, a customer may come in contact with a higher level of exterior threat because of the business practices of the other subscribers [6]. When you are dealing with information technology within an organization, the threat is mostly for the organization alone to bear.

- **Distributed Data Centers**

Theoretically, a cloud computing environment should be less prone to mishaps because suppliers can offer an environment that is distributed geographically. And organizations should participate in the cloud computing services that do not require geographically dispersed provider to initiate the study regularly disaster recovery plan and work. [7]

- **Shared Risk**

If the software as a service provider of infrastructure needs, it may be best to get those infrastructure of infrastructure as a service provider, rather than build it [8]. And thus is designed layers service provider cloud by SaaS layers on top of IAAS. In this type of multi level order of the service provider, shares of each of the risk of security problems because the threat may have effects on all parties in all classes.

- **Coding**

We inform to every client, the coding had followed by protected practices in the cloud provider [7]. Also, you must write all the code using a technology standard that is documented and can be demonstrated on the client.

- **Data Leakage**

Must have a cloud computing project the ability to map the structure of the framework of policies to protect customers must comply with, and to discuss this issue. At a minimum, the data should be secured under consideration. Cloud provider needs also to be a strategy that feed the costumer protection occurrence protection policy to deal with any data leakage that can happen [9].

2.6. The major Technology of cloud computing security:

The factors below are supported by Natural Science Foundation of Shandong Province of China (2011)[8]

2.6.1. Trusted Access Control

Researchers have more concerned in cloud computing modules, so It can not completely trust the service providers. So, how we can implement access control with object data access control with non-traditional. Which means to obtain more attention, and which are depend on encryption techniques to manage and easy access, and include: focused on the establishment of key hierarchy and strategy to provide management technique for the disabled; standards-based encryption feature, based on proxy re-encryption method and access management technology shrub ensures that the key username or revision and so on.

2.6.2. Retrieval and Processing of the Cipher-text

Some features will be lost when data goes into cipher text, as a result of the data analysis technique failure. There are many techniques of cipher text to recovery: Depending on the mode index of security and protection through the development of the revision index search phrases, retrieves keyword index exists, this approach will compare every word and confirm if there are the keywords, and their own statistics.

The design of cryptographic secret which depend on homomorphic algorithm. In the beginning of the eighty decade, the homomorphism was suggested from a variety of add or algorithm homomorphism beating , but it turned out the existence of a safety problem , and Follow-up in the event of an interruption in, and there is still a long distance Practically.[8]

2.6.3. Protection of data privacy

The data life cycle have concerned about data privacy protection on the cloud on each level. In the phase of the data generation and computation, the central information , flow control and distinctive privacy protection technology had integrated by Roy, and it has come up with system of privacy, prevented leakage of the Illegality data privacy in the process of computing calculations, and supported the density as a result of the expense by the automatic addition. Mowbray said, Privacy and management tools based on the client, and the introduction of confidence-centric model used to help users to control data storage and use of sensitive information on the cloud.

Munts Mulero shows, Privacy technologies treatment of pre-existing, which containing anonymous, as anonymity, and processing data, that there is a massive problem will be facing, when data had published, and some existing solutions. Rankova proposed, Search provided by Interactive Data Search Engine anonymous. It can make the search an interactive database with each other, and they need to get aspects, while ensuring that the query search was not known on the versus side.

2.6.4. Virtual Technology Solution

Virtual solution is one of the best techniques to distinguish the cloud computing services. Cloud computing model depends on virtual technology solution on cloud architecture by cloud providers to introduce a security and isolation data to his customers.

Isolation actuators provides by Santhanam based on virtual machines under the grid environment security and performance provides by Raj with realize separation by two of the resource management techniques. first, distribution of basic with cache level, Second, Partitioned cache with page of dyeing.

The writers supports Wei in his insight about the security problem in virtual technology image file. Because of it's have a high level of integrity. It's assist to solve many problems i.e. access control, security breach, source tracking, filtering and it's easy to detect data from attacking.[8]

2.6.5. Trusted technology

Trusted solution has become a big matter into cloud environment where provide IaaS trustworthy manner, nowadays trust has become a hot environment of research because of a lot of security issues.

