International Journal of Trend in Scientific Research and Development (IJTSRD)
Volume 3 Issue 5, August 2019 Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470

Risk Management of Secure Cloud in Higher Educational Institution

Moe Moe San[1], Khin May Win[2]

[1]Faculty of Computer Science, [2]Faculty of Information Science,
[1,2]University of Computer Studies, Pathein, Myanmar

How to cite this paper: Moe Moe San | Khin May Win "Risk Management of Secure Cloud in Higher Educational Institution" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-3 | Issue-5, August 2019, pp.1314-1319, **https://doi.org/10.31142/ijtsrd26638**

IJTSRD26638

ABSTRACT

Cloud Computing is one of the most widely used today in higher educational institutions and other business organizations. It provides many advantages for higher educational institutions by sharing IT services on cloud. However, a cloud provider needs to manage the cloud computing environment risks in order to identify, assess, and prioritize the risks in order to mitigate those risks, improve security and confidence in cloud services. Risk assessment is a core of risk management, estimates and prioritizes risks to reduce their impact and maximize the benefits of cloud computing for higher educational institutions. Fuzzy Logic is adopted to deal with insufficient information and estimate the severity and the likelihood of each risk mathematically. The proposed framework identifies the security risk factors for higher educational institution in cloud computing and how to measure and evaluate based on Fuzzy Logic. It can improve the accuracy and efficiency of cloud security risk assessment on the basis of previous research results.

KEYWORDS: *Cloud Computing; Risk Management; Security; Fuzzy Logic; Higher Educational Institution*

I. INTRODUCTION

The use of cloud computing in institutions of higher learning has provided many benefits to universities and colleges. The cloud helps ensure that students, teachers, faculty, and staff have on demand access to critical information using any device from anywhere.

Even though the great benefits of using cloud in higher educational institutions, there are some challenges that hinder the wide scale adoption of this technology in various sectors of the universities.

The key benefits of cloud in education can be categorized according to stakeholders who use cloud resources and services in higher educational sectors. Students can store anything electronically such as their schedule, class notes, reports and any other documents. Students have the opportunity to access the system easily at any time to get courses online, attend the online exam, and upload their assignments and projects through the cloud to the instructors.

Organizers in educational sectors are wishing to use cloud services that are not radically different from those services that totally managed within their own centers. However, they are in fact facing a range of substantial new challenges. Challenges in higher educational institutions, need to investigate various aspects of cloud challenges such as threats, risks, and attack models. Challenges in cloud computing are categorized into four main aspects; Network, Access control, Cloud infrastructure, and Data Security. With regard to the risks of network security in a cloud environment, hacking and intrusion are increased.

Access Control includes important security issues such as authentication, identification, and authorization. Data Security risks constitute the biggest challenge for adopting cloud computing in higher educational institutions.

Cloud computing being a novel technology introduces new security risks that need to be assessed and mitigated, consequently, assessment of security risks is essential, the traditional technical method of risk assessment. In higher educational institutions, security and privacy requirements, Attacks on cloud, threats to cloud computing and risks & security concerns are demanded on research work. Fuzzy Logic is widely used in various areas of Cloud Computing. Risk assessment and prioritization in Cloud Computing is very much essential to reduce and manage the risk and to enjoy the unlimited services of Cloud Computing. The proposed framework will identify the security risk factors for higher educational institution in cloud computing and it will estimate the risk rate with probability and impact of risk by using Fuzzy Logic.

This paper will be organized as follows. In section II, mention the literature review of previous papers. Section III will provide an overview of cloud computing, risk management and Fuzzy Logic. Section IV will present identification of risk factors in higher educational institution and section V proposed risk management framework using Fuzzy Logic based on literature review. Finally, section VI will conclude for this paper.

II. LITERATURE REVIEW

The security challenges and risk assessment are one of the main topics that recently researchers focus on for adopting cloud computing in educational sectors. Various researchers presented risk analysis frameworks and methods to reduce cloud risks to improve cloud performance for cloud consumers.

The work in [1] provided a framework gives guidelines on most of the aspects of secure clouds including: security and privacy requirements, attacks and threats that clouds are vulnerable to and risks and concerns about cloud security. The author proposed a generic security model for cloud computing that helps satisfy its security requirements.

