A Scenario-Based Methodology for Cloud Computing Security Risk Assessment

Prof. Hany Ammar, Ishraga Mohamed Ahmed Khogali

Abstract

Cloud computing has been one of the major emerging technologies in recent years. However, for cloud computing, the risk assessment become more complex since there are several issues that likely emerged [1]. In this paper we survey the existing work on assessing security risks in cloud computing applications. Existing work does not address the dynamic nature of cloud applications and there is need for methods that calculate the security risk factor dynamically. In this paper we use the National Institute of Standards and Technology (NIST) Risk Management Framework and present a dynamic scenario-based methodology for risk assessment. The methodology is based using Bayesian networks to estimate likelihood of cloud application security failure which enable us to compute the probability distribution of failures over variables of interest given the evidence. We illustrate the methodology using two case studies and highlight the significant risk factors. We also show the effect of using security controls in reducing the risk factors.

1. Introduction

Cloud computing is a new technology that provide real promise to business with real advantages in term of cost and computational power. Cloud computing depends on complex architectures that allow providers to deliver different services in different models such as software-as-a-service (SaaS), which allows cloud customers to process and use licensed software on the cloud providers' resources only. The cloud services can also be provided as platform-as-a-service (PaaS) which lets the consumers to rent only a platform that gives more control to the consumer to configure it as needed. The last model is infrastructure-as-a-service (IaaS), which provides the consumers with a complete infrastructure where they deploy different machines and storage resources[1].

However, it's important to consider security and data protection when it comes to widespread cloud adoption [2] because cloud computing raises severe security concerns that existing in traditional system as well as issues that appear to be specific to that domain. Although most of these concerns are not new, already exist in traditional IT environment, they need more consideration because of the dynamic nature of cloud computing platform. The National Institute of Standards and Technology (NIST) defines the IT risk as "the net mission impact considering (1) the probability that a particular threat-source will exercise (accidentally trigger or intentionally exploit) particular information system vulnerability and (2) the resulting impact if this should occur" [1].

Security risk assessment is aim at examining possible threats, vulnerabilities, the likelihood and impact of them [3] to define appropriate controls for reducing or eliminating the risks [4].

However, Cloud computing encompasses new technologies such as virtualization and there are both new risks to be determined and old risks to be re-evaluated and mitigated [5]. Moreover, cloud-computing environment is dynamic that make the traditional assessments developed for conventional IT environments do not readily fit it. Therefore, there are need to dynamic risk assessment method where frequent updates of risk evaluation information are used to evaluate risk exposure, as close as possible to real-time [6].
Hence, the introduction of cloud specific security risk assessment methodology that fit the dynamic nature of the cloud has significant importance and scope. Recently, several studies have been conducted to improve traditional security risk assessment techniques and present new paradigms for analyzing and evaluating security risks in cloud environment. However, it is still challenge and a growing area of research to find security risk assessment method for cloud environment [3].

1.1. Bayesian Networks

IN recent years, Bayesian Networks (BNs) have become increasingly recognized as a potentially powerful solution to complex risk assessment problems [7]. BNs have been widely used to represent full probability models in a compact and intuitive way. In the BN framework, the independence structure in a joint distribution is characterized by a directed acyclic graph, with nodes representing random variables and directed arcs representing causal or influential relationships between variables [7]. If the variables are discrete, then the conditional probability distributions (CPDs) CPDs can be represented as node probability tables (NPTs), which list the probability that the child node takes on each of its different values for each combination of values of its parents[7]. BNs offer the advantage of being able to reason in the presence of uncertainty, prior assumptions, and incomplete data [8].
Further, they are able to learn from evidence in order to update their prior beliefs. Similarly, BN models do not just predict a single value for a variable; they predict its probability distribution. By taking the marginal distributions of variables of interest, we get a ready-made means of providing quantitative risk assessment [8].

The remainder of this paper is organized as follows: In Section 2, we will present the related work. In Section 3, we will present our security risk assessment method for cloud environment. In Section 4, we will present motivating examples (Ecommerce application and hybrid Live VM migration scenario) to explain our method more.

2. Related Work

As we will see in this section there are several work towards risk assessment in cloud computing environment have been presented in the literature.
In [9] Daniele et al.(2009) proposed to estimate the level of risk based on the likelihood of an incident scenario, mapped against the estimated negative impact. The likelihood of an incident scenario is given by a threat exploiting vulnerability with a given likelihood. The likelihood of each incident scenario and the business impact was determined in consultation with the expert group contributing to this report, drawing on their collective experience. In cases where it was judged not possible to provide a well founded

estimation of the likelihood of an occurrence, the value is N/A. In many cases the estimate of likelihood depends heavily on the cloud model or architecture under consideration. However, there method is not quantitive and the estimation of risk levels is based on ISO/IEC 27005. One of the most important recommendations of their report is a set of assurance criteria designed to assess the risk of adopting cloud services. A fully quantitative risk assessment framework would further improve this methodology [12].

In [10] Amit Sangroya et al. (2010) present approach that can be primarily used by the perspective cloud users before putting their confidential data into a cloud. It is easily adaptable for automation of risk analysis. However, they define variables that can be used where there are some past statistics about the service provider [10]. The most obvious finding to emerge from this study is that, there is a need of better trust management framework and there is a lack of structured analysis approaches that can be used for risk analysis in cloud computing environments.

Xuan Zhang et al. (2010) in [11] present information risk management framework that provides better understanding for critical areas of focus in cloud computing environment, to identifying a threat and identifying vulnerability. It is covering all the cloud service models and cloud deployment models. Cloud providers can apply this framework to their organizations to do risk mitigation [11]. However, the risk assessment in this paper is mainly qualitative and not quantitative.

Prasad Saripalli et al. (2010) in [12] present a Quantitative risk and impact assessment framework (QUIRC), to assess the security risks associated with cloud computing platforms. The advantages of the QUIRC methodology are as follows. A quantitative approach gives vendors, customers and regulation agencies the ability to comparatively assess the relative robustness of different cloud vendor offerings and appr oaches in a defensible manner. It also can be helpful in alleviating the considerable FUD (Fear, Uncertainty and Doubt) associated with cloud platform security issues and assure that they are dealing with these issues in an effective way [12]. However, the limitations of the approach include the large amount of input information on meticulous collection of input data and probabilities of events, which requires collective industry SME inputs [12]. Moreover, this framework does not cover risks during all the stages of the lifecycle of the service when it exists on the cloud [13].

Burton S. Kaliski et al. (2010) in [14] introduced risk assessment as a service. Risk assessment as a service is a new paradigm for measuring risk as an autonomic method that follows the on-demand, automated, multi-tenant architecture of the cloud – a way to get a continuous “risk score” of the cloud environment with respect to a given tenant, a specific application, or more generally, for use by new tenants and applications [14]. They proposed a cloud-based *assessment as a service* paradigm as a promising alternative. However, they did not implement such a service but rather offer a general paradigm to be followed [14]. As well as they do not suggest method to calculate risk score.

Afnan Ullah et al. (2012) in [15] propose a methodology for performing security risk assessment for cloud computing architectures presenting some of the initial results. They consider the deployment and operation stages in the cloud lifecycle. Deployment stage where the initial placement of services on cloud providers, and the service operation stage where cloud resources and data managed by the cloud provider to fulfill the Service Level Objectives. However, at the operation stage, along with the calculated security risk for this

stage, the risk assessment tool will be interacting with the monitoring database and additional tools like a network and historical database to monitor if certain threats are becoming live [15].This work considers the three security requirement for information systems (Confidentiality, Integrity and Availability), but they do not consider other security requirements that are unique to cloud platforms such as (multi-party trust considerations, mutual auditability and Usability). Their future work include testing this system on a cloud platform with monitoring agents installed which will log certain threats when they occur. This will then be extended to determine threats which may be eventually occur based on the data being collected and difficult to determine directly from the events [15].

In [16] Saadia et al.(2015) proposed a new risk assessment method in which the measure of an IT risk can be determined as a product of threat, vulnerability and asset values. Where the asset value of each cloud actor is the average of the weight of confidentiality, availability and integrity ; the vulnerabilities value for each cloud actor specified basing on the absence or ineffectiveness of controls; threat value is calculated as product of probability of occurrence and the impact where each threats is mapped to indicative number of vulnerabilities and assets. However, the risk value will be depend on the actor and their corresponding assets, their security objectives and their corresponding vulnerabilities. To improve the architecture and consolidate the security risk assessment for cloud computing multi-agent systems can be used. [16].

In [17] Shareeful et al. (2017) presents a risk management framework that enables users to identify risks, based on the relative importance of the migration goals for specific migration scenarios and analyzed the risks with a semi-quantitative approach. They use the analytic hierarchy process (AHP) where each goal is compared with the other goals based on its importance level within the organizational context for the cloud migration. The net risk calculation depends on the associated risk factor values. Each risk factor value is estimated through the product of its probability and impact of overall risk. However, they use subjective judgment depending on individual perception for defining probability and impact values. The risk value is obtained by averaging the risk factors' values. Finally, the net risk level is the sum product of risk level and relative importance of affected migration goal. However, if the number of goals were to increase, the net risk level estimation would be more complex[17]. They are currently working on defining a guideline for risk management activities along with a checklist so that the framework could provide better hands-on support to potential cloud users. They are also planning to develop migration goals and a risk taxonomy and integrate it with the guidelines.

In [3], Fatimah M. Alturkistani et al. present a classification of cloud-based security risk assessment methods and tools. They suggests to have a collaborative security risk assessment method where the assessment is conducted in collaboration between customers and providers. They argue that this will add great assistance to both service providers and consumers alike.

In table 1 we summarize those related work with the technique suggested in them ,their problems and the model or tool proposed in it. However, [14] is just a paradigm to be followed. [9] is semi-quantitative. [10] need past statistics about the service provider. [11] does not cover risks during all the stages of the lifecycle of the service when it exists on the cloud. [15] do not consider other security requirements that are unique to cloud platforms. [16] the risk value will be depend on the actor.[17] use subjective judgment depending

on individual perception for defining probability and impact values. Moreover, none of them are dynamic to fit the dynamic nature of the cloud computing environment.

Table 1: Summary of the related works.

Lit. Ref	Context of Research	Technique Used	Problems	Model/ Tool/ Proposed
9	Security risk assessment method for cloud computing	Likelihood of an incident scenario, mapped against the estimated negative impact.	-Semi-quantitative [4]. -The estimation of risk levels is based on ISO/IEC 27005.	-Framework include additional standards. -Set of assurance criteria designed to assess the risk of adopting cloud services. - A fully quantitative risk assessment framework [12].
10	Risk analysis approach that can be primarily used by the perspective cloud users.	Build a trust matrix to analyze the data risk.	The variables have been defined in this method can be used where there are some past statistics about the service provider. A lack of structured analysis approaches that can be used for risk analysis in cloud computing environments.	Better trust management framework.
11	Information risk management framework	The Risk assessment step have four major processes (Likelihood Determination, Impact Analysis, Risk Determination according to Risk Scale, and Control Recommendations).	Risk assessment in this paper is not quantitative.	-

12	Quantitative risk and impact assessment framework (QUIRC)	Security risk under each Security Objective category would be average over the cumulative, weighted sum of n threats that map to that SO category and assign a weight for each of the SO categories. Then, Net Security Risk (R) to the application integrated over the SO is a weighted average.	This framework requires the careful collection of input data for Probabilities of events. Moreover, it does not cover risks during all the stages of the cloud lifecycle [13].	-
14	Risk assessment as a service	It is a paradigm to be followed.	No implementation as well as there are no method suggested to calculate risk score.	The dynamic assessment service
15	Methodology for performing security risk assessment for cloud computing architectures.	A number of stages have identified for performing a complete risk assessment (High level analysis of the system, Identifying the assets involved, Identify the threats in each cloud deployment scenario, High-level analysis of each threat, Risk Evaluation using evaluation matrix, and Risk Treatment).	They consider the three security requirement for information systems but they do not consider other security requirements that unique to cloud platforms.	Testing this system on a cloud platform with monitoring agents installed which will log certain threats when they occur.
16	Comprehensive and shared risk assessment method for cloud computing	Risk determined as a product of threat, vulnerability and asset values.	The risk value will be depend on the actor and their corresponding assets, their security objectives and their corresponding vulnerabilities.	-Use Multi-agent systems to improve the architecture and consolidate the security risk assessment for cloud computing.

17	A risk management framework for cloud migration decision support	Identify risks based on the relative importance of the migration goals for specific migration scenarios and analyzed the risks with a semi-quantitative approach.	-They use subjective judgment depending on individual perception for defining probability and impact values.	- Guideline for risk management activities along with a checklist. - Develop migration goals and a risk taxonomy and integrate it with the guidelines.