Santos suggested TCCP of cloud computing platform trustworthy. It provides a box-type environment, the implementation of closed based on this platform, IAAS service provider ensures confidentiality of the guest virtual systems running. In addition, IAAS service provider of secure service introduced to allows the user to start by virtual machine. Trusted hardware and software has provided by trusted computing technology. Sadeghi believes that trusted design the credibility of the symbolic software, under Security briefing model authentication, It is under non-disclosure of any information, as well as it's proving itself a credible method. it can be perform various functions to be data confidentiality and integrity with sensitive operation as data encryption. to solve outsourcing of data. [8].

3. Problem statement:

There are many problems and challenges face the cloud computing providers and the cloud clients. Therefore, data have to be isolated to avoid data leakage.

This paper suggests that to protect cloud computing, the service providers should secure data first. overall, companies should defending their information, it is very important to classify their data to know what guidelines they must adhere to secure them:

- Its sensitivity to handled at a specific trust levels.
- Determine what stage of protection they need. Different design in cloud offers various levels of business.
- Identify what kinds of information and procedures to move to the cloud. [9]

4. Research model:

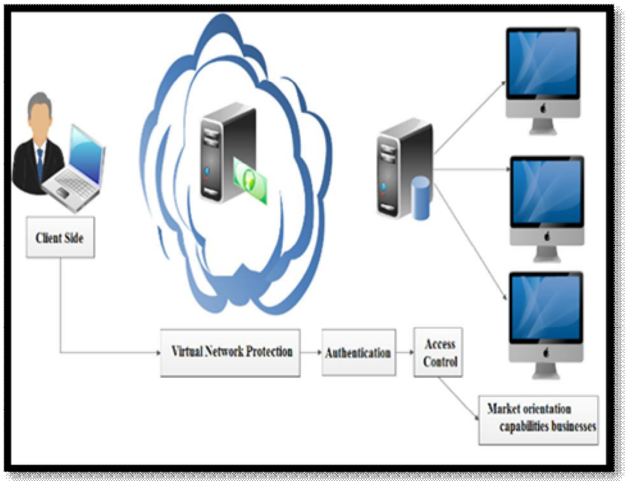
The model suggests that cloud computing facility should be created by the service providers by incorporating the requirements of the business.

To co-create value for sustainability, organizations need to take a more extensive view of the surroundings in which it competes. There is a need for the corporation to make and sustain resource alignment abilities that allow collaborating firms to develop "solution" to business problems that customers will value (Teece, 2010)[11].

Cloud system structure used to convey the Iaas include software and hardware habitant in the cloud. Although there are several perspectives, they all share the same core elements, namely: People, Procedures and Technology. Organizations of all sizes across nearly every industry are investigating new ways to address their business. Cloud computing provides many alternatives to the problems had faced.

The authors have developed a conceptual framework for co-creation of value for business. The dynamic ability value co-creation framework should involve of the following capabilities:

- Client-Side Security abilities
- Virtual System Security capabilities
- Authentication Business capabilities
- Management of cloud services abilities (Access Control)
- Market alignment abilities businesses


Client Side
Virtual Network Protection
Authentication
Access Control
Market orientation capabilities businesses

(Fig 1. Framework for Co-creation of Value on IT Business in cloud computing)

Data will be stored in the cloud which has built in a distributed environment with others data client. As the enterprises are moving delicate data, it have to be ensured that the data can only be used by authorized persons showing proper authentication so the data remains safe from any unauthorized users.

4.1. The proposed model:

The proposed model provide universal service to the customers, with a high level of trust to be trustworthy on the customers. like,

- Client-Side Security abilities:

A successful protection against strikes needs both a protected customer and a secure Website infrastructure. The Browsers was be an important element in a cloud environment. Because of plug-ins and extensions for them are disreputable for their security issue [12]. Moreover, many web browser add-ons do not offer automatic up to dates that increases vulnerabilities.

- Virtual System Security capabilities:

Virtualization systems consist of switches and hubs on network, that is configured as part of the virtual environment. they have the ability to create software which allow VMs to connect directly immediately and efficiently effectively "For example, VMware virtual network infrastructure that supports the same networks that host subnet is created especially for VMS does not require access to the external network". Security protection devices can not noticeable the traffic over networks, such as matching attack network-based and firewall protection. This model provide or avoid a lack of protection against attacks to services providers in cloud computing, by create virtual network to make duplication of the actual protections. [12].

