Journal of Applied Sciences

ISSN 1812-5654

science alert

ANSInet
an open access publisher
http://ansinet.com

Journal of Applied Sciences 15 (7): 953-967, 2015
ISSN 1812-5654

RESEARCH ARTICLE OPEN ACCESS

DOI: 10.3923/jas.2015.953.967

Threat Modeling Approaches for Securing Cloud Computing

[1]A. Amini, [1]N. Jamil, [1]A.R. Ahmad and [2]M.R. Z'aba
[1]College of Information Technology, Universiti Tenaga Nasional, Selangor, Malaysia
[2]MIMOS Berhad, Technology Park Malaysia, Kuala Lumpur, Malaysia

ARTICLE INFO
Article History:
Received: December 29, 2014
Accepted: April 25, 2015

Corresponding Author:
A. Amini
College of Information Technology,
Universiti Tenaga Nasional,
Selangor, Malaysia

ABSTRACT
The cloud computing delivers services of processing data by using parallel and high computational processors virtually and remotely. This is very useful and beneficial to enterprises that have limitations in terms of processing resources, data storages and man power. However, one of the main challenge in cloud computing is data security. Supposed each user has an access to the domain based on the privilege given by the server. However, an attacker always has the opportunity to bypass the privilege by exploring and exploiting every vulnerability and threat found in the cloud computing environment. A systematic approach to identify vulnerabilities and threats is thus very important to ensure only authorized party is allowed to access the data. In this study, several approaches of vulnerability and threat modeling are reviewed and found that none of them is suitable for the cloud computing environment. Therefore, authors presented a dynamic model of identifying vulnerabilities and threats in the cloud computing environment. The proposed model enables the organization to systematically identify vulnerability and threats and analyze the security risk when they use cloud computing services.

Key words: Cloud computing, data security, threat modeling, vulnerability

INTRODUCTION

Cloud computing as a new distributed computing paradigm delivers on-demand services by decreasing capital investment on infrastructure and maximizing the usage of available resources. Cloud technology brings application and infrastructure services mobility and physical/hardware platform independency to the existing distributed computing and networking application (Demchenko *et al*., 2012). By growing cloud computing and making compute resources available for consumers, IT industry becomes more flexible, scalable, capable and cost effective for developing and hosting applications. However, by adopting this new powerful emerging system, security has been cited as the most essential and critical issue. For understanding security issues, threats, vulnerabilities and risks should be analysed as different factors that influenced cloud computing security.

Threat modeling as a systematic and comprehensive analysis of threats and vulnerabilities is needed to provide confidentiality, integrity and availability for deploying cloud computing security. Threat modeling collects background information required in the form of usage scenario, external dependencies, implementation assumption, internal and external security implementation detail (Malik *et al*., 2008). A number of threat modeling techniques have been developed for evaluating and analyzing the threats and vulnerabilities such as:

- Microsoft threat modeling is a model to offer an efficient process that includes five logical steps from classifying assets to addressing and classifying threats and vulnerabilities
- Microsoft's Threat Analysis and Modeling (TAM) (Malik *et al*., 2008) is a model based on business objectives that have to be met by application. The TAM tools have been used to generate and classify threats by measuring their harm effects on system's components
- Practical Threat Analysis (PTA) (McRee, 2008) defines an effective risk mitigation plan for specific system architecture to obtain the value of system's assets
- Threat model framework and methodology for Personal Networks (PNs) (Jehangir and de Groot, 2012). This threat model by analyzing personal network gives a good view of system's assets and their values. Determining all assets by UML diagrams gives opportunity to protect data and network functions against any threats

- Threat modeling in pervasive computing paradigm by developing cloud computing, each user is faced by different security domains with multi identify. The above model presents a new threat modeling to incorporate the problem of pervasive computing environment

Unfortunately by growing cloud as a large scalable distributed computing, all above methodologies do not incorporate problems, so new approaches for threat modeling have to be evolved to solve problems of pervasive computing security.

This study presents a methodology of the threat model to deploy a secure computing environment by showing threats and vulnerabilities in the cloud computing and determining security solutions. The proposed methodology to build threat model consists of several steps, those after considering all steps the result represents the final threat model for cloud computing.

MATERIALS AND METHODS

Security issues of cloud computing: Before, a closer look is taken at cloud-specific threats, vulnerabilities and solutions, we define vulnerability and threat as follows:

- Threat is harm or unauthorized access that might occur due to vulnerability and destroy organization assets, organization operations or system information
- Vulnerability is any weakness in information system, system security procedures, internal controls or implementation that could be exploited or triggered by a threat resources (Bertino *et al*., 2010)

Cloud computing threats: Cloud Security Alliance (CSA) (Soares *et al*., 2013) as a security assurance provider released the security guidance for critical areas in cloud computing for managing risks and understanding security threats. The most of significant threats that are related to on-demand nature of cloud computing are categorized as below:

- **Data lose or leakage (T1):** This threat is measured as the most critical and terrifying threat for businesses and consumers. Any data deletion by service provider or baleful accident such as fire can lead to lose the consumer's data
- **Account or service hijacking (T2):** This weakness allows attackers to steal credentials and access to critical areas of cloud computing services. The organization should prohibit the sharing of credentials between different services and users and use strong authentication techniques
- **Insecure interface (T3):** Cloud computing's customers use Application Programming Interface (API) or software interfaces to interact and manage cloud services. Authentication, access control and monitoring technologies for APIs protect computing resources from malicious attacks
- **Denial of service (T4):** Distributed Denial of Service (DDoS) is the major security threat to availability when it comes to increase reliability of organizations on public cloud services (Lohman, 2011). On the other hand, this attack prevents users from accessing their data or applications and there is no way to reach their destination. Cloud service providers need to be sure about availability protection and customers need to be sure about the level of availability protection within a provider
- **Malicious insider (T5):** The system has been damaged by authorized employee, business partner or administrator that has access to a network or resources. This dangerous threat affects the confidentiality, integrity or availability of business information
- **Data breaches (T6):** One of the worse situations for each organization is unauthorized access or illegal viewing data by competitors. Data encryption can reduce the risk of this threat, but should be careful about encryption key because if you lose it, you will lose your data as well
- **Abuse of cloud services (T7):** Cloud computing providers do not enforce any strong registration process and any user with a valid credit card can register to receive cloud services (Hamza *et al*., 2013). Integrating of registration faint and weak fraud detection allow attacker to leverage data by offensive cloud models same as PaaS and IaaS
- **Insufficient due diligence (T8):** The cost reduction, access to pool of resources and improving security are the most important interesting factors for organization to rush cloud computing. Without understanding of Cloud Service Provider (CSP) environment, mismatched expectation has been created as a critical issue on security control of cloud computing. However, for sufficient qualification of resources, organizations have to understand the service provider offerings and risks
- **Insecure VM migration (T9):** By migrating different VMs during hybrid and federated clouds, attackers can access data illegally and transfer VM to untrusted host (Hashizume *et al*., 2013). Virtualization as the main component of IaaS is the main goal to be targeted by attackers. Trusted cloud computing and encryption technology protect data resources from insecure VM migration

Threat of shared vulnerabilities exists in all models (IaaS, PaaS, SaaS) because underlying components that deploy infrastructure, platforms and applications does not offer strong isolation between cloud computing models.

Cloud computing vulnerability: Vulnerability is a probability of an asset that will be unable to resist the action of a threat agent (The Open Group, 2009). By moving organization's critical data and applications to cloud computing, different significant vulnerabilities should be considered based on CC's

technologies, essential cloud characteristics, known security controls and state-of-the-art cloud offerings (Grobauer *et al*., 2011). In this study, indicators were discussed as cloud specific vulnerabilities:

- **Session riding (V1):** Session riding refers to send command to web application by hackers to gain unauthorized access for the information or use web service weaknesses for giving the chance to hackers to do malicious activities same as deleting of user data or sending spam to a network via internet
- **Virtual machine escape (V2):** This vulnerability allows attacker runs code on a VM that let operating system to break out and interact directly with the hypervisor to access host operating system and other virtual machines (Rouse, 2009). For detecting and preventing system should detect malicious activity at VM level
- **Obsolete cryptography (V3):** Developing not enough strong encryption or no encryption at all allows attacker to decode encrypted data. To protect system from this vulnerability, user should be sure the true data is encrypted, use proper key storage and develop a good algorithm
- **Unauthorized access to management interface (V4):** The cloud management interface has access to cloud service users to manage on-demand services. An unauthorized access enables attackers to gain total control of users and applications
- **Internet protocol (V5):** The lack of authentication methods that is not a part of the base protocol design, allows attackers to inject their malicious traffic to network. On the other hand, the IP protocol or related protocols same as UDP and TCP are vulnerable to different type of Denial of Service (DoS) attacks, including session hijacking and cash poisoning
- **Data recovery (V6):** Cloud computing allows resources to be allocated or reallocated by different users. This elastic characteristic could lead to data stolen, data breaches and other security threats. The most of organizations use third party vendors to recover data so they should consider security risk of handling data with outside company and ensure proper security vetting of the service provider (Kenyon, 2010)
- **Metering and billing (V7):** Cloud computing meters and measures services such as storage, user account and processing are used to optimize service delivery. Applicable vulnerabilities contain metering and billing data treatment and billing elusion (Rai and Bunkar, 2014)
- **Vendor lock-in (V8):** Vendor lock-in is the situation that cloud's user is dependent to a single vendor and is unable to deal with another provider without substantial and inconvenience. The lack of the standards is the main reason that users cannot transfer easily from one provider to another.

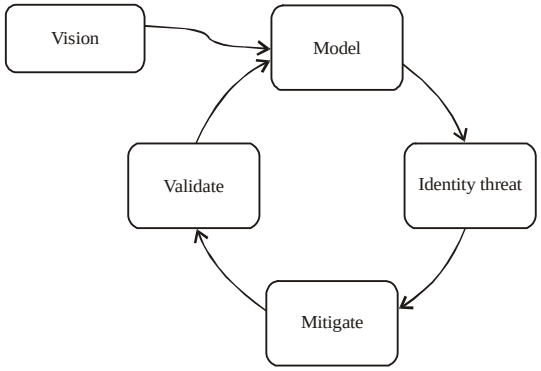

Fig. 1: SDLC process diagram

Existing threat modeling frameworks: In this section, existing threat models are discussed and new approach has been evolved to satisfy and fulfill cloud computing as a pervasive computing paradigm.