3. Proposed Method for Security Risk Assessment for Cloud Computing

Our dynamic method for risk assessment is depend on the National Institute of Standards and Technology (NIST) Special Publication (SP) 800- 30 which is a comprehensive framework that defines a set of risk assessment activities in nine steps [18] which explained in figure 1 .In addition, we will use a Bayesian network in likelihood determination step (step5). Therefore we will go through the following steps:

STEP 1: SYSTEM CHARACTERIZATION

In this step, the boundaries of the IT system are identified, along with the resources and the information that constitute the system. Therefore, output from this step will be a good picture of the system environment, and delineation of system boundary [18].

STEP 2: THREAT IDENTIFICATION

The goal of this step is to identify the potential threat-sources and compile a threat statement listing potential threat-sources that are applicable to the IT system being evaluated. Therefore, output from this step will be a threat statement containing a list of threat-sources that could exploit system vulnerabilities [18].

STEP 3: VULNERABILITY IDENTIFICATION

The goal of this step is to develop a list of system vulnerabilities (flaws or weaknesses) that could be exploited by the potential threat-sources. Therefore, output from this step will be a list of the system vulnerabilities (observations) that could be exercised by the potential threat-sources [18].

STEP 4: CONTROL ANALYSIS

The goal of this step is to analyze the controls that have been implemented, or are planned for implementation, by the organization to minimize or eliminate the likelihood (or probability) of a threat's exercising a system vulnerability [18]. Therefore, output from this step: List of current or planned controls used for the IT system to mitigate the likelihood of a vulnerability's being exercised and reduce the impact of such an adverse event [18].

STEP 5: LIKELIHOOD DETERMINATION

To derive an overall likelihood rating that indicates the probability that a potential vulnerability may be exercised within the construct of the associated threat environment. Therefore, output from this step will

be Likelihood rating [18].

In this step, we will use Bayesian network model since it is enable to compute the posterior probability distribution of some variables of interest (unknown parameters and unobserved data) conditioned on some other variables that have been observed. Our methodology for developing scenario based Bayesian network as follows:

5.1 Identifying the important system interaction event.

5.2 Establishing the links between them.

5.3 Assigning states and probabilities to each event state (i.e. The conditional probabilities for the states of each child node are specified for all combinations of states of their parent nodes). The estimation of probabilities associated with each state can be elicited from experts, learned from data or a combination of these [19].

5.4 Testing diagnostic to find probabilities for intended state.

5.5 Measure the probabilities when set evidence base on given information.

To conducting these steps, we will use Genie tool.

STEP 6: IMPACT ANALYSIS

To determine the adverse impact resulting from a successful threat exercise of a vulnerability. Therefore, output from this step will be magnitude of impact [18] .

In this step we will depend on current FMECA severity categories for U.S. Federal Aviation Administration (FAA), NASA and European Space Agency space applications .

Table 2: FMECA Severity Categories [20].

Category	Description	Criteria
I	Catastrophic	Could result in death, permanent total disability, loss exceeding $1M, or irreversible severe environmental damage that violates law or regulation.
II	Critical	Could result in permanent partial disability, injuries or occupational illness that may result in hospitalization of at least three personnel, loss exceeding $200K but less than $1M, or reversible environmental damage causing a violation of law or regulation.
III	Marginal	Could result in injury or occupational illness resulting in one or more lost work day(s), loss exceeding $10K but less than $200K, or mitigatible environmental damage without violation of law or regulation where restoration activities can be accomplished.
IV	Negligible	Could result in injury or illness not resulting in a lost work day, loss exceeding $2K but less than $10K, or minimal environmental damage not violating law or regulation.

STEP 7: RISK DETERMINATION

The purpose of this step is to assess the level of risk to the IT system.The final determination of mission risk is derived by multiplying the ratings assigned for threat likelihood (e.g., probability) and threat impact [18]. Therefore, risk define as:

Risk = Probability x Impact

Therefore, the decision maker can predict the risk, where the risk of each node is calculated and the node with maximum risk value have to given more attention and high priority to add control for it.

STEP 8: CONTROL RECOMMENDATIONS

The goal of the recommended controls is to reduce the level of risk to the IT system and its data to an acceptable level . Therefore, output from this step is recommendation of control(s) and alternative solutions to mitigate risk [18] .

STEP 9: RESULTS DOCUMENTATION

Once the risk assessment has been completed (threat-sources and vulnerabilities identified, risks assessed, and recommended controls provided), the results should be documented in an official report or briefing . Therefore, output from this step is risk assessment report that describes the threats and vulnerabilities, measures the risk [18].

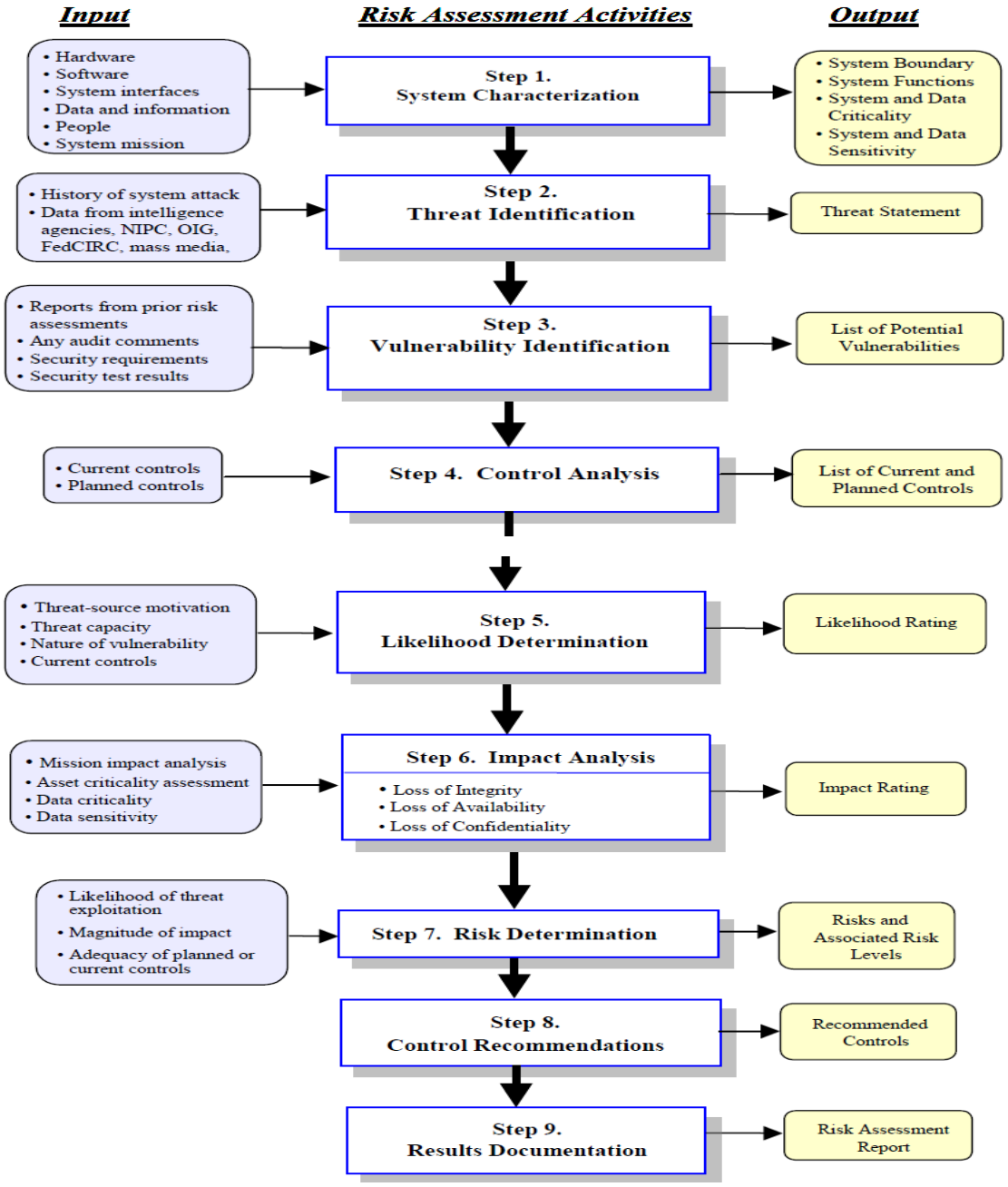


Figure 1: NIST Risk Assessment Methodology Flowchart [18]

4. Motivating Examples (case studies)

Our method will be based on specific scenario so we will explain every step on our method using two case studies in the following two subsections.

4.1. First Motivating Example (Ecommerce application):

Ecommerce on Cloud Computing is the specific application making good use of the cloud technology application in the business field, taking effective use of resources and reduce costs [21].For some e-commerce companies, entrusting the work to the third party contains some elements of risks. Going too much, the risks may be greater than the benefits for the business. Therefore, our first case study will be security risk assessment in buy book scenario for e-commerce in cloud computing environment. In the following we will explain our method using the buy book scenario for e-commerce application in cloud computing environment :

STEP 1: SYSTEM CHARACTERIZATION

We begin by explaining the buy book scenario for e-commerce in cloud computing environment using a sequence diagram in figure 2 to give good picture of the system.

STEP 2: THREAT IDENTIFICATION

We explained the potential threat for each event in the buy book scenario in figure 2.

STEP 3: VULNERABILITY IDENTIFICATION

The common cloud computing security vulnerabilities is:

- Insecure Coding

Injection Flaws, Cross-site Scripting (XSS), Cross-site Request Forgery (CSRF) , Buffer Overflows , Weak Authentication and/or Session Credentials .

- Security Misconfigurations [23]
- Unauthorized access to management interface.
- Internet protocol vulnerabilities.
- Data recovery vulnerability.
- Metering and billing evasion [24].

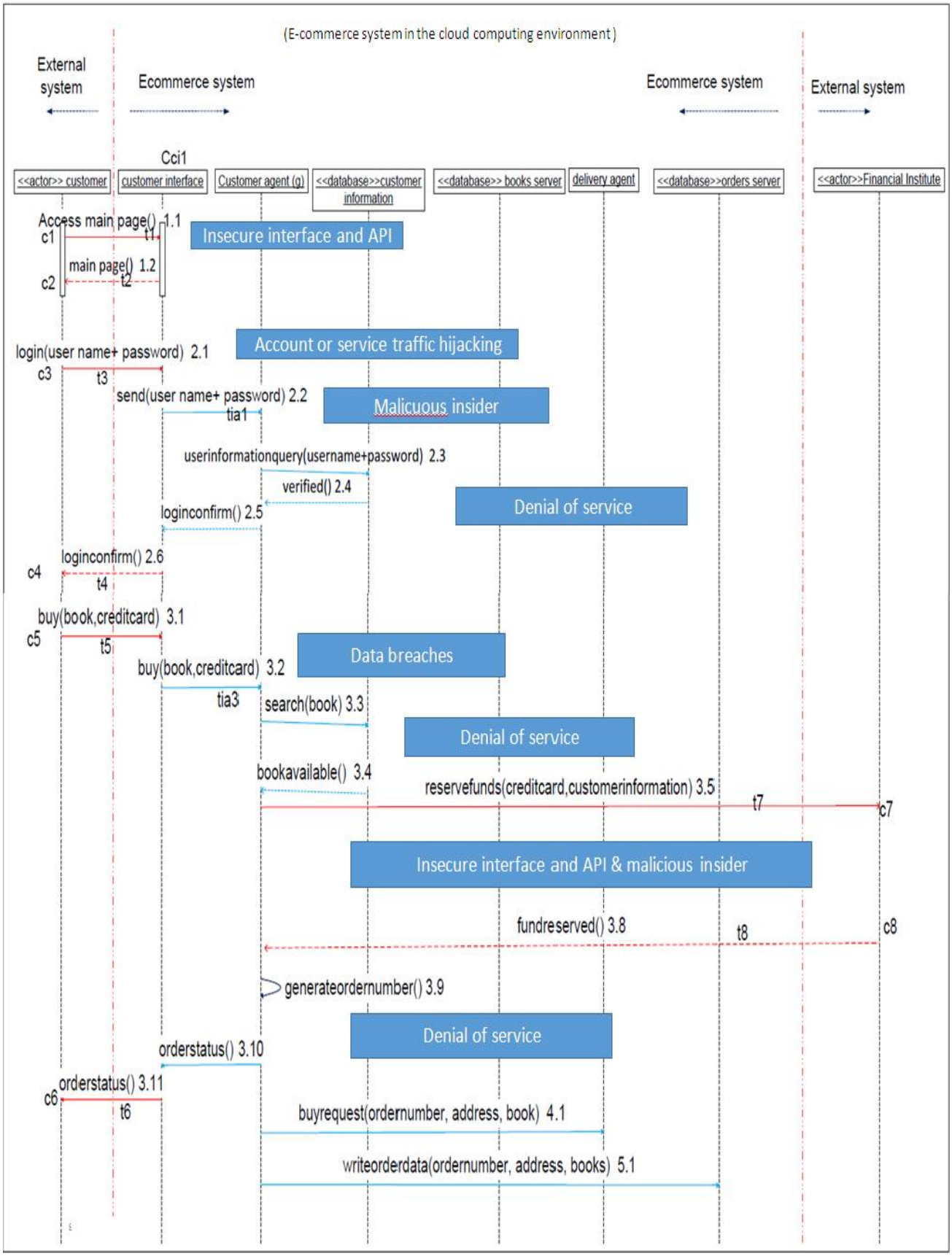


Figure.2. Sequence diagram of the buy book scenario [22]

STEP 4: CONTROL ANALYSIS

The detail to be asked to analyze control used for securing the system in the cloud computing environment include the following:

- The physical security and mechanical robustness of the datacenters
- Controls used to commission and decommission equipment within the datacenter, including hardware security controls such as hardware encryption devices
- Network operations and security features, including firewalls, protection against distributed denial of service (DDoS) attacks, integrity, file/log management, and antivirus protection.
- Basic IT controls and policies governing personnel, access, notification of administrator intervention, levels of access, and logging of access events [25].