In [2] the authors reviewed the literature on challenges of adoption cloud computing in institutions and universities. It also presented an overview of the security issues in the cloud service models and discussed the security challenges and risks and then provides helpful recommendations to avoid security challenges efficiently for adopting cloud computing in higher educational institutions.

The authors in [3] proposed a framework aims to treat the security issues by establishing a relationship among the cloud service providers in which the data about possible threats can be generated based on the previous attacks on other providers.

The authors in [4] provided a systematic review of the previously proposed risk management frameworks for cloud computing environments. It also presented the advantages and disadvantages of the previous risk management frameworks on cloud computing.

In [6], the authors described that Cloud-based model could be more robust, scalable and cost-effective and would Manage risk very well with the use of fuzzy Logic. The authors used three fuzzy inputs like Gracefulness, Processor – speed and Performance as fuzzy input to find out Trust Rating rate and get better result of performance.

The authors in [8] proposed a risk assessment method through a combination of Analytical Hierarchy Process (AHP) methodology and Mamdani fuzzy inference algorithm. This method provided federation of clouds without consideration identity federation based on risk assessment technology. In this method, input risk factors assigned to the decision block are described by the fuzzy sets, such as low, medium, high and some of the risk factors have a differently weighted role in the system. First of all, weighted factors are forwarded to the input of the decision-making system; weighted rules are established on these factors and obtained results forwarded to the next phase of the inference process. The aim of this proposed method is to forward a weighted input vector to the system. Limitation of this method is cannot be used in risk assessment process of all kinds enterprises, which have necessity hierarchical risk assessment.

In [11] the authors focused on a specific aspect of risk assessment as applied in cloud computing: methods within a framework that can be used by cloud service providers and service consumers to assess risk during service deployment and operation. It described the various stages in the service lifecycle where risk assessment takes place, and the corresponding risk models that have been designed and implemented. The impact of risk on architectural components, with special emphasis on holistic management support at service operation, is also described. The risk assessor is shown to be effective through the experimental evaluation of the implementation, and is already integrated in a cloud computing toolkit.

The aim of the authors in [12] is to propose a framework for assessing the security risks associated with cloud computing platforms. The fully quantitative, iterative, and incremental approach enables cloud customer/provider to assess and manage cloud security risks. It resulted of risk assessment leads to have appropriate risk management mechanism for mitigating risks and reach to an acceptance security level.

III. FUNDAMENTAL CONCEPTS

A. Cloud Computing

Cloud computing is one of the most rapidly growing areas in information technology. The key benefits of cloud computing in higher education can be categorized according to stakeholders who use cloud resources and services in higher education institutions. Students can store anything electronically such as their schedule, class notes, reports and any other documents. Furthermore, they able to back up their files to the cloud and retrieve them when needed. Students can earn e-copy of textbooks and have access to quality learning materials of their courses.

There are many definitions for cloud computing in the literature. The National Institute of Standards and Technology (NIST) defined cloud computing as : *"a 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) that can be rapidly provisioned and released with minimal management effort or service provider interaction"* [1]. NIST also defines three service models, *Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS).*

SaaS provider hosts and manages a given application in their data center and makes it available to multiple users over the Web. Oracles CRM on Demand, Salesforce.com are some of the well-known SaaS examples.

PaaS is an application development and deployment platform which delivered over the web to developers. PaaS facilitates development and deployment of applications without the cost and complexity of buying and managing the underlying infrastructure. All of the facilities required to support the complete life cycle of building and delivering web applications and services entirely available through Internet. This platform includes a database, middleware, development tools and infrastructure software. Well-known PaaS service providers include Google App Engine, Engine Yard.

IaaS is the delivery of hardware and software as a service. It is an evolution of traditional hosting that does not require any long term commitment and allows users to provision resources on demand. Amazon Web Services Elastic Compute Cloud (EC2) and Secure Storage Service (S3) are examples of IaaS services [10].

Cloud computing deployment models were defined by NIST and classified into four common modes; private, public, hybrid and community clouds.

Private cloud is deployed inside the boundary of the organization and is provisioned for exclusive use by specific consumers, its data and services cannot be accessed from outside of an organization.

Public cloud is owned and managed by a business, academic, or government organizations that provide cloud services for open use to the public.

The hybrid cloud is a composition of both public and private clouds characteristics.