Microsoft threat modeling: Threat modeling as a core of the Microsoft Security Development Lifecycle (SDL) (Fig. 1), proposes a model to identify and mitigate threats and vulnerabilities by reducing the total cost of development process. This methodology offers a good process cycle by following five logical steps, start from classifying assets, system overview by creating Data Follow Diagram (DFD), modeling and identifying threats by using STRIDE[1], addressing issues and finally ranking the threats by DREAD[2].

Vulnerabilities as an important and hazardous security risk in cloud computing have to be addressed by threat model but Microsoft threat modeling cannot model vulnerabilities. Another important challenge to adopt this popular model with cloud computing is predefining a set of threats as STRIDE. In addition, STRIDE defines a static method to identify threats that cannot be used in dynamic computing environment. For instance, denial of service as one of the top ranked threat in 2013 was not listed as cloud computing threats in 2010. However, defining new threats which are more critical than expected STRIDE, should be intended in our new threat model.

Microsoft's Threat Analysis and Modeling (TAM): Threat Analysis and Modeling (TAM) proposes a model to identify threats and facilitate system to define a security strategy (Fig. 2) (Malik *et al*., 2008). In the first step of this model, threat modeling has been addressed on the base of business objectives. Business objectives involve business needs and problems that have to be fulfilled by the application. Components as the main part of application's architecture, technology of creating components, user roles, trust level, authentication mechanisms and external dependencies are define as a second step. In the third step, TAM's tools generate

[1]STRIDE: Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, Elevation of Privilege
[2]DREAD: Damage potential, Reproducibility, Exploitability, Affected users, Discoverability

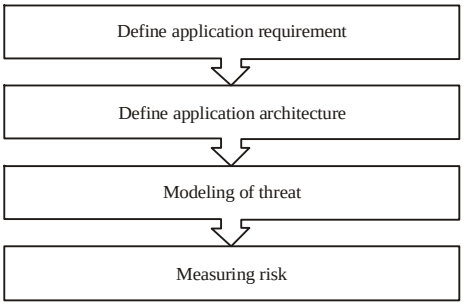

Fig. 2: TAN process diagram

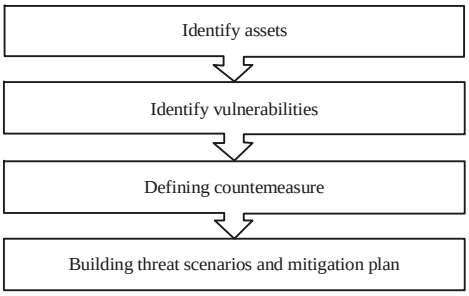

Fig. 3: PTA process diagram

and classify threats into confidentiality, integrity and availability. In the last step each threat is measured on the base of business needs.

The proposed threat modeling for computing environment unlike TAM has to determine assets which could be damaged by threats and need protection. The lack of identifying vulnerabilities is another issue of Microsoft threat analysis and modeling. On the other hand, determining and ranking threats are done as well in this model but this detecting and ranking vulnerability that are damaged by threats are not deployed.

Practical threat analysis: The Practical Threat Analysis (PTA) proposed a model to identify system vulnerabilities, map system assets, assess the risk of the threats and define an effective risk mitigation plan for a specific system architecture, functionality and configuration (McRee, 2008). The PTA by providing free tools for threat modeling allows provider to obtain system's assets values and level of damage that is caused by the attackers. The main functionality of PTA is defining a risk mitigation plan on the base of identify vulnerabilities and assets and assess the risk of threats. PTA technologies present PTA threat modeling and risk assessment that is shown in Fig. 3. Identifying assets and their financial values is done in the first step. The second step represents system's vulnerabilities on the base of architecture, functionality and different type of users. The effect of cost is calculated on the base of implementation cost. In the last step, threat scenario has been built to identify various threat and level of damage.

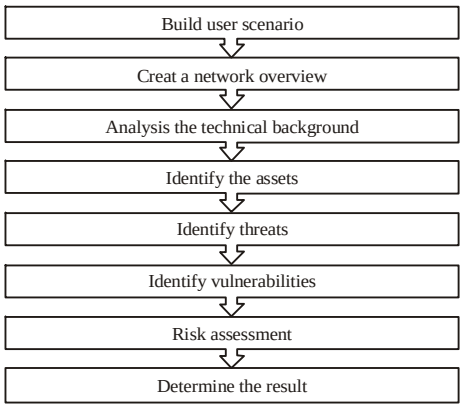

Fig. 4: Threat model for PNs

No risk evaluation method or methodology to calculate vulnerability's cost is an important issue. Actually, the cost of replacement, restoration or system down times is required to calculate the cost of vulnerabilities and thereby it gives idea to avoid system from different threats. The second disadvantage of this model is unranking vulnerability sizes. In the pervasive computing environment all known and credible vulnerabilities should be addressed. Anyway, vulnerabilities have to be ranked because known vulnerabilities can be eliminated and for unknown, some solutions should be deliberated. In PTA model, threats are ranked only by their financial values not by technical, functional, strategic or reputational values. Cloud computing as a complex multi-tenant environment, provides ability for users to be a member of different domains at the same times. In this situation, different factors and levels of security on the base of user's role should be considered to address threats not only financial values.