STEP 5: LIKELIHOOD DETERMINATION

In this step, we will use Bayesian network model so we developed Bayesian network for the buy book scenario for e-commerce in cloud computing environment with states for each node which explained in figure 3 with some probabilities tables contain probability that we assume for each state.

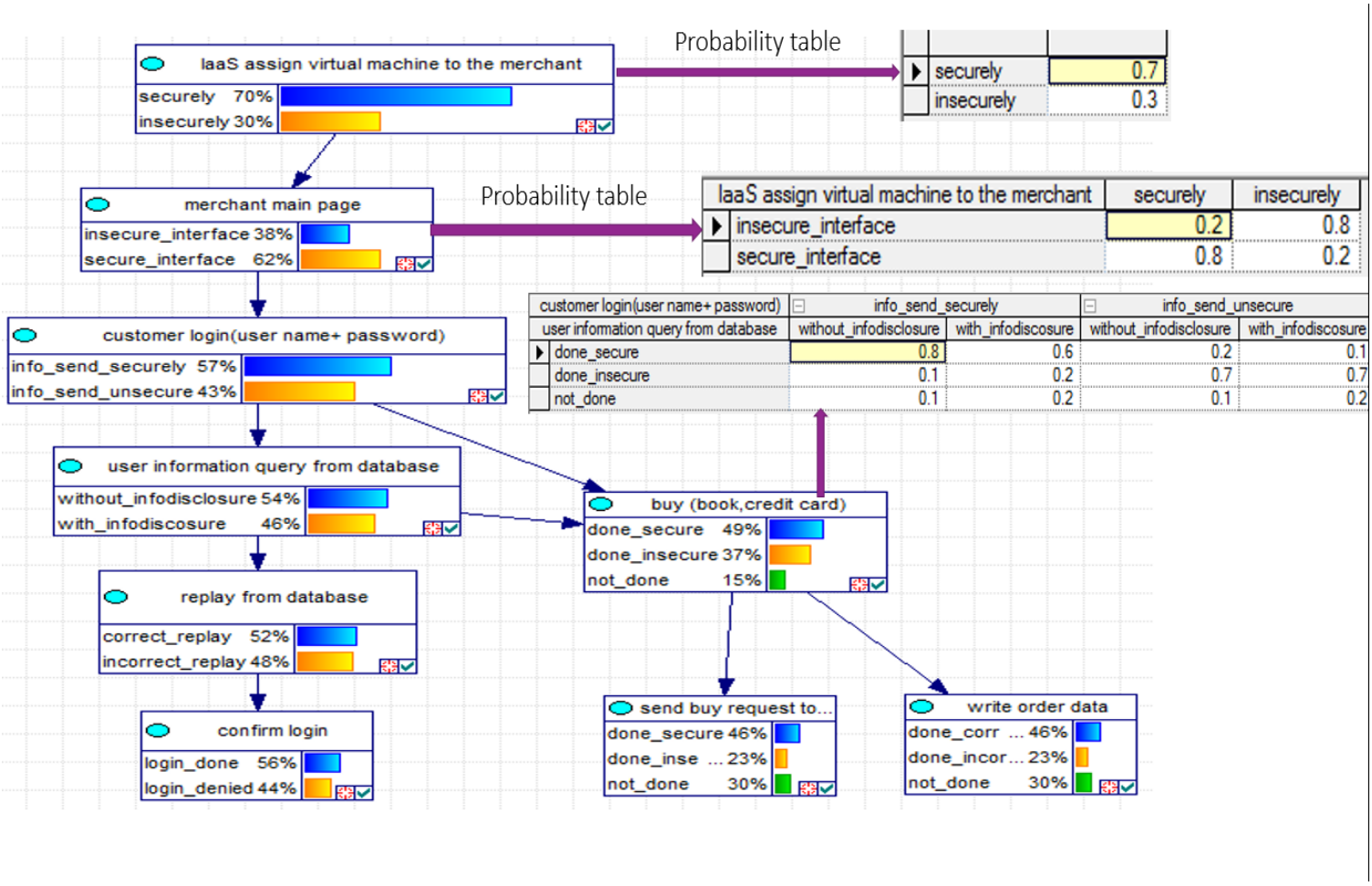


Figure. 3. Bayesian network for the buy book scenario.

In figure 4, we explain the diagnostic analysis for the Bayesian network for the buy book scenario by

selecting some state of the event and see their probability.

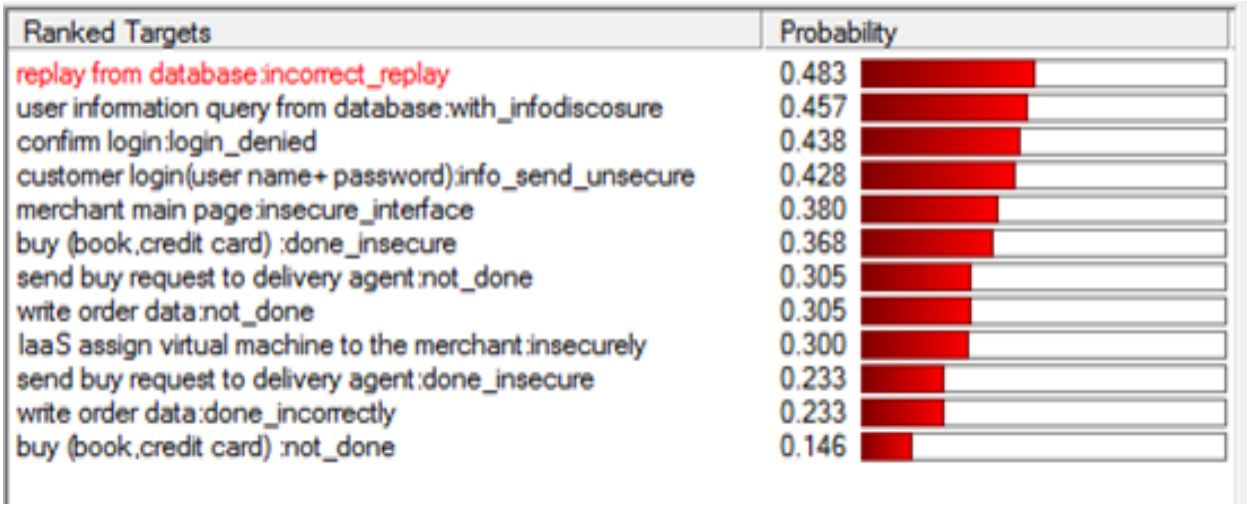


Figure 4: Testing diagnostic result for buy book scenario.

When set evidence base on given information we will notice the change in the probabilities for each state of the events. For example, for the buy book scenario in the customer login event if the evidence set to customer info sent insecurely, it will lead to change in the probability of states of all nodes as explained in figure 5.

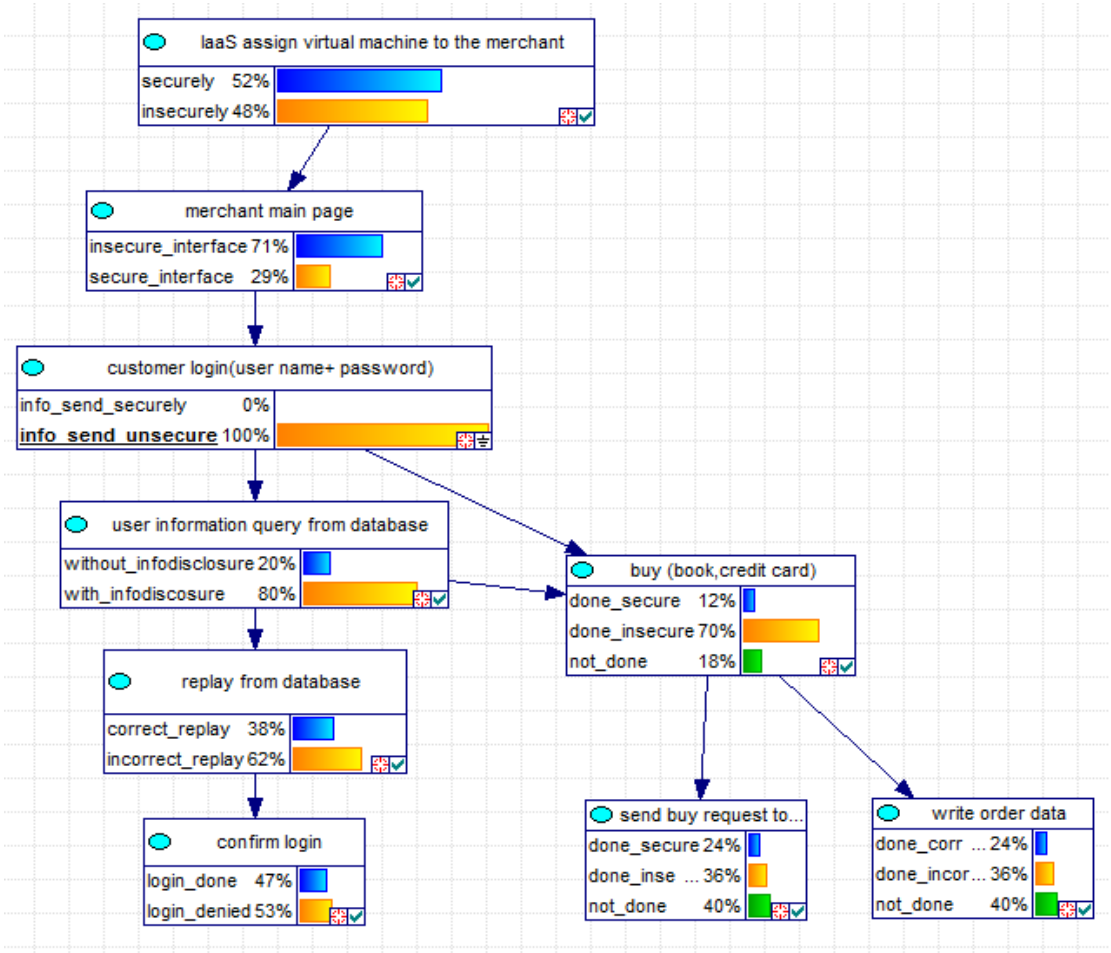
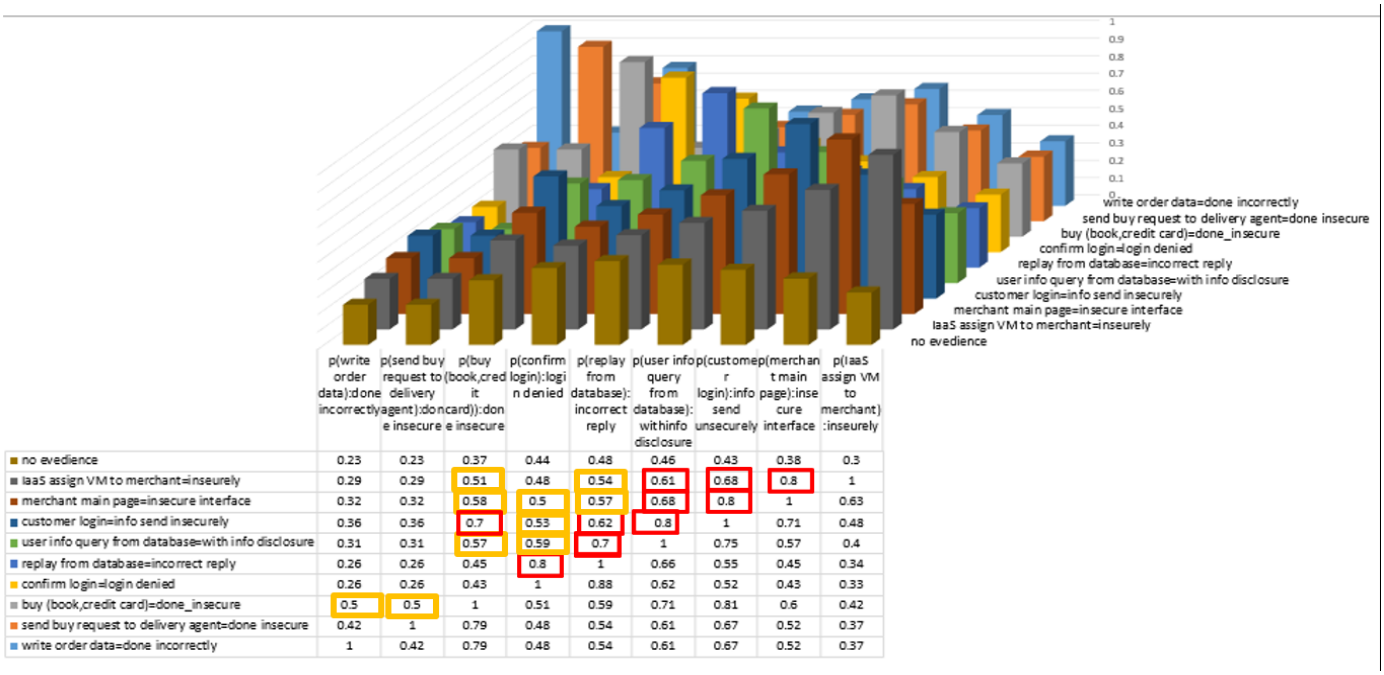


Figure. 5. Bayesian network when customer info send unsecure for the buy book scenario.