In the community cloud, the infrastructure and services are provisioned for use by the specific community of consumers or among several organizations that have same mission or target. It can be operated and managed internally in the community or by a third party [17].

B. Risk Management

The involvement of consumers on cloud computing in the risk management process is important because they are the only ones who know the value of their assets. Consumer participation should not be limited to the extent of inactivity, complicating the process. Risk identification (sub-processes of risk assessment) is critical processes in risk management based on rule based Fuzzy Logic. Risk assessment process is significant due to the fact of the problem such as failure is a key part of learning. Each of the provided services separately is needed to handle conflicts in the consumers' security requirements, due to the multi-tenancy feature of cloud computing.

The most central concepts in risk management are the following: an *asset* is something to which a party assigns value and hence for which the party requires protection. An *unwanted incident* is an event that harms or reduces the value of an asset. A *threat* is a potential cause of an unwanted incident whereas vulnerability is a weakness, flaw or deficiency that opens for, or may be exploited by, a threat to cause harm to or reduce the value of an asset. An unwanted incident and its consequence for a specific asset, risk. The level or value of a risk derived from its likelihood and consequence.

A fundamental issue in the characterization and representation of risk is to properly and appropriately carry out the following steps:

- Analyze the triggering events of the risk, and by breaking down those events formulate adequately their accurate structure.
- Estimate the losses associated with each event in case of its realization.
- Forecast the probabilities or the possibilities of the events by using either statistical methods with probabilistic assessments, or subjective judgments with approximate reasoning.

After the possible risks have been identified, they are assessed in terms of their potential severity of loss and probability or possibility of occurrence. This process is called *Risk Assessment (RA)*. The input quantities for Risk Assessment can range from simple to measurable (when estimating the value of a lost asset or contracted penalty associated with non-delivery) to impossible to know for certain (when trying to quantify the probability of a very unlikely event). *Risk Management (RM)* is the process of measuring or assessing risk and on the basis of the results developing strategies to manage that risk and control its implications. Managing a type of risk includes the issues of determining whether an action or a set of actions - is required, and if so finding the optimal strategy of actions to deal with the risk. The actions applied in a comprehensive strategy consist of an appropriate combination of the following measures:

- Transferring the risk to another party.
- Avoiding the risk.
- Reducing the negative effects of the risk, and
- Accepting or absorbing some or all of the consequences of a particular risk [11].

C. Fuzzy Logic

Fuzzy Logic provides a simple way to arrive at a definite conclusion based upon vague, ambiguous, imprecise, noisy or missing input information. The type of logic matters more than the simple true or false values. Zadeh, proposed the fuzzy logic in 1965; as it has the ability to deal with imprecise as well as incorrect information, it is now used widely. The human expertise is embedded in the system as the fuzzy logic is very close to the human mind. In various fields such as washing machines, image processing, microprocessors, air conditioners and microcontrollers, fuzzy logic has been widely used. Having the ability of handling the inaccurate inputs there is a fuzzy inference that has been used widely for the solving of the control along with the problems of reasoning in the environments that are uncertain. There are also three other major components for a typical inference model:

The Inference Engine: this defines all fuzzy logic operators with their defuzzifier that has been used in the inference process.

The Membership Functions: this degree of the fuzzy element will belong to its corresponding fuzzy set that has been defined in the membership function. The mapping of the crisp values to their degrees of membership which can vary between that of 0 and 1 and each input and output variable will have a similar set of the membership functions.

Rule base: The inference model that is defined by the "If-Then" rule comprises this set. The "AND" or "OR" operators connect the antecedent and consequent fuzzy propositions in "If antecedent Then consequent". This is how a rule structure looks like. There are 5 main steps in the inference procedure:

A. Fuzzification: For obtaining the corresponding membership degrees of every input variable, with regard to particular fuzzy set, input crisp values into membership functions.
B. The applying of Fuzzy Operations: this is for obtaining the membership of degree for the antecedent using the "AND" and the "OR" operators.
C. Implication: Use the defined implication operator for obtaining the fuzzy set of each and every rule.