Threat model framework and methodology for Personal Networks (PNs): The PN as an intelligent and user-centric network consists of devices belonging to user for personal purpose, develop new application, telecommunications, entertainment and improve services (Jehangir and de Groot, 2012). Figure 4 shows primary steps of proposed threat model for PNs. Each of these main steps consists of some sub-steps (Prasad, 2007).

In the first step, the use case has been derived to describe everything in network from user's view. In the next step, the network requirements have been retrieved from use case diagrams and also network architecture, environment and technologies have been explained. In the third step, UML sequence diagram has been used to clarify data flows and determine which actors and devices are involved. The assets or everything that could be damaged should be determined and protected from harmful attacks in the next step. The fifth step involves all threats and expected result of them. The main outcome is determining threat scenario to extract fundamental threats and likelihood. After discovering threats, is possible to

see and understand vulnerabilities that are affected by terrible threats. In the seventh step, highest risks have been determined by threat and vulnerabilities profile. The final step consists of the reports that involve threats and vulnerabilities rank on the base of risk and size.

This framework gives a good view of system by describing all network details, covering all functionalities and deploying use case. As mentioned before, in cloud computing user is faced by many services and domains that may have different and unknown vulnerabilities so proposed framework unlike PN's threat model need to be updated by new threats and vulnerability profiles.

Threat modeling in pervasive computing paradigm: By cloud computing as an on-demand service, provides reliability to user's daily life. Each user has multi identifies for different security domain so implementing security schema is a big challenge for cloud computing. This model (Fig. 5) presented as a new threat modeling to incorporate the problem of pervasive computing environment (Malik *et al*., 2008).

In the first step all user's roles need to be established with their service usage and authentication mechanisms. The use case scenario and diagrams can be used in this method to identify users and their level of access to different services. In the computing environment, each user can be a part of various domains with different roles. Identifying security domains that is mentioned in step two, presents the way that user interacts with applications inside the domain. Various type of user same as authorized user, admin and unregistered user have different trust levels. Identifying trust level in the third level, assists user to access the resources depending upon its trust level. In the next step, all vulnerabilities need to be detected. Known vulnerabilities can be eliminated and unknown vulnerabilities should be consider to protect system from harm attacks. Risk evaluation as a forth step, presents fair idea to avoid computing environment from threats. Threats have been qualified on the base of cost expectancy that is involved restoration and replacement cost. In the last step, new vulnerabilities and threats have been identified and post them to forth step for keeping system secure.

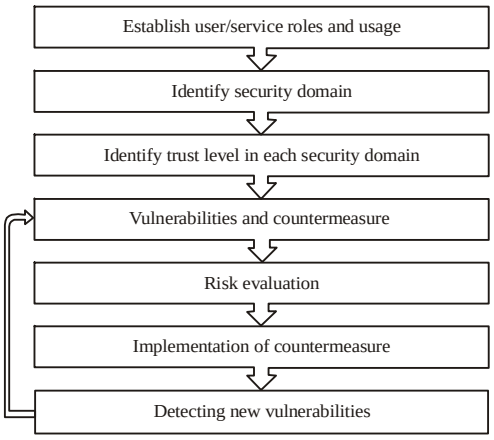

Fig. 5: Threat modeling process for pervasive computing

Today, by developing small and medium enterprises and growing the number of assets, the traditional assets tracking methods cannot be used anymore. In proposed framework unlike above model, cloud based assets management has been developed rather than traditional infrastructure to manage data, software, hardware and etc.

Before have a closer look at proposed model, we illustrate all details of discussed models in Table 1 to analyze and compare existing models by proposed model. Table 1 is based on characteristics of threat model to be adopted by cloud computing. In the next part of this study, each characteristic of new threat modeling schema was discussed to identify and rank threats and vulnerabilities.

RESULTS AND DISCUSSION

Proposed threat model: The proposed model for cloud computing security is shown in Fig. 6. This model consists of four main steps that each step involves some sub steps. The first step is identifying assets and clarifying who or what has access to assets. Trust represented by the term reliability that is using for multiple redundant web services to qualified trust between user and service provider or between different providers. Further, the second step defines capability of provider to provide user requirements literally. Identifying unique threats and addressing them by developing suitable

Table 1: Comparison of existing threat models by proposed model

	Existing threat models					
Characteristics of threat modeling	Microsoft threat modeling	TAM	PTA	Personal network threat modeling	Pervasive computing threat modeling	Proposed threat model
Identifying and classifying assets	✓		✓	✓	✓	✓
Establishing user's roles						✓
Identifying security domains					✓	✓
Estimating trustworthiness					✓	✓
Scanning domain security						✓
Identifying threat	✓	✓		✓	✓	✓
Identifying vulnerability				✓	✓	✓
Implementing countermeasure					✓	✓
Ranking and measuring threats	✓	✓		✓	✓	✓
Ranking and measuring vulnerabilities				✓		✓
Defining new assets, threats or vulnerabilities					✓	✓