- Authentication:

Most of cloud service providers endure the (SAML) Security Assertion Markup Language and use it to manage customers and verify previously so offering accessibility to platforms and information. SAML introduce techniques for data exchange, such as motivation regarding on a matter or verification information among participating websites [10].

- Access Control:

Besides documentation, required the ability to get privileges to users and maintain control over access to resources as well, as part of the identity management. Criteria such as language and access control extensible Markup (XACML) can be used to control access to cloud resources, rather than using the interface property service provider. XACML concentrates on the procedure for reaching at permission resolutions, which enhances SAML's focus on the means for shifting verification and permission resolutions among the entities involved. XACML is able to managing Service Interfaces property for most suppliers, and some cloud companies, such Amazon.com and Google Apps. This is already in position. Messages was be attacked when it passed among XACML entities because of his vulnerable and it is harmful by third parties, Which makes it important to be safety scales in position to protect resolutions demands and permission resolutions from potential offensives, through illegal detection, replay, removal and adjustment [12].

- Data Isolation:

This model proposed data isolation to keep database integration and safety from outside attack or illegal users. This tool working with the structure of virtual system to get users a factual system after the access control stage was done. This techniques means to keep data away from illegal users, by encryption. even customers, finish his own process to buy from the cloud portal. After the system analyze the entities records from client to inform on this is a real purchase. Then the system moved from virtual system to a real one to make the business process are safety. So the system can book a goods and up-date the database repository.

4.2. Cloud Goals in this model:

These goals will be accomplished through a cloud investment strategy:

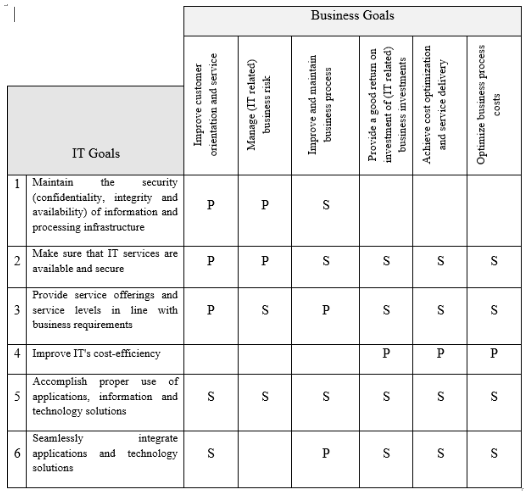
- Reduce the costs to subscribers companies.
- Introduce another IT solutions through the virtual system to confirmed best practice procedures
- Improved client satisfaction through to make duplication of the actual protections.
- Standards authentication and guidance
- Improved performance
- Improved the services abilities
- Make a business value

4.3. Business Processes:

A business procedure is a organized set of activities developed to generate a particular outcome or accomplish a goal. This implies a high emphasis on how work is performed within an organization, in contrast with the product approach in which the emphasis is on what is created. Therefore, the procedure is a specific sequence of perform activities through time and area, with a beginning, an end, and clearly assign inputs and outputs

4.4. Business/It alignment in cloud security model:

A relational procedure that enable both IT people and business to achieve their liabilities in endure of business/IT alignment to create value from information technology to inform business investments. [13]



		Business Goals					
	IT Goals	Improve customer orientation and service	Manage (IT related) business risk	Improve and maintain business process	Provide a good return on investment of (IT related) business investments	Achieve cost optimization and service delivery	Optimize business process costs
1	Maintain the security (confidentiality, integrity and availability) of information and processing infrastructure	P	P	S			
2	Make sure that IT services are available and secure	P	P	S	S	S	S
3	Provide service offerings and service levels in line with business requirements	P	S	P	S	S	S
4	Improve IT's cost-efficiency				P	P	P
5	Accomplish proper use of applications, information and technology solutions	S	S	S	S	S	S
6	Seamlessly integrate applications and technology solutions	S		P	S	S	S

(Figure 2, Business/IT goals)

The authors said, the results of the model was thorough understanding of the goals of information technology and business goals and how to connect. This paper contains detailed findings on how the goals of information technology can support business goals. Figure 2, shows in a matrix how the goals of information technology are relevant to business goals. For example, the IT goal "Make sure that IT services are available and secure" does prop all business goals in a primary (P) or a secondary manner (S). And IT goal "Accomplish proper use of applications, information and technology solutions" does prop all business goals in a secondary (S) manner. And the IT goal "Improve IT's cost-efficiency" does prop some business goals in a primary manner (P). [13].