D. Aggregation: an aggregate of output fuzzy sets for all the rules that make use of a defined aggregation operator.
E. Defuzzification: using a defined defuzzification algorithm that is for transforming all the collected fuzzy set within a crisp value. The inference of fuzzy logic flows from an input variable to all the output variables. The analog inputs have been translated into that of fuzzy values using the fuzzification in their input interfaces. These rule blocks a compromise of the rules of linguistic control in which a fuzzy inference will take place and the linguistic variables will be the outputs of this particular rule block.

IV. IDENTIFICATION OF RISK FACTORS

According to previous discussed different security levels that an organization must have are explained below:

Personnel Security*:* With personnel security an organization appoint authorized individual or group of individuals for accessing and allocating all the organization resources and data.

Eavesdropping: An unauthorized user can access the data because of interception in network traffic; it may result in failure of confidentiality. The Eavesdropper secretly listen the private conversation of others. This attack may be done over email, instant messaging.

Information Security: With information security an organization can safeguard and protect the confidentiality and correctness (integrity) and assets information for processing and storage.

Physical Security: With this security an organization can protect its physical assets and other essential properties from unauthorized access and misuse.

Network Level Security: With network security an organization protects its networking components & connections. It also protects organization contents that are transferred through networks.

Operations Security: With operational security an organization protects the information of all transactions and operations performed regularly.

Communications Security: With communication security an organization protects various technologies, communications media and their content from unauthorized access.

The literature noted a number of concerns about managing security and privacy in cloud computing. In [1] some concerns are:

Access control: how can cloud users govern access control risks when the levels and types of access control used by cloud providers are unknown?

Monitoring: how can accurate, timely and effective monitoring of security and privacy levels achieved in business-critical infrastructure when its providers are not prepared to share such information at SLA?

Applications development: how to accomplish application development and maintenance in the cloud when CSPs are responsible to?

Data retentively: how can the cloud user achieve appropriate confidence that the data have been actually and securely removed from the system by the cloud provider and are not merely made inaccessible to him?

Testing: how can consumers test the effectiveness of security control when these tests may not be made available by CSPs?

Physical access control: how can the cloud user achieve requirements for physical access when its measures are established and fully controlled by CSPs?

Incident management: how can the cloud user determine appropriate thresholds and criteria in order to respond to incident?

The International Standards Organization (ISO), in ISO7498-2 [1], suggested a number of information security requirements, they are

Identification and Authentication management: The authentication and identity management module is responsible for authenticating users and services based on credentials and characteristics. In the cloud computing, with this security principle we must identify the client making requests and their access privileges. If any client is not assigned to any service then he is denied for that service. The client authentication by username and password are also validated before accessing to any cloud service. The identification and authentication is the essential security principle for all types of clouds.

Access control: Access Control includes important security issues such as authentication, identification, and authorization. Authorization preserves referential integrity in cloud environment. With this rule only authorized person access the cloud resources. All the unauthorized persons are denied for cloud services and resources .It can resolve authorization issue in cloud environment is to establish a solid confidence between Cloud Service Providers (CSPs) and customers who should both trust cloud administrators as well.

Confidentiality: Confidentiality is a core requirement to maintain control over the data of many organizations that may be located across several distributed databases. Emphasizing confidentiality and protection of users' data and profiles at all levels will enforce information security principles at different levels of cloud applications.

Integrity: refers to protecting cloud data and software from unauthorized deletion, modification, theft or fabrication, this ensures that data has not been tampered with or abused. Integrity includes data accuracy, completeness and ensures Atomicity, Consistency, Isolation and Durability (ACID).

Non-repudiation: With this principle security of cloud data is maintained by some Security protocols and token provisioning for transmission of data on cloud server to client and vice versa. To maintain non-repudiation different

concepts are applied such as digital signatures, confirmation acknowledgement etc..

Availability: Another cloud security principle is availability of cloud vender. It refers to cloud data, software and also hardware being available, usable and accessible to authorized users upon demand. CSPs should be able to continue providing customers with services even in case of the existence of security breaches, malicious activities or system faults. Availability is an important factor in choosing among various CSPs.

Compliance and Audit: compliance with regulations and laws is a necessary privacy requirement to ensure that the cloud deployment meets the requirements of general legislation, sector-specific rules and contractual obligations.

Transparency: the operation of the cloud should be sufficiently clear to users and CSPs. Users must be able to get a clear overview of where and how their data will be handled. They also must be able to determine who the cloud provider is and where his responsibility ends.