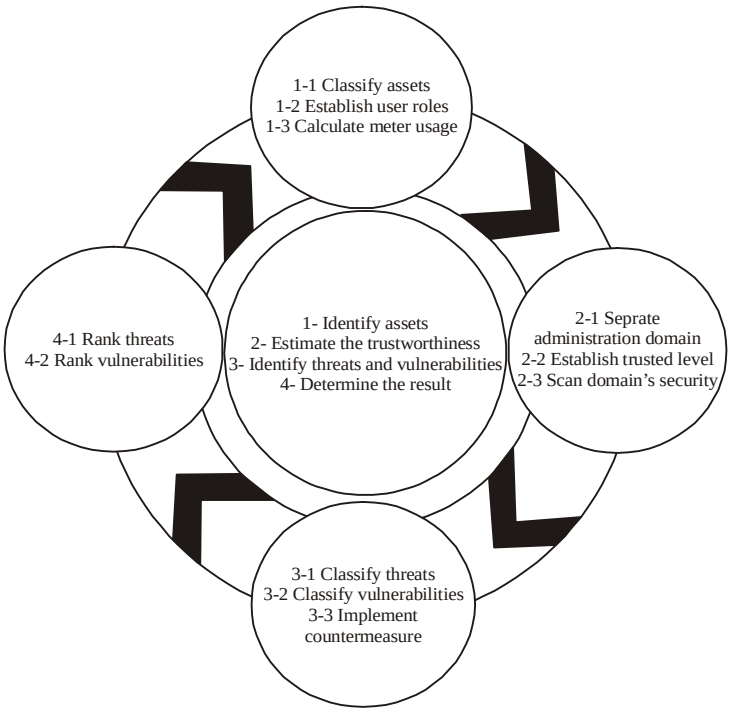

Fig. 6: Proposed threat modeling framework for cloud computing

countermeasure has been demonstrated in the third step. The main goal of this step is detecting and identifying new subsequently threats to improve security. The final step, presents system rating to identify more dangerous and effected threats and vulnerabilities.

Identify assets: The IT asset is data, software or hardware that is owned by company and used for business activities. The organizations have to be ensured these assets are accessed by authorized users and they are configured with latest security technologies to protect against security threats and vulnerabilities. The most unauthorized access or effective change during configuration management is being made by unofficial user to system. Therefore, knowing enterprises machines and their location is required to protect system from malicious attacks. Today, organizations use feasible and efficient asset management tools (SAM) to analyze their own data, software and hardware. Anyway, these tools by optimizing and managing IT assets help organization to identify what they have, control cost and risk and improve security. For discovering and monitoring assets and identifying users' roles in our suggested framework, some substeps (Fig. 6) have been proposed.

Classify assets: To implement threat modeling framework is necessary to define assets that can be damaged and need protection. The defined assets should be categorized on the base of their value that is measured by loss of availability, confidentiality and integrity types. Moreover, assets classification allows companies to store and manage their data by sensitivity and determine risks. For instance, a company has computing resource (memory, storage or CPU), encryption key, applications and customers' personal information that can be classified by different values, damage costs and trust levels. Today, most of organizations are aware of data classification significant. Every enterprise has different assets that have to be managed and classified successfully so can not specify some special and unique assets classifications for all businesses. The below mentioned and discussed assets categorizations are the most important data that by protecting them, each organization meet its final targets.

Private information: By developing social networks, personal data can be exchanged between various enterprises and users for sharing and interacting more experiences. However, private data management is a key to protect data from malicious threats. The most significance threats to offend private information have been shown in Fig. 7. The major challenges and harms for private information are collecting and extracting information by unauthorized access, using fake data for registration and lacking of controls and standards. By deploying private information manager applications more private and confidential data has to be kept secure to help enterprises to meet the acceptable level of confidentiality, integrity and availability.

Financial assets: In recent years, by developing dramatically web service technologies, more and more financial and e-commerce values are shared and accessed by users and enterprises.