The outcomes of this paper provide authentic guidance. The writers focus in the correlation between the security problem and the trust to enhance build up business goals and the goals of information technology for a particular enterprise and this way you get the best participate in the business/IT alignment issue.

5. Conclusion:

This model attempt to permitted by a virtualization part will provide a provide duplication of the actual protections to make a better market and a safety environment. The system appliances will help simplify this conversion. Cloud computing, in synchronism with virtualization software to keep data far from illegal users, and will also create new business designs that will enable providers to offer a single product on the premises, on demand, or in a hybrid deployment pattern. While it is necessary to begin understanding the new characteristics that will begin to appear to offer application and components to end customers.

From author's perspective, to protect cloud computing, the service providers should secure data first. Overall, companies should defending their information, and then protected the infrastructure. In this aria, the authors developed model to kept data from leakage and secure it on cloud computing.

6. Acknowledgements:

We would like to thank our Prof. Dr. Mohd Adam Suhaimi for his kind assistant and great contribution in this research.

7. References

1- Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R., Lee, G., Patterson, D., Rabkin, A., Stoica, I., Konwinski, A., & Zaharia, M., (2010). A view of Cloud Computing. Communications of the ACM, 53 (4), 50-58.

2- Low, C., Chen, Y., & Wu, M. (2011). Understanding the determinants of cloud computing adoption. Industrial Management & Data Systems, 111(7), 1006–1023.

3- Barber, H. H., Lawler, J., Desai, S., & Joseph, A. (2012). A Study of Cloud Computing Software-as-a-Service (SaaS) in Financial Firms. Education special interest group of the AITP, 5(2205), 1–14.

4- Joseph, A., Kim, P., & Wu, P. (2013). Information Systems Applied Research Special Issue: Cloud Computing In this issue, 6(3), 1–33.

5- Bisong, A. (2011). AN OVERVIEW OF THE SECURITY CONCERNS IN, *3*(1), 30–45.

6- Wang, C., Chow, S. S. M., Wang, Q., Ren, K., & Lou, W. (2013). Privacy-Preserving Public Auditing for Secure Cloud Storage. Institute of Electrical and Electronics Engineers (IEEE), 62 (2), 1–12.

7- Wang, C., Wang, Q., Ren, K., & Lou, W., (2009). Ensuring data storage security in Cloud Computing. International Workshop on Quality of Service, 1–9.

8- Ming, T., & Yongsheng, Z., (2012). Analysis of Cloud Computing and Its Security. Information Technology in Medicine and Education (ITME), 1, 379–381.

9- Hamouda, S., (2012). Security and privacy in cloud computing. *Cloud Computing Technologies, Applications and Management (ICCCTAM)*, 241–245.

10- Zissis, D., & Lekkas, D., (2012). Addressing cloud computing security issues. Future Generation Computer Systems,28(3),583–592.

11- Teece, D. J. (2010). Business Models, Business Strategy and Innovation. Long Range Planning, 43(2-3), 172–194.

12- Jansen, W. a., (2011). Cloud Hooks: Security and Privacy Issues in Cloud Computing. *Hawaii International Conference on System Sciences*, 1–10.

13- Van, G. W., & De, H. S. (2008). Enterprise governance of information technology: Achieving strategic alignment and value. New York: Springer.

14- Edwards, J. (2009). Cutting through the fog of cloud security. Computerworld. Framingham: 43, (8), 3-26

15- Francis, T., & Vadivel, S. (2012). Cloud computing security: Concerns, strategies and best practices. Cloud Computing Technologies, Applications and Management (ICCCTAM), 205–207.