Governance: data on the cloud is vulnerable since it is processed and stored remotely. Customers have concerns about why their personal information is requested and who will use it. Governance ensures protecting data against various malicious activities and helps control cloud operations.

Accountability: implies that security and privacy gaps are correctly addressed [10].

V. PROPOSED FRAMEWORK USING FUZZY RULE BASED

This proposed framework is the principal step to identify the risk factors as internal and external factors for secure cloud. And analyze the risk to evaluate the probability of that impact and to measure risk attributes and to output results using fuzzification with rule based. This framework would focus on security challenges in cloud computing and to have highly protected, safe and sound cloud computing in higher educational institution. This framework is summarized as follows:

A. Data collection

Data extraction from educational data of public cloud computing. This dataset contains various risk attributes.

B. Identification each Risk Factor

Determine on risk factors and security concern on cloud computing such as Access Control, Monitoring, Data retentively, Testing, Physical access control, Incident management etc.

C. Fuzzification with Rule Based

Determination of main parameters is necessary for risk assessment in this step. The measure of each parameter is used by linguistic terms and transforming to the appropriate fuzzy number.

D. Weight age Assignment to each sub category

Weight age would be assigned randomly to the risk attributes.

E. Analysis of result

Apply the fuzzy rule based system to the risk attributes and their results are categorized in Very Low, Low, Medium, High and Very High.

1. Fuzzy Rule Based

Considering the input parameter x from the universe X, and the output parameter y from the universe Y, the statement of a system can be described with a rule base (RB) system in the following form:

Rule1: IF x=A1 THEN y= B1
Rule2: IF x=A2 THEN y= B2
Rule n: IF x=An THEN y= Bn ,

This is denoted as a single input, single output(SISO) system
If there is more than one rule proposition, i.e. the ith rule has the following form

Rule i: IF x1=A1i AND x2= A2i…THEN y=bi
Then, this is denoted as a multi input, single output (MISO) system.

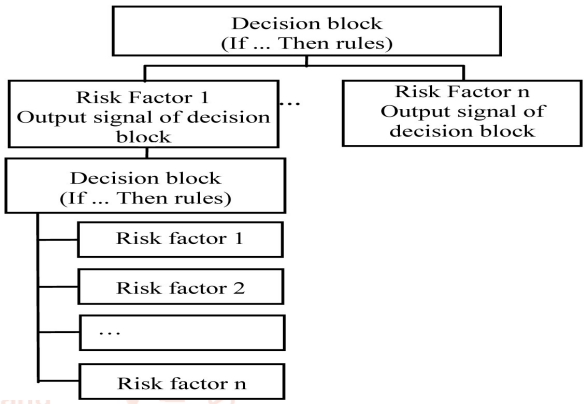
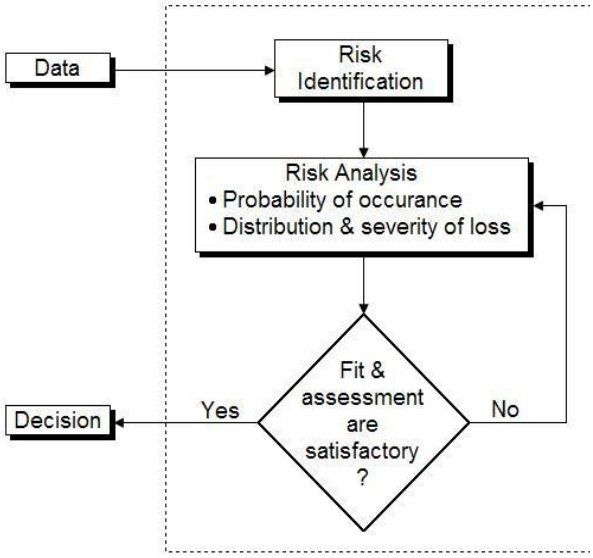


Figure: Hierarchical risk management structure.

2. Risk Management Flow Chat



VI. Conclusion

This paper focused on risk management/assessment of secure cloud in higher educational institution. It presented identification of cloud risk factors and analysis for measurement of risk attributes. Cloud computing represents an opportunity for higher educational institution to take the enormous benefits of cloud services and resources in the educational process. However, the cloud users remain concerned about the major obstacle that may prohibit the

adoption of cloud computing on a large scale. This will lead to many security issues such as privacy, confidentiality, integrity and availability etc. Thus, more matured risk management frameworks need for cloud security. Fuzzy Logic is applied to provide the performance of cloud computing for the risk assessment evaluation method with new features than previous methods. Fuzzy rule based management would provide mitigations of risks on cloud computing in higher educational institution.