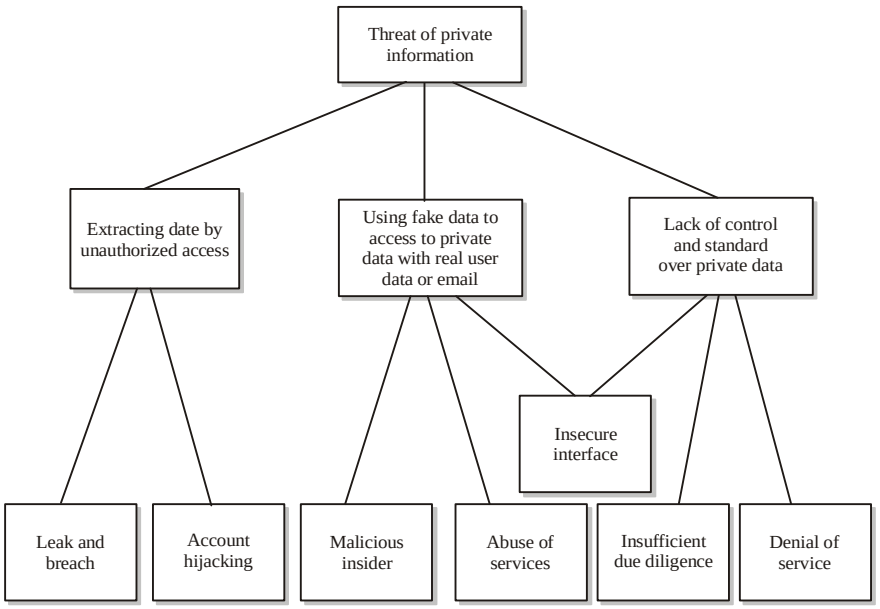

Fig. 7: Significance threats to offend privacy data

Unfortunately, this opportunity becomes the primary target for attackers to access financial assets by deploying cyber threats. For instance, Phishing and DDoS attacks are the major cyber threats that steal user financial assets same as password, bank account detail, credit card number and other confidential enterprises information. However, understanding and analyzing financial assets during threat modeling process allows enterprises to protect data from data stolen through on-line services.

Computing and network assets: This asset is an entity that is capable of creating, sustaining or destroying value at any stage in its life-cycle (Amadi-Echendu, 2004). Analyzing actual network devices or tangible assets (data center, server, desktop computer, router, switch and etc.) and providing security controls is necessary to protect system from malicious insider threats or attacks that are targeted physical assets for terrible damages. The network assets management as an on-demand service allows organization to manage risks and threats, reduce cost and increase the reliability of system.

Application assets: Applications are usually used to store, transfer and process of valuable information. For this reason, enterprises have to be sure about implementing and developing application securely. Application threat modeling by looking application as attacker's view helps enterprises to manage security risks and threats. Each application utilizes different data that allow organization to determine risk and level of expected security. For example an application consists of financial, personal information or users' account numbers. Eventually, analyzing application assets in threat modeling approach can improve security and reduce costs. Human error, malfunction, spoofing, spamming and malware as the major threats should be detected to protect other assets from malicious attacks.

Establish user's roles: Cloud computing by providing data ubiquity, flexibility of access and relicense, gives opportunity to users for accessing the required service anywhere, anytime and pay per their usage (Ryan, 2013). Each user might assume different roles in various domains, for instance a user might be an administrator with high level privilege in one domain and be a user with low level privilege in another domain. However, establishing the user roles with authentication, authorization and access control mechanisms is necessary for improving data confidentiality, integrity and availability. Nowadays, by progressing online services, organizations same as bank and insurance industry attract huge number of users. For using this excellent opportunity organization have to determine their users' roles to control accesses and improve security. In such enterprises same as bank is impossible to assign users to roles manually so some techniques like as Role Based Access Control (RBAC) assigns organization roles to user, defines privileges and supports security policies (Takabi *et al*., 2007). Furthermore, domain administrator should assign or remove roles for user or group of users on the base of requested service. For example a developer can be assigned as cloud database developer role to develop and deploy application or he/she can be assigned as a cloud user to implement an application.

By migrating more and more applications and services to the cloud as a centralized data center, CC providers are faced by more access control problems. In fact, cloud computing opportunities same as diversity and dynamicity make

authentication and authorization processes more complex because each cloud user has different access permissions in the same cloud. By the same token, using multiple services on the same cloud by the same user, the authentication and login time increase and also managing more identity process by user make system unsecure. Organization's purpose is managing different roles and assigning them to user to optimize their access control system. Eventually, some access control method same as Cloud Optimized RBAC (coRBAC) (Tianyi *et al*., 2011) merge distributed authentication services, manage organization role and user in internal network, provide individual authentication service and improve efficiency of access control systems.

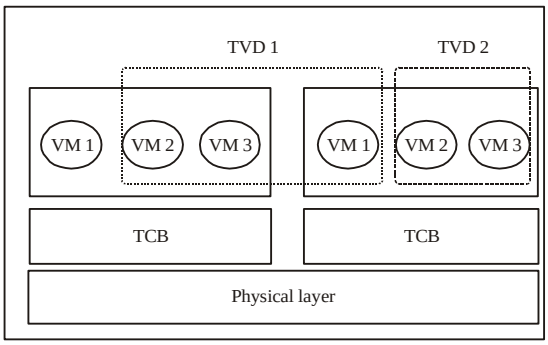

Fig. 8: TVD architecture

Meter usage: Metering and billing are two important issues that should be addressed during threat modeling framework. In computing area storage and network services have to be metered by duration and amount of used. Service Level Agreement (SLA) is a fixed cost or static method that is used as a metering mechanism. Particularly, by developing multi-tenancy and on-demand services, providers have to be used dynamic pay-per-use mechanisms in cloud computing to make bill based on dynamic tariff plan and real-time pricing (Narayan *et al*., 2012). Furthermore, dynamic metering of cloud services is to prevent wastage of compute resources and improve overall utilization of the cloud infrastructure.