By this way we can see if we change the probability of insecurity for any event the related changes in the posterior probabilities for each events after setting evidence.

In figure 6 at the first row we explain the probability for the all events to be unsecure without setting for any evidence then we see each time if we set the evidence for one of the event to be done unsecure and observing the related changes in the posterior probabilities for other events. Therefore, at the second row we see if we set the evidence for the IaaS assign VM to merchant event to insecurely. Then the third row explain if we set evidence for the merchant main page to insecure interface and so on.



	p(write order data):done incorrectly	p(send buy request to delivery agent):done insecure	p(buy (book,credit card)):done insecure	p(confirm login):login denied	p(replay from database): incorrect reply	p(user info query from database): withinfo disclosure	p(customer login):info send unsecurely	p(merchant main page):insecure interface	p(IaaS assign VM to merchant) :inseurely
no evedience	0.23	0.23	0.37	0.44	0.48	0.46	0.43	0.38	0.3
IaaS assign VM to merchant=inseurely	0.29	0.29	0.51	0.48	0.54	0.61	0.68	0.8	1
merchant main page=insecure interface	0.32	0.32	0.58	0.5	0.57	0.68	0.8	1	0.63
customer login=info send insecurely	0.36	0.36	0.7	0.53	0.62	0.8	1	0.71	0.48
user info query from database=with info disclosure	0.31	0.31	0.57	0.59	0.7	1	0.75	0.57	0.4
replay from database=incorrect reply	0.26	0.26	0.45	0.8	1	0.66	0.55	0.45	0.34
confirm login=login denied	0.26	0.26	0.43	1	0.88	0.62	0.52	0.43	0.33
buy (book,credit card)=done_insecure	0.5	0.5	1	0.51	0.59	0.71	0.81	0.6	0.42
send buy request to delivery agent=done insecure	0.42	1	0.79	0.48	0.54	0.61	0.67	0.52	0.37
write order data=done incorrectly	1	0.42	0.79	0.48	0.54	0.61	0.67	0.52	0.37

Figure 6: The probability of insecurity for each event with the related changes in the posterior probabilities for each event after setting evidence.

STEP 6: IMPACT ANALYSIS

For the buy book scenario we determine the impact resulting from a successful threat in the following table that explain each event with it is severity (Impact).

Table 3. The impact resulting from a successful threat for each event in the buy book scenario.

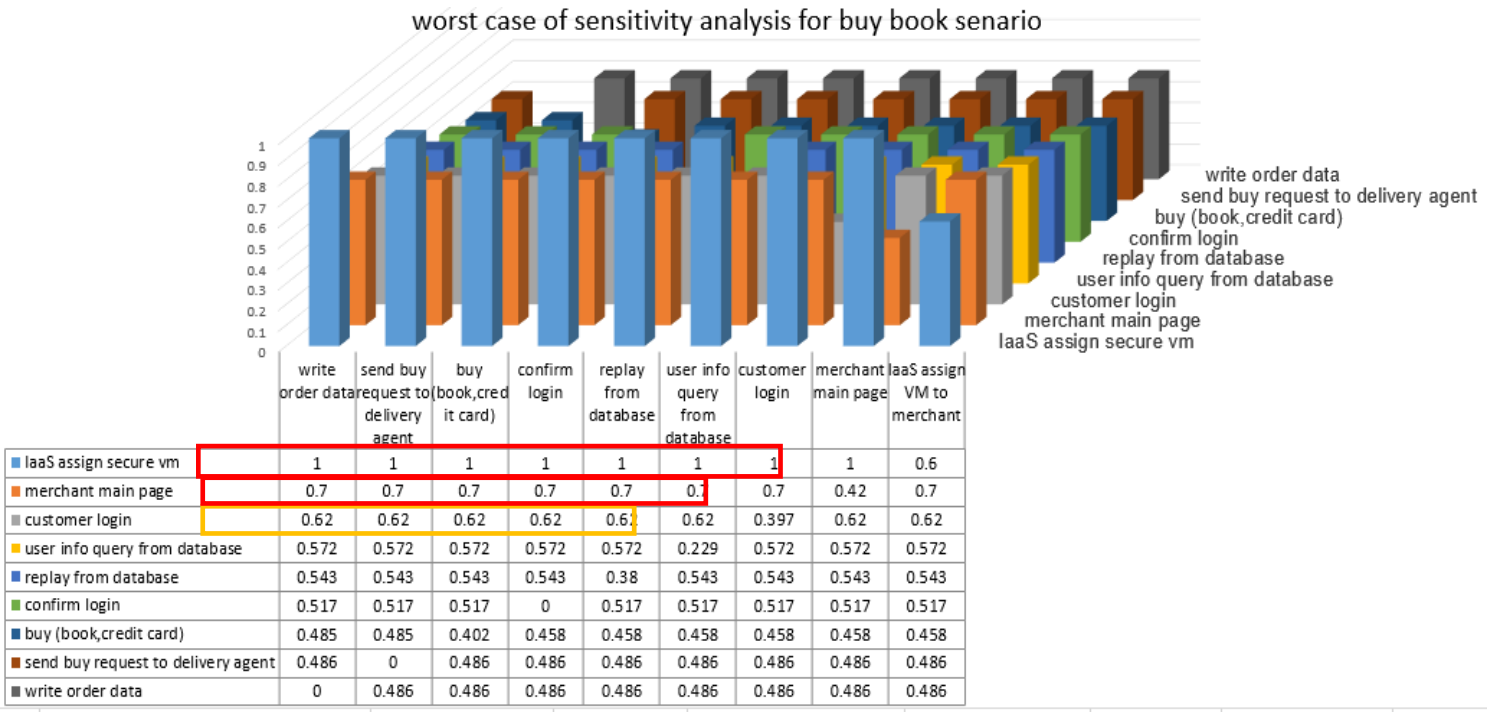
Event	Threat	Effect on system	Severity
IaaS assign VM to merchant	Insecure VM assigned to merchant	Deal with infected VM	Catastrophic
Access main page	Insecure main page accessed	Deal with another website (hacker web site)	Critical
Login :send (user name +password) to customer agent	Insecure sending	User name and password disclosed	Critical

user information query from database	Information disclosure	User name and password disclosed	Critical
replay from database	database don't work correctly or denial of service attack is done and reply not done correctly	Service denied	Significant
confirm login	denial of service attack is done and confirmation not done	Service denied	Significant
buy (book , credit card)	Insecure sending	credit card disclosed	Catastrophic
send buy request to delivery agent	Insecure sending	Buy request updated	Critical
write order data	Inconsistent database	System inconsistent	Critical

Risk Scale: Catastrophic (.95); Critical (.75); Marginal (.5)

If the severity of events not known we can use value for severity from sensitivity analysis results which enable us to see the impact of each event on the other events.

We explain in figure 7, the worst case of sensitivity analysis result for the Bayesian network, which we constructed for buy book scenario.As we can see from the figure , the first event IaaS assign VM to merchant affecting on all event by 100% percent so it have to given more priority to add control methods for it to be more secure. Then, the merchant main page security affecting on all event after it by .7 so it have to given the second level of priorty. Then, the customer login effect on all event after it by .62 so it have to give the third level of priority and so on.



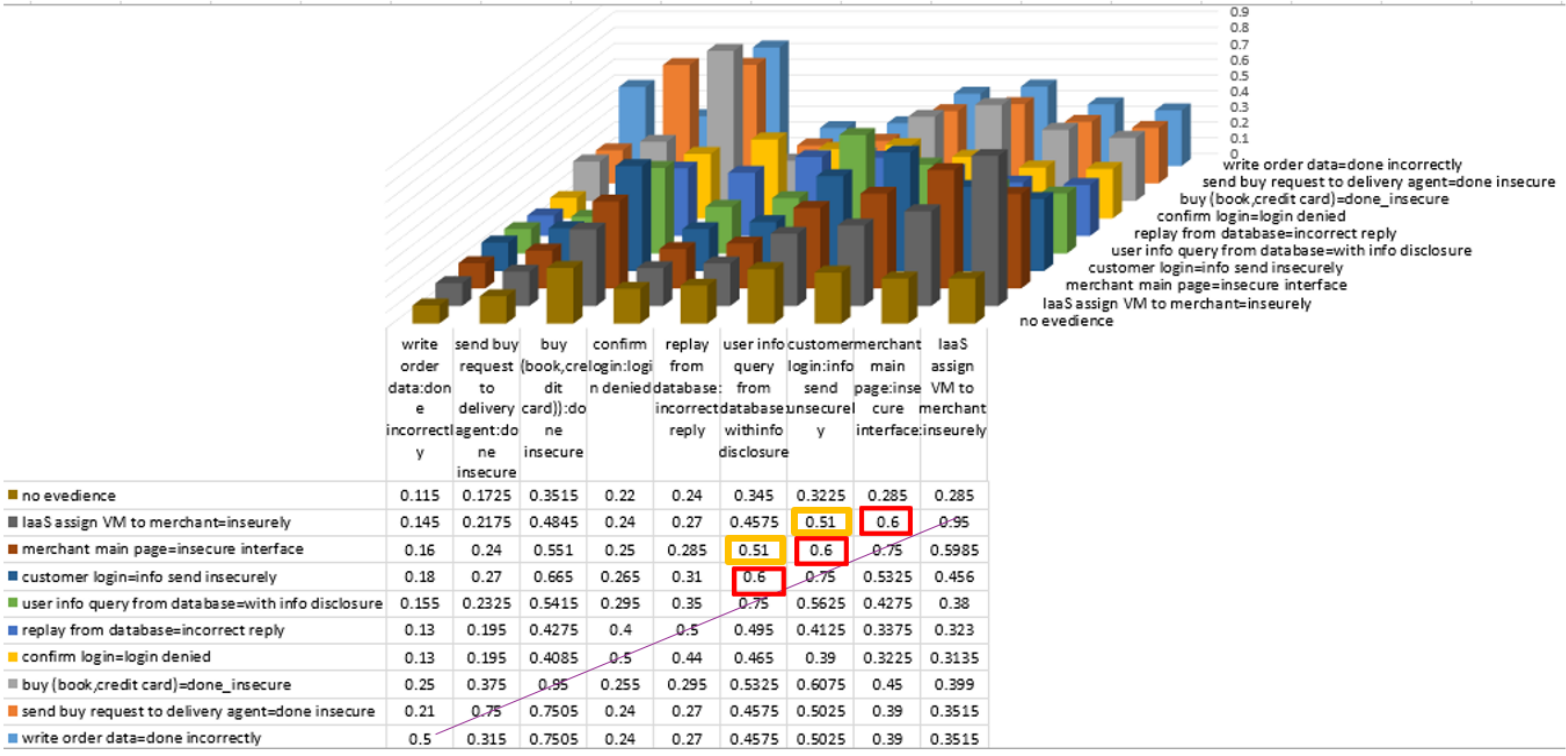
	write order data	send buy request to delivery agent	buy (book,credit card)	confirm login	replay from database	user info query from database	customer login	merchant main page	IaaS assign VM to merchant
IaaS assign secure vm	1	1	1	1	1	1	1	1	0.6
merchant main page	0.7	0.7	0.7	0.7	0.7	0.7	0.7	0.42	0.7
customer login	0.62	0.62	0.62	0.62	0.62	0.62	0.397	0.62	0.62
user info query from database	0.572	0.572	0.572	0.572	0.572	0.229	0.572	0.572	0.572
replay from database	0.543	0.543	0.543	0.543	0.38	0.543	0.543	0.543	0.543
confirm login	0.517	0.517	0.517	0	0.517	0.517	0.517	0.517	0.517
buy (book,credit card)	0.485	0.485	0.402	0.458	0.458	0.458	0.458	0.458	0.458
send buy request to delivery agent	0.486	0	0.486	0.486	0.486	0.486	0.486	0.486	0.486
write order data	0	0.486	0.486	0.486	0.486	0.486	0.486	0.486	0.486