References

[1] Ahmed E. Youssef, Manal Alageel, "A Framework for Secure Cloud Computing", *International Journal*, International Journal of Computer Science, KSA, *July 2012*, *ISSN1694-0814*

[2] Khalil H. A. Al-Shqeerat, Faiz M. A. Al-Shrouf., "Cloud Computing Security Challenges in Higher Educational Institutions-A Survey", *International Journal*, International Journal of Computer Applications (0975 – 8887), Germany, , *March 2017*, *Volume 161 – No 6*

[3] Atif Ishaq, Muhammad Nawaz Brohi, "Cloud Computing in Education Sector with Security and Privacy Issue", *International Journal*, International Journal of Advances in Engineering & Technology, UAE, *December 2015*, ISSN: 22311963

[4] Rana Alosaimi, Mohammad Alnuem, "Risk Management Frameworks for Cloud Computing: A Critical Review", *International Journal*, International Journal of Computer Science & Information Technology , Saudi Arabia, , *August 2016*, *Volume 8 – No 4*

[5] Jun.Liu, Zuhua Guo, " Research on Cloud Security Risk Assessment based on Fuzzy Entropy Weight Model", Advanced Science and Technology Letters Vol.139 (EEC 2016), pp.390-395

[6] Rachna Satsangi, Dr. Pankaj Dashore,Dr.Nishith Dubey, "Risk Management in Cloud Computing Through Fuzzy Logic", International Journal of Application or Innovation in Engineering & Management (IJAIEM), Volume 1, Issue 4, December 2012, ISSN 2319 – 4847

[7] Anjali Kinra, "Risk Assessment of Multiple Factors using Fuzzy Logic", International Journal of Computer Science and Mobile Computing, Vol.4 Issue.7, July-2015, pg. 464-475, ISSN 2320–088X

[8] Rasim Alguliyev, Fargana Abdullayeva, "Development of Fuzzy Risk Calculation Method for a Dynamic Federation of Clouds", Scientific Research Publishing Inc., Intelligent Information Management, 2015, 7, 230-241

[9] Drissi S. Houmani H. Medromi H., "Survey: Risk Assessment for Cloud Computing", International Journal of Advanced Computer Science and Applications (IJACSA), *Vol. 4, No. 12, 2013*

[10] Moe Moe San, Khin May Win, "A Framework for Secure Cloud Based Computing in Higher Educational Institution", 16th International Conference on Computer Applications 2018 (ICCA, 2018),22-23 February, 2018, pg 19-27.

[11] Djemame, K orcid.org/0000-0001-5811-5263, Armstrong, D, Guitart, J et al. A Risk Assessment Framework for Cloud Computing. (2016) IEEE Transactions on Cloud Computing, 4 (3). pp. 265-278. ISSN 2168-7161

[12] Alireza Shameli-Sendi and Mohamed Cheriet Synchromedia Laboratory for Cloud Computing E´cole de technologie supe´rieure Montreal, Canada, "Cloud Computing: A Risk Assessment Model", 2014 IEEE International Conference on Cloud Engineering, 978-1-4799-3766-0/14 $31.00 © 2014 IEEE DOI 10.1109/IC2E.2014.17

[13] Erdal Cayirci, Alexandr Garaga, Anderson Santana de Oliveira, Yves Roudier, "A Cloud Adoption Risk Assessment Model" , 2014 IEEE/ACM 7th International Conference on Utility and Cloud Computing, 978-1-4799-7881-6/14 $31.00 © 2014 IEEE DOI

[14] Jing Li, Qinyuan Li , " Data security and risk assessment in cloud computing " , ITM Web of Conferences **17**, 03028 (2018)

[15] Prasad Saripalli, Ben Walters, "A Quantitative Impact and Risk Assessment Framework for Cloud Security", 2010 IEEE 3rd International Conference on Cloud Computing, 978-0-7695-4130-3/10 $26.00 © 2010 IEEE DOI 10.1109/CLOUD.2010.22