The metering application improves utilization of the infrastructures, cost and management of computing resources by developing dynamic pay-per-use pricing model. These great opportunities are the major interesting factors for organizations to adopt their resources and services to cloud computing. Eventually, attackers are interested to attack system by insufficient due diligence threat and metering and billing vulnerabilities to create the critical issues on security control of cloud computing. Due to the great importance of billing and metering, we proposed to use dynamic mapping pricing and effective billing mechanisms for cloud services based on the current load on the using of cloud infrastructures.

Estimate the trustworthiness: Trust is reliability in distributed systems, among two entities that relay on their credibility to deploy trustworthiness and improve security. Nowadays, trust plays an important role to integrate heterogeneous environments for estimating trustworthiness by confidentiality, integrity, availability, reliability and authenticity (Kallath, 2005). Separating administrative domains, identifying system's vulnerabilities and developing confidence level of trust are required for determining and estimating trust among different distributed systems.

Separating administration domains: Each domain as an administrative boundary collects assets and user roles that share common trust requirements with the same system's expectations. Particularly, different domains have different security levels and different information types so is necessary to isolate domains for security reason and isolate risks from different domains (Dong *et al*., 2009). Eventually, the major challenge of security domain is an unauthorized access that prevents other domains to establish a secure relation with harmed domain.

Virtualization as the main feature and crucial technique allows computing duties, run under the virtual environment rather than physical hardware (He and Liang, 2012). Furthermore, leveraging virtualization and trusted computing technologies are required to develop threat modeling framework in distributed multi domains environment. Trusted Virtual Domains (TVD) (Fig. 8) as a coalition of virtual machines that trusted each other provides isolated computing environment, obvious trusted relationships, secure communications and transparent policy enforcement (Lohr *et al*., 2010). On the other hand, TVDs provides limited boundaries to protect distributed environment over several physical platforms. The Trusted Computing Base (TCB) by responding to present domains trustworthiness, security and TVD policy, guarantees data integrity and confidentiality in execution environment. The most important critical and complex issues that have to be addressed by TVD is satisfying business level of security by simplifying management, improving level of trust and containment.

Establish trust level: Trust level is based on varied and wide necessary trust criteria same as user's roles, offered services, assets, organization structure and technology issues in each virtual domain that offer trustworthiness as a final result. Furthermore, is difficult to understand which trust perspective can be used by domain to asses trust. The trust level in a specific environment or domain always is helpful for manager or director to make their decision. On the other hand, establishing trust between different domains is based on assessment of trust level and balance of trustworthiness among different individual domains (Msanjila and Afsarmanesh, 2007a). However, measuring trustworthiness is complex with single values or metrics so several constraints have to be met to measure trust level of each domain. Nevertheless, this study tried to present the most important elements for modeling trust level in various domains with different trust perspectives.

Users: Different users with different accesses create various trust levels in each domain. For instance, different users same as administrator, authorized users, unregistered users have different trust levels.

Trust perspectives: Each character has a unique trust perspective for deciding on useful information to assess trust level. The organization, social, financial, technology and behavior are the more identified perspectives (Msanjila and Afsarmanesh, 2007b).

Time: Trust level in each virtual domain is dynamic and depending on changes of assessment approaches same as users, assets or other factors. Eventually, time as an important factor should be addressed for modeling trust level in each domain.

Trust level assessment in each domain is the fundamental step for establishing trust relationships among different domains. The main aims of this step is ensuring the acceptable level of trust in each domain, each domain's member conform to the specified trust level, trustworthiness for each object is met and allows trust's experts to more focus on low level trust domain to identify threat and vulnerabilities. For presenting trust level in an understandable format, we can rate trustworthiness in five rating namely Strongly less trustworthy, less trustworthy, average trustworthy, more trustworthy and strongly more trustworthy (Msanjila and Afsarmanesh, 2007b).

Scanning domain security: Scanning of distributed system for management purpose is a complex task by heterogeneity and distribution of resources and tools (Sladic *et al*., 2011). By developing web services and distributed environments managing and protecting system against vulnerability is a crucial task that seeks out security faults and weaknesses by using different tools same as vulnerability scanning and firewalls. Detecting vulnerability by scanning distributed and virtual environment is used in this research to detect some dangerous gaps and weaknesses before exploiting by threats. Traditional vulnerability control center and several scanning agents in limited area. These models are obsoleted for scanning same as Nessus, X-Scan and agent-based, are using only one functional scanning entity or one scanning domain-based vulnerability scanning. In other words, only one control center handle huge amount of tasks so bottle-neck as the main issue affects system by poor accuracy and time performance (Wang *et al*., 2013). By developing distributed environment more efficient security management method is required. For this reason, it seems necessary to develop domain-oriented distributed scanning mechanism to satisfy system by high scanning efficiency, simple service providing, flexible deployment and incredible scalability (Chao *et al*., 2009). In this model, each administration domain has own scanning resources to detect vulnerabilities and all scanning resources are managed by controlling domain or integrated center. These principles allows huge amount of tasks have to be analyzed without any bottleneck and satisfy load balancing.