Figure. 7. Bayesian network sensitivity analysis results for the buy book scenario

STEP 7: RISK DETERMINATION

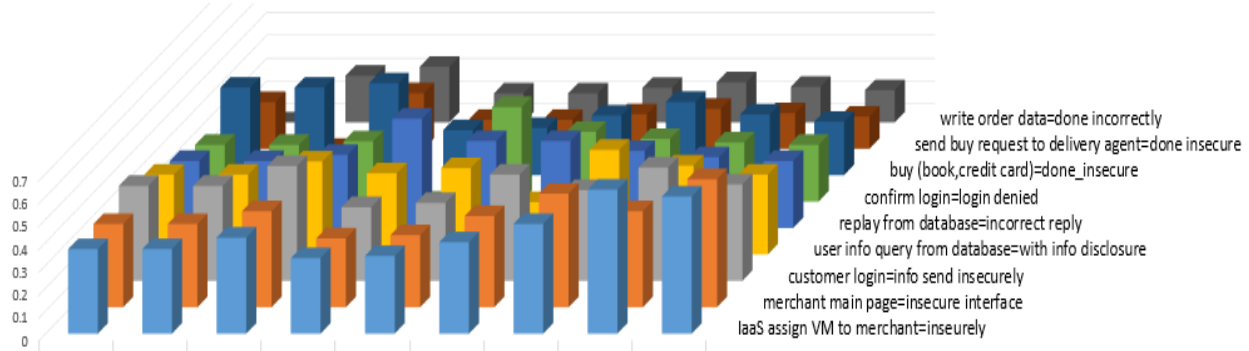
For the buy book scenario the result after we calculating the value of risk by multiplying the ratings assigned for event likelihood (e.g., probability) and its impact to assess the of risk of every event on the other event is explained in figure 8.

As we can see from figure 8 at the first row we explain the probability for the all events to be insecure without setting for any evidence. Then we see each time if we set the evidence for one of the event to be done insecure and observing the related changes in the posterior probabilities for other events. Therefore, at the second row we see if we set the evidence for the IaaS assign VM to merchant event to be done insecurely. As we notice the most event affected is the event that merchant main page to be insecure interface by .6 percent and so on. In addition we can see the prior probabilities for other events if we set the evidence. For example, if we set evidence the buy book event done insecurely this mean in the customer login event info was sent insecurely by .6 percent and so on.



	write order data:done incorrectly	send buy request to delivery agent:done insecure	buy (book,credit card)):done insecure	confirm login:login denied	replay from database: incorrect reply	user info query from database withinfo disclosure	customer login:info send unsecurely	merchant main page:insecure interface:	IaaS assign VM to merchant inseurely
no evedience	0.115	0.1725	0.3515	0.22	0.24	0.345	0.3225	0.285	0.285
IaaS assign VM to merchant=inseurely	0.145	0.2175	0.4845	0.24	0.27	0.4575	0.51	0.6	0.95
merchant main page=insecure interface	0.16	0.24	0.551	0.25	0.285	0.51	0.6	0.75	0.5985
customer login=info send insecurely	0.18	0.27	0.665	0.265	0.31	0.6	0.75	0.5325	0.456
user info query from database=with info disclosure	0.155	0.2325	0.5415	0.295	0.35	0.75	0.5625	0.4275	0.38
replay from database=incorrect reply	0.13	0.195	0.4275	0.4	0.5	0.495	0.4125	0.3375	0.323
confirm login=login denied	0.13	0.195	0.4085	0.5	0.44	0.465	0.39	0.3225	0.3135
buy (book,credit card)=done_insecure	0.25	0.375	0.95	0.255	0.295	0.5325	0.6075	0.45	0.399
send buy request to delivery agent=done insecure	0.21	0.75	0.7505	0.24	0.27	0.4575	0.5025	0.39	0.3515
write order data=done incorrectly	0.5	0.315	0.7505	0.24	0.27	0.4575	0.5025	0.39	0.3515

Figure 8: The risk of each event with the related change after setting evidence based on probability of insecurity and severity we specified for each event.



	write order data=done incorrectly	send buy request to delivery agent=done insecure	buy (book,credit card)=done_insecure	confirm login=login denied	replay from database=incorrect reply	user info query from database= with info disclosure	customer login=info send insecurely	merchant main page=insecure interface	IaaS assign VM to merchant=inseurely
IaaS assign VM to merchant=inseurely	0.37	0.37	0.42	0.33	0.34	0.4	0.48	0.63	0.6
merchant main page=insecure interface	0.364	0.364	0.42	0.301	0.315	0.399	0.497	0.42	0.56
customer login=info send insecurely	0.4154	0.4154	0.5022	0.3224	0.341	0.465	0.397	0.496	0.4216
user info query from database=with info disclosure	0.34892	0.34892	0.40612	0.35464	0.37752	0.229	0.4576	0.38896	0.34892
replay from database=incorrect reply	0.29322	0.29322	0.32037	0.47784	0.38	0.3801	0.33666	0.30951	0.29322
confirm login=login denied	0.24816	0.24816	0.26367	0	0.4136	0.30503	0.27401	0.2585	0.24816
buy (book,credit card)=done_insecure	0.38315	0.38315	0.402	0.19694	0.2061	0.26106	0.3206	0.26564	0.23358
send buy request to delivery agent=done insecure	0.20412	0	0.243	0.12636	0.12636	0.15066	0.17496	0.15552	0.14094
write order data=done incorrectly	0	0.20412	0.243	0.12636	0.12636	0.15066	0.17496	0.15552	0.14094

Figure 9: Risk value based on likelihood and sensitivity analysis results

In figure 9, we explain the result after we calculating the value of risk by multiplying the ratings assigned for event likelihood (e.g., probability) and its impact from sensitivity result which explained in figure 6. We can see the significant risk will be if the IaaS assign VM to merchant insecurely the risk of the merchant

main page be insecure will be.63.

STEP 8: CONTROL RECOMMENDATIONS

The best practices around security controls and processes for cloud computing are:

1. PHYSICAL SECURITY

- Fortifying physical data centers
- Multiple control layers
- Access authentication and 7×24 monitoring

2. NETWORK SECURITY

- Production environment completely separate
- Firewall and network zone segregation
- Two-factor authentication remote access
- Host based intrusion detection

3. APPLICATION SECURITY

- HTTPS for all incoming/outgoing data transfer
- Data encryption for credit card payment information
- Secure application design, development and testing
- Application firewall for an extra layer of perimeter protection

4. VULNERABILITY MANAGEMENT

- Internal and external network scans
- Security application scans
- Web application penetration testing
- Keep critical patches up-to-date [26]

STEP 9: RESULTS DOCUMENTATION

From figure 7 we can see the risk value for every event in the buy book scenario without evidence and the risk value for each event if there is information or evidence that is specific event done insecurely . Therefore, the event with maximum risk value and the event effecting on it have to given more attention and high priority to add control for it.

If we consider threshold for significant risk from .6 we can see the following significant risk:

- If the IaaS assign VM to merchant insecurely the risk of:
  - The merchant main page be insecure will be.6
- If the merchant main page be insecure interface the risk of :
  - Customer login(info send insecurely) will be.6
- If the customer login info send insecurely the risk of:
  - User info query from database with info disclosure will be .6

If we consider for the buy book scenario the result of the risk calculated depending on sensitivity result, which explained in figure 8, we can see the significant risk will be if the IaaS assign VM to merchant insecurely the risk of the merchant main page be insecure will be.68.

4.2. Second Example (Hybrid Live VM Migration):

Live migration of virtual machines exposes the contents of the VM state files to the network. An attacker can do the following actions:

a) Access data illegally during migration

b) Transfer a VM to an untrusted host

c)Create and migrate several VM causing disruptions or DoS

This can be possible because VM migration transfer the data over network channels that are often insecure, such as the Internet [27].

Therefore, our second case study will be security risk assessment for Hybrid Live VM Migration scenario in cloud computing environment. In the following we will explain our method on it:

STEP 1: SYSTEM CHARACTERIZATION

The sequence diagram that we use to explain hybrid Live VM migration to give good picture of the system is shown in figure 10.

STEP 2: THREAT IDENTIFICATION

We explained the potential threat for each event in figure 10.

STEP 3: VULNERABILITY IDENTIFICATION

The most vulnerabilities that is inherent in cloud computing due to using virtual machine and migration of it are:

-The co-location of virtual machines due to multi-tenant environment where an attacker's virtual machine tries to reside in the same server of the victim's virtual machine with purposes of misuse .

- An attacker who creates a valid account can create VM image containing malicious code such as a Trojan horse. If another customer uses this image, the virtual machine that he creates will be infected .

- The contents of virtual machines such as the kernel, applications, and data being used by these applications can be compromised during live migration [27].

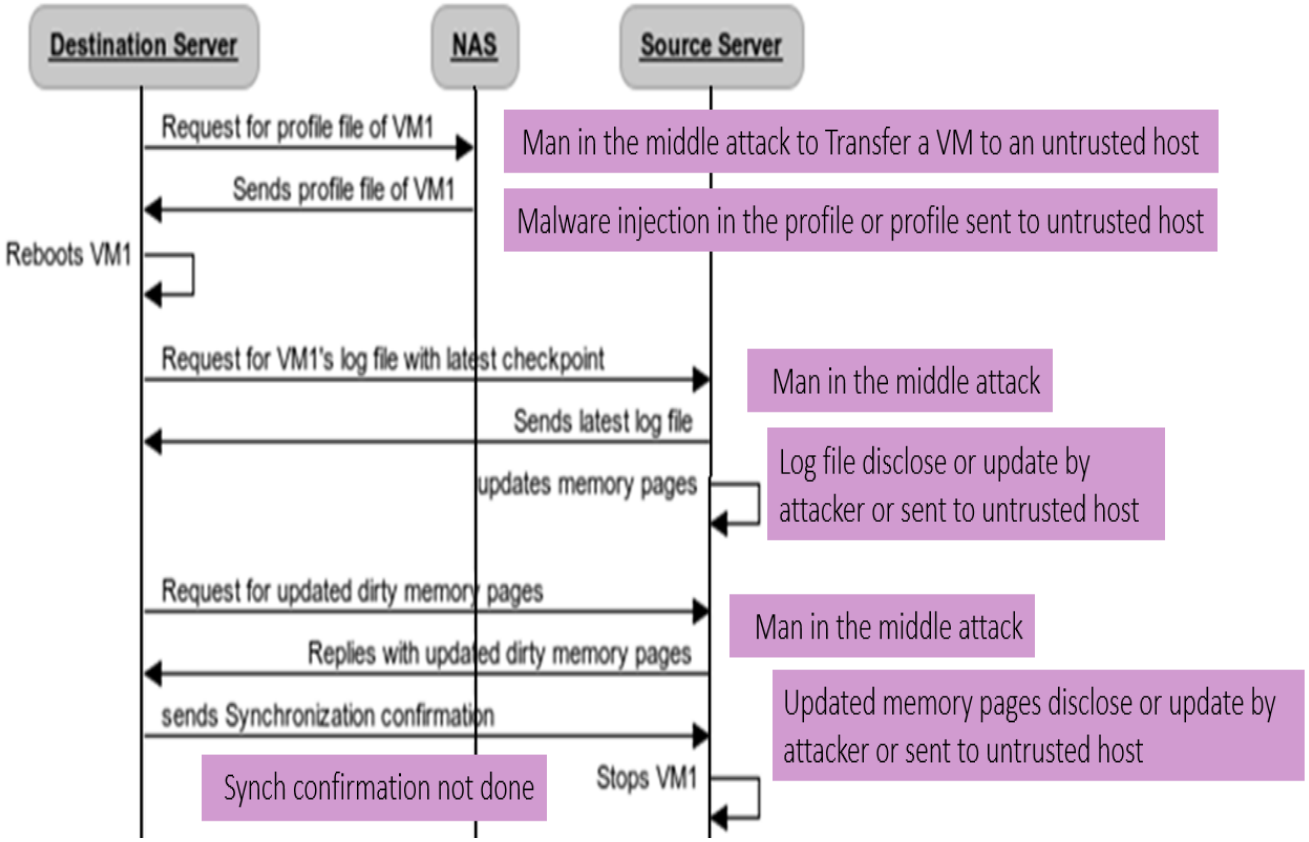


Figure.10. Sequence diagram of the hybrid Live VM migration scenario [28]

STEP 4: CONTROL ANALYSIS

The analysis include security control to be applied before migration, during migration process, and after migration. The detail to be asked to analyze control include the following:

• Are the source and destination physical hosts trusted.

• Are an authorized access to management interface; authenticated and authorized management capabilities (VM creation, deletion, migration etc) are in place.

• Is the migration data remains confidential and unmodified during the transmission.

• Control used for protection against network attacks, intrusions and malicious codes.

• The presence of mechanisms to detect and report suspicious activities.

• Protection against vulnerabilities in the migration software [29].

STEP 5: LIKELIHOOD DETERMINATION

In figure 11, we explain the Bayesian network we developed for the hybrid Live VM Migration in cloud computing environment with states for each node and their probability that we assume.

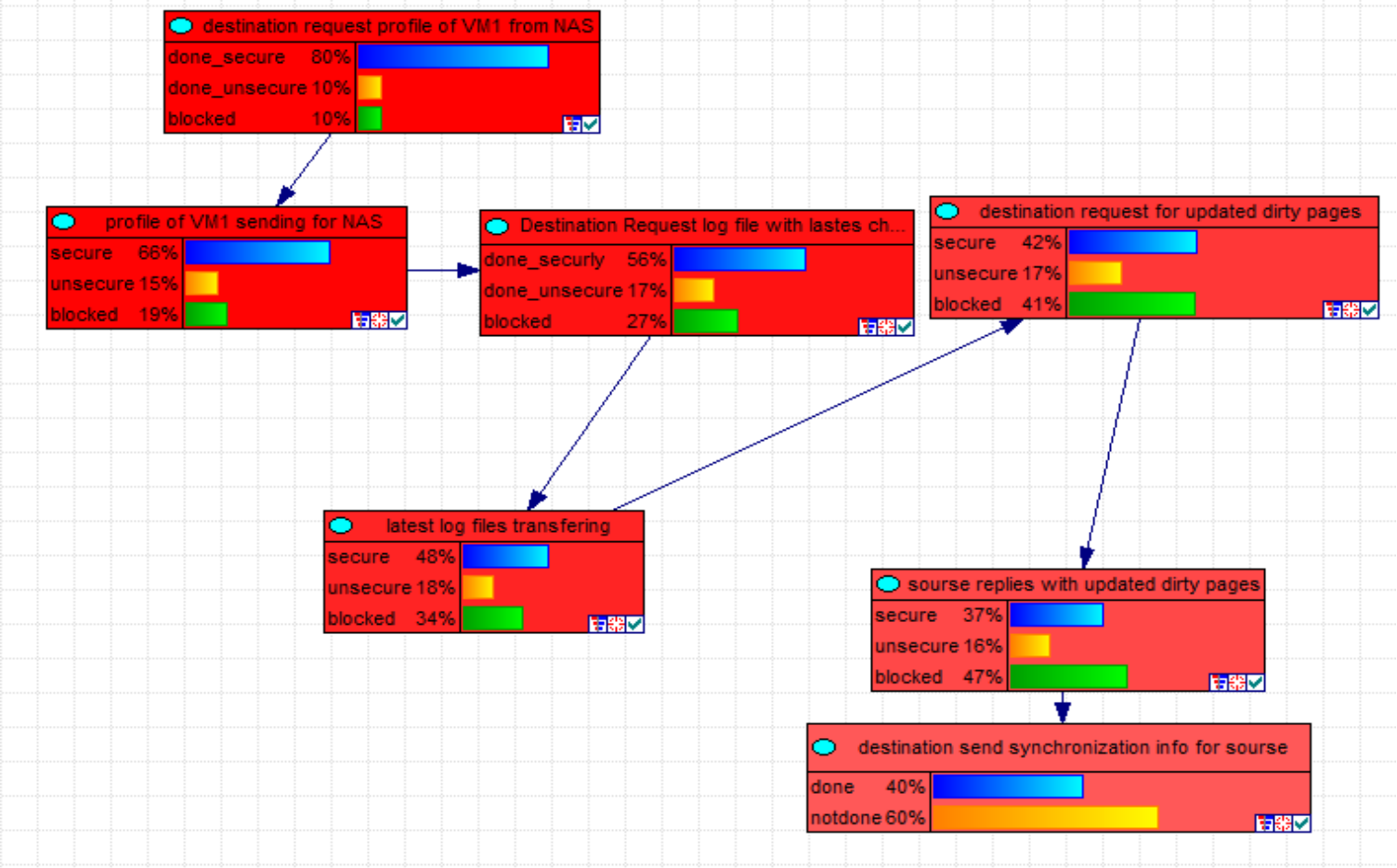


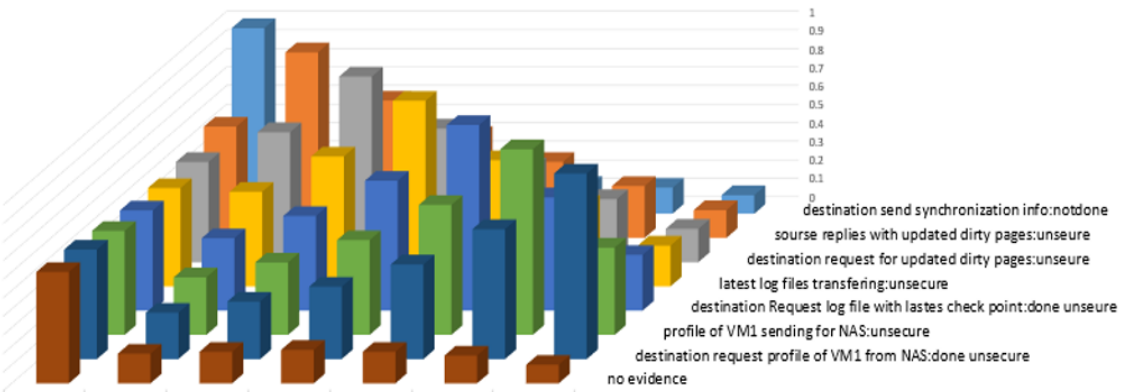
Figure. 11. Bayesian network for the hybrid Live VM Migration scenario.

In figure 12, we explain the diagnostic analyses for the Bayesian network for the hybrid Live VM migration by selecting some state of the event and see their probability.

Ranked Targets	Probability
destination send synchronization info for sourse :notdone	0.603
sourse replies with updated dirty pages:blocked	0.469
destination request for updated dirty pages:blocked	0.410
latest log files transfering :blocked	0.344
Destination Request log file with lastes check point from source:blo...	0.271
profile of VM1 sending for NAS:blocked	0.190
latest log files transfering :unsecure	0.175
Destination Request log file with lastes check point from source:don...	0.171
destination request for updated dirty pages:unsecure	0.171
sourse replies with updated dirty pages:unsecure	0.162
profile of VM1 sending for NAS:unsecure	0.150
destination request profile of VM1 from NAS:blocked	0.100
destination request profile of VM1 from NAS:done_unsecure	0.100

Figure 12: Testing diagnostic result for the hybrid Live VM migration scenario.

Then from figure 13, we can see the probability of insecurity for each event with the related changes in the posterior probabilities for each events after setting evidence for the hybrid Live VM migration scenario.



	destination send synchronization info for sourse :not done	sourse replies with updated dirty pages:unsecure	destination request for updated dirty pages:unseure	latest log files transfering :unsecure	destination Request log file with lastes check point from source:done unsecure	profile of VM1 sending for NAS:unsecure	destination request profile of VM1 from NAS:done unsecure
no evidence	0.6	0.16	0.17	0.18	0.17	0.15	0.1
destination request profile of VM1 from NAS:done unsecure	0.59	0.25	0.31	0.39	0.51	0.7	1
profile of VM1 sending for NAS:unsecure	0.56	0.31	0.39	0.51	0.7	1	0.47
destination Request log file with lastes check point:done unseure	0.54	0.39	0.51	0.7	1	0.61	0.3
latest log files transfering:unsecure	0.53	0.51	0.7	1	0.68	0.44	0.22
destination request for updated dirty pages:unseure	0.54	0.7	1	0.72	0.51	0.34	0.18
sourse replies with updated dirty pages:unseure	0.6	1	0.74	0.55	0.41	0.28	0.15
destination send synchronization info:notdone	1	0.16	0.15	0.15	0.15	0.14	0.1

Figure 13: The probability of insecurity for each event with the related changes in the posterior probabilities for event after setting evidence for the hybrid Live VM migration scenario.

From figure 13, we can see the following significant likelihood:

- Without evidence the destination send synchronization info for source :not done probability is .6
- If the destination request profile of VM1 from NAS: done unsecure the probability that:
  - The profile of VM1 sending for NAS: unsecure will increase to .7
- If the profile of VM1 sending for NAS: unsecure the probability that:
  - The destination request log file with lasts check point from source: done unsecure will increase to .7
- If the destination request log file with lasts check point from source: done unsecure the probability that:
  - The latest log files transferring :unsecure will increase to .7
- If the latest log files transferring :unsecure the probability that:
  - The destination request for updated dirty pages: unsecure will be .7
- If the destination request for updated dirty pages: unsecure probability that:
  - The source replies with updated dirty pages: unsecure will be .7
- If the source replies with updated dirty pages: unsecure probability that:
  - The destination send synchronization info for source :not done will be .6

STEP 6: IMPACT ANALYSIS

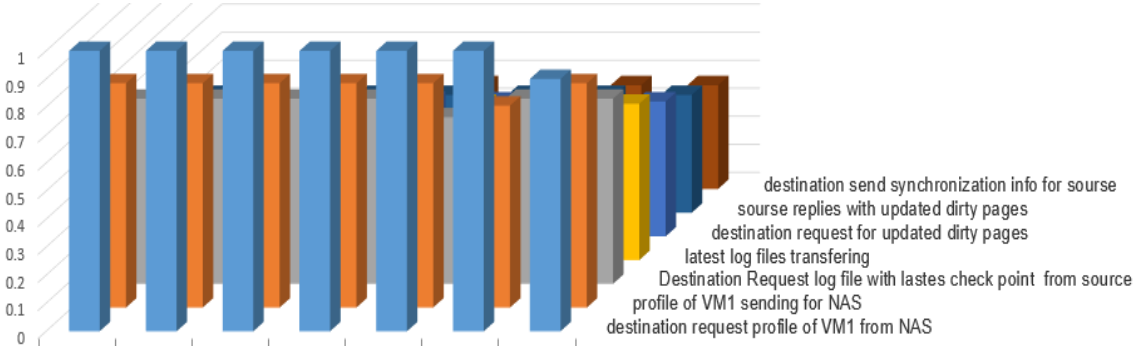
In Table 4. We explain the impact resulting from a successful threat for each event in the hybrid Live VM migration scenario.

Table 4. The impact resulting from a successful threat for each event in the hybrid Live VM migration scenario.

Event	Effect on system Severity
destination request profile of VM1 from NAS	Critical
profile of VM1 sending for NAS	catastrophic
Destination Request log file with lasts check point from source	critical
latest log files transferring	catastrophic
destination request for updated dirty pages	critical
source replies with updated dirty pages	catastrophic
destination send synchronization info for source	marginal

On the other hand, we can conduct sensitivity analysis for constructed Bayesian network using that will enable us to see the impact of every event on the others.

In figure 14, we explain the worst case of sensitivity analysis result for hybrid live VM migration for the Bayesian network, which we constructed.



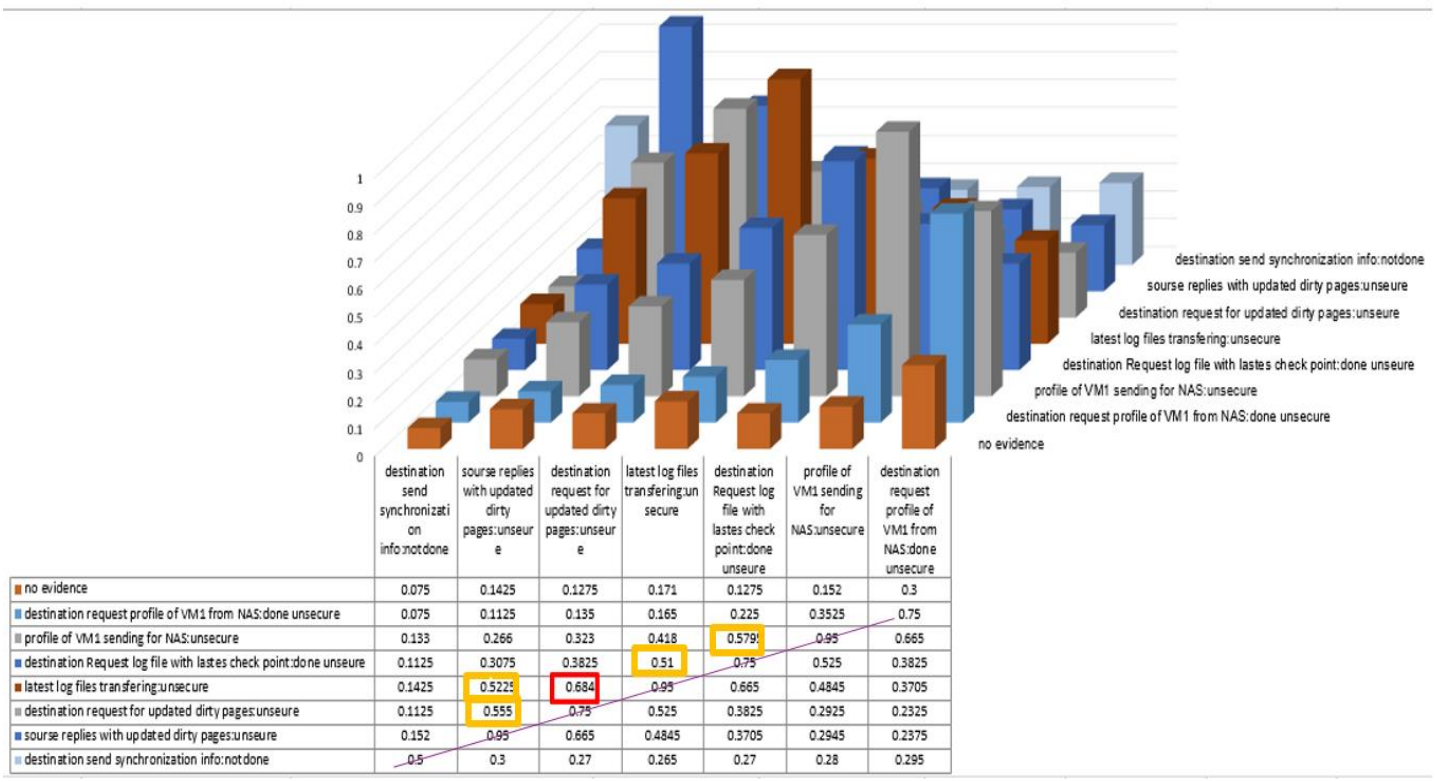
	destination send synchronization info	sourse replies with updated dirty pages	destination request for updated dirty pages	latest log files transfering	Destination Request log file with lastes check point	profile of VM1 sending for NAS	destination request profile of VM1 from NAS
destination request profile of VM1 from NAS	1	1	1	1	1	1	0.9
profile of VM1 sending for NAS	0.8	0.8	0.8	0.8	0.8	0.72	0.8
Destination Request log file with lastes check point from source	0.66	0.66	0.66	0.66	0.594	0.66	0.66
latest log files transfering	0.558	0.558	0.558	0.502	0.558	0.558	0.558
destination request for updated dirty pages	0.481	0.481	0.433	0.481	0.481	0.481	0.481
sourse replies with updated dirty pages	0.42	0.354	0.42	0.42	0.42	0.42	0.42
destination send synchronization info for sourse	0	0.37	0.37	0.37	0.37	0.37	0.37

Figure. 14. Bayesian network sensitivity analysis results for the hybrid Live VM migration scenario

As we can see from figure 14, the first event destination request profile of VM1 from NAS is more event affecting on all other event so it have to give more priority to add control methods for it to be more secure.

STEP 7: RISK DETERMINATION

From figure 15, we can see the risk of each event with the related change after setting evidence for the hybrid Live VM migration scenario.



	destination send synchronization info:notdone	sourse replies with updated dirty pages:unseure	destination request for updated dirty pages:unseure	latest log files transfering:unsecure	destination Request log file with lastes check point:done unseure	profile of VM1 sending for NAS:unsecure	destination request profile of VM1 from NAS:done unsecure
no evidence	0.075	0.1425	0.1275	0.171	0.1275	0.152	0.3
destination request profile of VM1 from NAS:done unsecure	0.075	0.1125	0.135	0.165	0.225	0.3525	0.75
profile of VM1 sending for NAS:unsecure	0.133	0.266	0.323	0.418	0.579	0.95	0.665
destination Request log file with lastes check point:done unseure	0.1125	0.3075	0.3825	0.51	0.75	0.525	0.3825
latest log files transfering:unsecure	0.1425	0.5225	0.684	0.95	0.665	0.4845	0.3705
destination request for updated dirty pages:unseure	0.1125	0.555	0.75	0.525	0.3825	0.2925	0.2325
sourse replies with updated dirty pages:unseure	0.152	0.95	0.665	0.4845	0.3705	0.2945	0.2375
destination send synchronization info:notdone	0.5	0.3	0.27	0.265	0.27	0.28	0.295

Figure 15: The risk of each event with the related change after setting evidence for the hybrid Live VM migration scenario

STEP 8: CONTROL RECOMMENDATIONS

Insecure VM Migration can be stopped by the following countermeasures:

- A Trusted Cloud Computing Platform (TCCP) that provide confidential execution of guest virtual machines. It provides secure VM launch and migration operations.

- PALM a secure migration system that provides VM live migration capabilities under the condition that a VMMprotected system is present and active.

- The connection between the source and the destination VMMs should be authenticated and encrypted during the migration process.

- Isolate VM migration traffic to prevent eavesdropping attacks [27].

STEP 8: RESULTS DOCUMENTATION

From figure 15, we can see the following significant risk:

- If the latest log files transferring :unsecure the risk that:
  - The destination request for updated dirty pages: unsecure will be .684

5. Effect of using security controls in reducing the risk factors

If we add security control to the system we have to reassess the security risk depending on the new value for state probabilities that we will change to see its effect in reducing the risk factors . For example, figure 16 illustrate the Bayesian network which we construct for buy book scenario if we change in some states probabilities for some events.

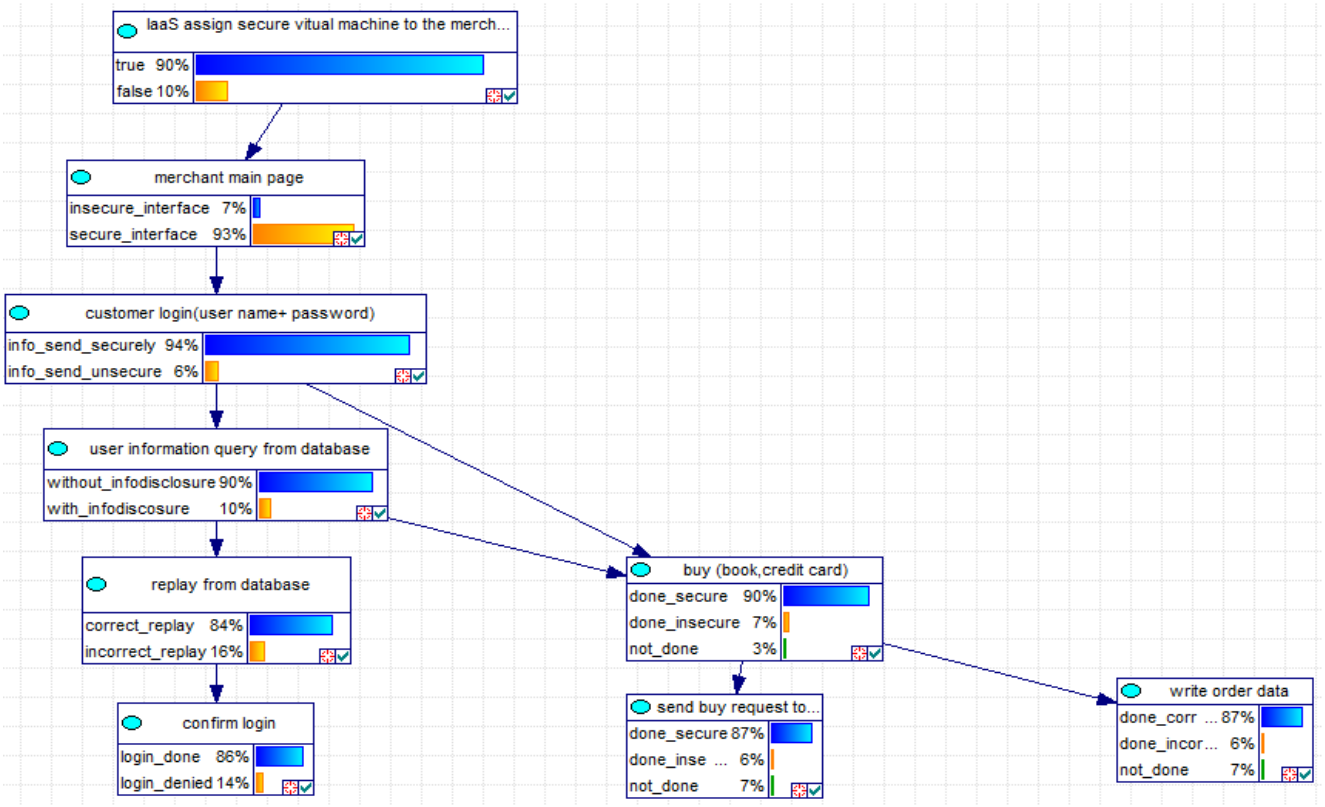


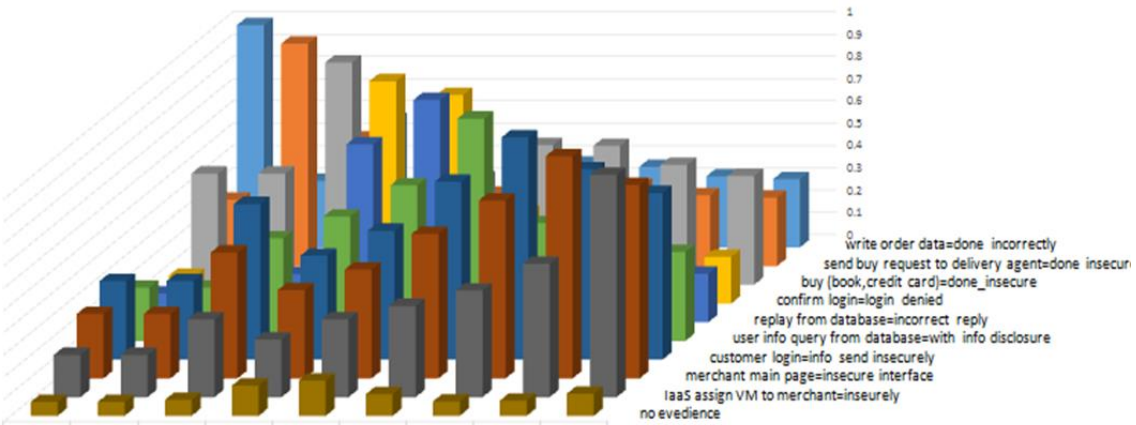
Figure 16: Bayesian network after change in some states probabilities for some events.

Based on the new probabilities the new testing diagnostic result for buy book scenario will be as explained in figure 17.

Ranked Targets	Probability
replay from database:incorrect_replay	0.159
confirm login:login_denied	0.136
IaaS assign secure vitual machine to the merchant:false	0.100
user information query from database:with_infodiscosure	0.098
buy (book,credit card) :done_insecure	0.072
send buy request to delivery agent:not_done	0.069
write order data:not_done	0.069
merchant main page:insecure_interface	0.069
customer login(user name+ password):info_send_unsecure	0.065
send buy request to delivery agent:done_insecure	0.063
write order data:done_incorrectly	0.063
buy (book,credit card) :not_done	0.030

Figure 17: Testing diagnostic result for buy book scenario after change in some states probabilities for some events.

In addition we explain in figure 18 the new value of the probability of insecurity for any event and the related changes in the posterior probabilities for each events after setting evidence.



	p(write order data):done incorrectly	p(send buy request to delivery agent):done insecure	p(buy (book,credit card)):done insecure	p(confirm login):login denied	p(replay from database):incorrect reply	p(user info query from database):withinfo disclosure	p(customer login):info send unsecurely	p(merchant main page):insecure interface	p(IaaS assign VM to merchant):inseurely
no evedience	0.063	0.063	0.072	0.136	0.159	0.098	0.065	0.069	0.1
IaaS assign VM to merchant=inseurely	0.19	0.19	0.35	0.26	0.35	0.41	0.48	0.6	1
merchant main page=insecure interface	0.29	0.29	0.566	0.397	0.49	0.65	0.8	1	0.87
customer login=info send insecurely	0.354	0.354	0.7	0.468	0.58	0.8	1	0.856	0.75
user info query from database=with info disclosure	0.24	0.24	0.462	0.56	0.7	1	0.53	0.46	0.4
replay from database=incorrect reply	0.129	0.129	0.217	0.8	1	0.433	0.235	0.213	0.219
confirm login=login denied	0.124	0.124	0.206	1	0.938	0.408	0.223	0.202	0.21
buy (book,credit card)=done_insecure	0.5	0.5	1	0.387	0.478	0.629	0.625	0.54	0.489
send buy request to delivery agent=done insecure	0.299	1	0.573	0.267	0.326	0.376	0.362	0.319	0.307
write order data=done incorrectly	1	0.299	0.573	0.267	0.326	0.376	0.362	0.319	0.307

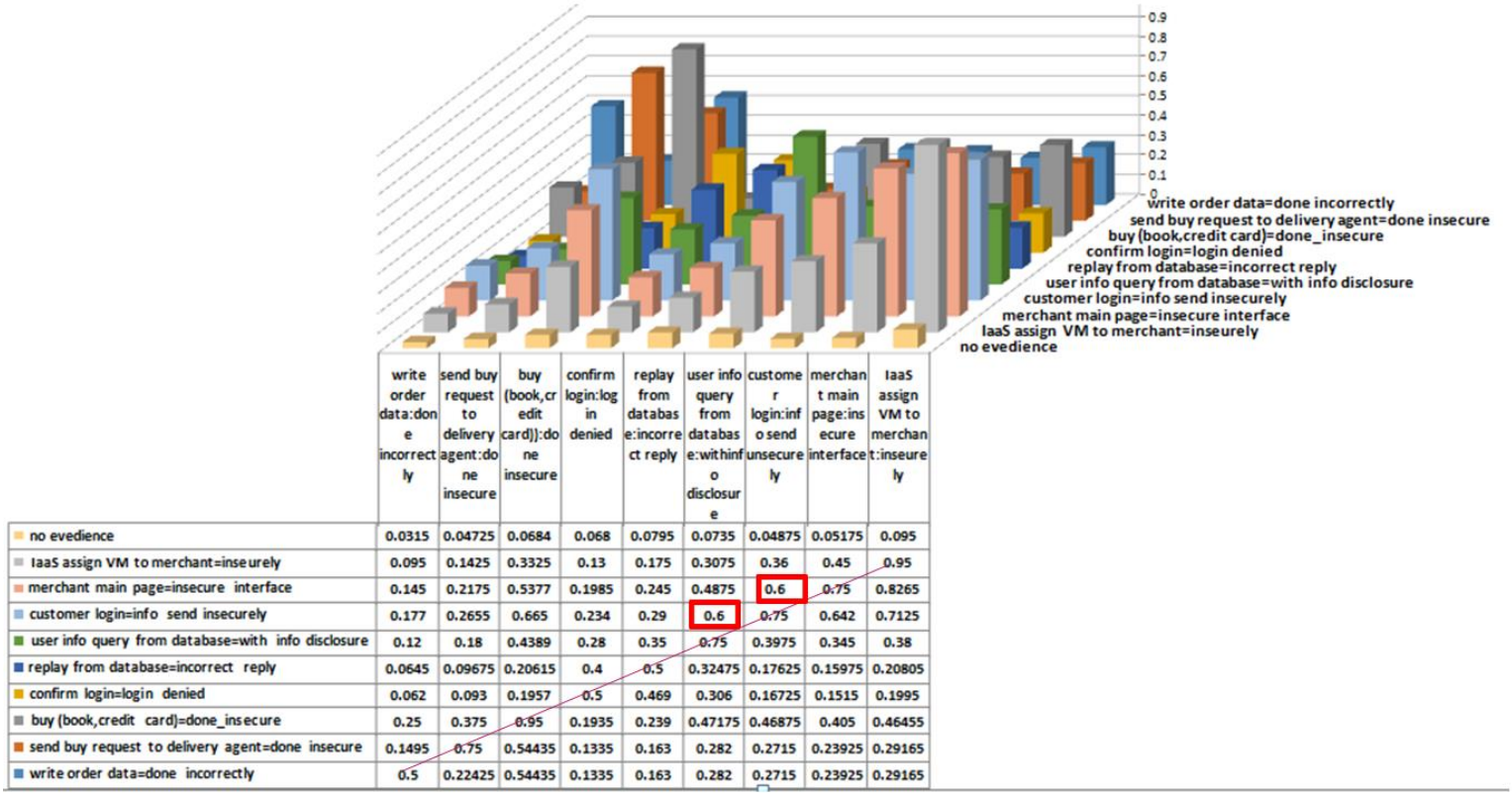
Figure 18: The probability of insecurity for each event with the related changes in the posterior probabilities for each event after setting evidence.

Based on this new value of the probability the result after we calculating the value of risk by multiplying the event probability and its impact in figure 19.

As we can from this figure the significant risk will be:

- If the merchant main page be insecure interface the risk of :
  - Customer login(info send insecurely) will be.6
- If the customer login info send insecurely the risk of:
  - User info query from database with info disclosure will be .6

Therefore we can see the effect of adding security controls in reducing the risk factors.



	write order data:done incorrectly	send buy request to delivery agent:done insecure	buy (book,credit card)):done insecure	confirm login:log in denied	replay from database:incorrect reply	user info query from database:withinfo disclosure	customer login:info send unsecurely	merchant main page:insecure interface	IaaS assign VM to merchant:inseurely
no evedience	0.0315	0.04725	0.0684	0.068	0.0795	0.0735	0.04875	0.05175	0.095
IaaS assign VM to merchant=inseurely	0.095	0.1425	0.3325	0.13	0.175	0.3075	0.36	0.45	0.95
merchant main page=insecure interface	0.145	0.2175	0.5377	0.1985	0.245	0.4875	0.6	0.75	0.8265
customer login=info send insecurely	0.177	0.2655	0.665	0.234	0.29	0.6	0.75	0.642	0.7125
user info query from database=with info disclosure	0.12	0.18	0.4389	0.28	0.35	0.75	0.3975	0.345	0.38
replay from database=incorrect reply	0.0645	0.09675	0.20615	0.4	0.5	0.32475	0.17625	0.15975	0.20805
confirm login=login denied	0.062	0.093	0.1957	0.5	0.469	0.306	0.16725	0.1515	0.1995
buy (book,credit card)=done_insecure	0.25	0.375	0.95	0.1935	0.239	0.47175	0.46875	0.405	0.46455
send buy request to delivery agent=done insecure	0.1495	0.75	0.54435	0.1335	0.163	0.282	0.2715	0.23925	0.29165
write order data=done incorrectly	0.5	0.22425	0.54435	0.1335	0.163	0.282	0.2715	0.23925	0.29165

Figure 19: The risk of each event with the related change after setting evidence based on probability of insecurity and severity we specified for each event.

6. Conclusion:

Despite the fact that cloud computing offers many cost benefits for their cloud consumers, number of security risk are emerging in association with cloud usage that need to be assessed.

However, Risk assessment is a complex undertaking, usually based on uncertain information while managing uncertainties is a tedious task and the nature of occurrence of threats and vulnerabilities change rapidly.

This paper presents method for security risk assessment in cloud computing that will enable the cloud provider to assess the risk based on existing scenario, and prioritizing security risks. It is using Bayesian network that allows entering evidence so probabilities in the network are updated when new information is available. Depending on the assessment results the cloud provider can establishing controls so that the risk can be reduced to an acceptable level. For illustration of the method, we explained it is in two scenario. However, our method need to have initial probabilities for events occurrence depending on existing control and threat analysis.

7. References:

1. Almathami, Mohammed, "SLA-based risk analysis in cloud computing environments" ,Thesis. Rochester Institute of Technology, 2012.

2. http://blogs.datadirect.com/2013/07/banking-security-cloud.html
3. Fatimah M. Alturkistani, Ahmed Z. Emam, "A Review of Security Risk Assessment Methods in Cloud Computing", New Perspectives in Information Systems and Technologies, Volume 1 , Springer International Publishing, 2014.
4. Drissi S., Houmani H. and Medromi H., Survey: Risk Assessment for Cloud Computing, University Hassan II Aïn Chock. ENSEM Casablanca, Morocco, (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 4, No. 12, 2013.
5. J. Oriol Fit´o, Mario Mac´ıas and Jordi Guitart, Toward Business-driven Risk Management for Cloud Computing, Barcelona Supercomputing Center and Technical University of Catalonia, 978-1-4244-8909-1/$26.00 _c 2010 IEEE.
6. David Lopez,Oscar Pastor, Luis Javier Garcia Villalba," Data model extension for security event notification with dynamic risk assessment purpose",Science China Information Sciences, Volume 56, Issue 11, pp 1-9, November 2013.
7. Norman E. Fenton, Member, IEEE Computer Society, Martin Neil, And Jose Galan Caballero, "Using Ranked Nodes To Model Qualitative Judgments In Bayesian Networks",Ieee Transactions On Knowledge And Data Engineering, Vol. 19, No. 10, October 2007.
8. Peter Hearty, Norman Fenton, David Marquez, and Martin Neil, Predicting Project Velocity in XP Using a Learning Dynamic Bayesian Network Model, Ieee Transactions On Software Engineering, Vol. 35, No. 1, January/February 2009.
9. Daniele Catteddu and Giles Hogben," cloud computing :Benefits, risks and recommendations for information security", The European Network and Information Security Agency (ENISA),2009.
10. Amit Sangroya, Saurabh Kumar, Jaideep Dhok, Vasudeva Varma, "Towards analyzing data security risks in cloud computing environments", International Conference on Information Systems, Technology, and Management (ICISTM 2010).
11. Xuan Zhang, Nattapong Wuwong, Hao Li ,Xuejie Zhang, "Information security risk management framework for the cloud computing environments",10th IEEE International Conference on Computer and Information Technology (CIT 2010), China.
12. P. Saripalli and B. Walters, "QUIRC: A quantitative impact and risk assessment framework for cloud security", In the Proceedings of the IEEE 3rd International Conference on Cloud Computing, pp. 280-288, 2010.
13. Jaydip Sen, "Security and privacy issues in cloud computing", Innovation Labs, Tata Consultancy Services Ltd., Kolkata, INDIA
14. Burton S. Kaliski Jr. and Wayne Pauley “Toward risk assessment as a service in cloud environments,” EMC Corporation, Hopkinton, MA, USA 2010.
15. Afnan Ullah, Khan, Manuel Oriol, Mariam Kiran, Ming Jiang, Karim Djemame , "Security risks and their management in cloud computing", 4th International Conference on Cloud Computing Technology and Science ,UK,University of York, Switzerland ,Barcelona, Spain, 2012 IEEE.

16. Saadia Drissi1, Siham Benhadou1, Hicham Medromi1,"A New Shared and Comprehensive Tool of Cloud Computing Security Risk Assessment", National High School of Electricity and Mechanics, ENSE, 2015.
17. Shareeful Islam ,Stefan Fenz , Edgar Weippl and Haralambos Mouratidis, "A Risk Management Framework for Cloud Migration Decision Support"
, J. Risk Financial Manag. 2017, 10, 10; doi:10.3390/jrfm10020010.
18. Gary Stoneburner, Alice Goguen, and Alexis Feringa ,"Risk Management Guide for Information Technology Systems: Recommendations of the National Institute of Standards and Technology", NIST Special Publication 800-30, July 2002.
19. Marit E. Kragt,"A beginners guide to Bayesian network modelling for integrated catchment management", Landscape Logic Technical Report No. 9, July 2009.
20. Symantec Security Response,"Assessing the Severity of Threats, Events, Vulnerabilities", February 2006.
21. Shen Juncai and Qian Shao," Based on Cloud Computing E-commerce Models and Its Security", International Journal of e-Education, e-Business, e-Management and e-Learning, Vol. 1, No. 2, June, 2011.
22. Fadi HajSaid, Yousef Hassouneh and Hany Ammar," Security Risk Assessment of Software Architecture", ICCTA 2011, 15-17 October 2011, Alexandria, Egypt.
23. Adam Goslin, Chief Operations Officer, PCI Compliance Updates, E-Commerce / Cloud Security.
24. Bernd Grobauer, Tobias Walloschek and Elmar Stöcker, " Understanding Cloud Computing Vulnerabilities", Aug 15, 2011.
25. Microsoft Corporation," Microsoft Dynamics CRM Online security and compliance planning guide" ,September 2013.
26. Pritesh Parekh and Joe Andrews ,"Keeping Your Cloud Secure – a CIO's Favorite".
27. Keiko Hashizume, "A Reference Architecture For Cloud Computing And Its Security Applications ",Florida Atlantic University , 2013
28. Kumar Narander and Saxena Swati ,"An Efficient Live VM Migration Technique in Clustered Datacenters", Research Journal of Recent Sciences ISSN 2277-2502 Vol. 3(IVC-2014), INDIA , 2014
29. Mahdi Aiash, Glenford Mapp, Orhan Gemikonakli, "Secure Live Virtual Machines Migration: Issues and Solutions",Advanced Information Networking and Applications Workshops (WAINA), 2014.
30. CSA, The Notorious Nine: Cloud Computing Top Threats in 2013, Top Threats Working Group, CSA, 2013.
Available:https://cloudsecurityalliance.org/download/the-notorious-nine-cloudcomputing-top-threats-in-2013