Identify threats and vulnerabilities: By developing information and communication technology, organizations are more interested to outsource their computational resources on virtual domains. In fact, this huge amount of data can be damaged by threats from different resources (employees' activities or malicious attacks by attackers). Therefore, management and risk assessment need to understand and analyze threats and vulnerabilities as a crucial security issues. Thus, effective security classification is necessary to identify and organize threats and vulnerabilities into classes based on the intended effect of attacks and develop solutions to prevent system from effective threats (Jouini *et al*., 2014).

There are several threat classification methods on the base of attack and attacker achievements like unauthorized access.

Threat classification: The classification of threat allows manager to protect system by identify characteristics of threats and select efficient security solution. The most of classification's approaches are based on threat definitions. On the other hand, threats are defined as a technique that is used by attacker to exploit vulnerabilities or impact system. For instance, three dimensional model (Ruf *et al*., 2003) is represented on the base of attack technique by dividing threats to three subdivisions: motivation, localization and agent (Fig. 9).

- Threat agent is the actor that imposes the threat on specific assets and is divided to human, technological and force majeure
- The threat motivation is sufficient to classify threats to answer the question 'why' a threat is created. Threat motivation is classified into two classes: Deliberate and accidental
- Threat localization represents the origin of threats, internal or external

Hybrid model or information system security threat cube classification model (Geric and Hutinski, 2007) uses classification criteria that are necessary for constantly changing environments (Fig. 10). The three main steps of this model are:

- Security threat frequency shows the frequency of security threat occurrence
- Area of security threat activity shows the main domain that is effected by the threat same as personal, physical, communication and operational security

Security threat source represents the type of threat's resource same as insider and outsiders sources.

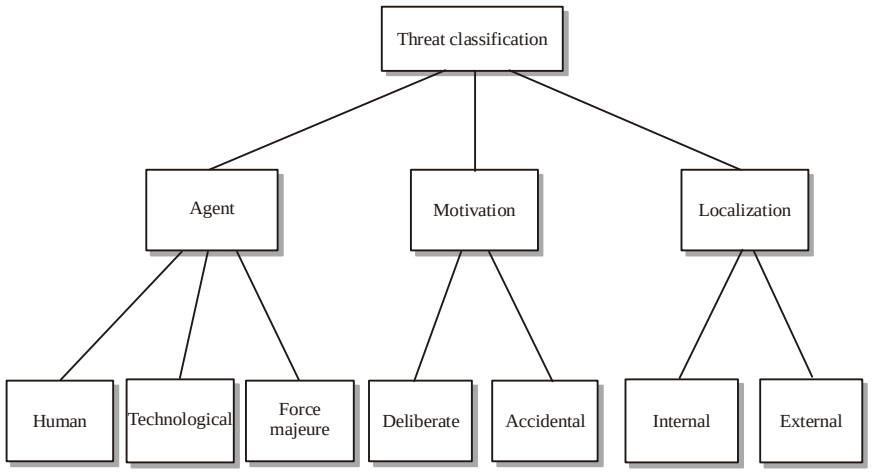

Fig. 9: Three dimension model

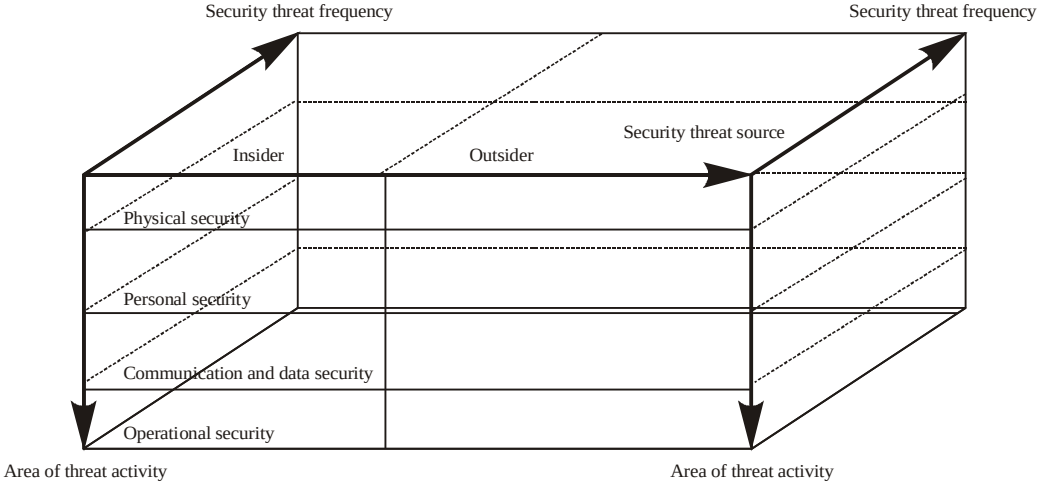

Fig. 10: Threat cube classification model

Information security threats classification pyramid (Alhabeeb *et al*., 2010) has been presented to classify threats in a dynamic environment and deliberate threats based on three factors:

- Attackers' prior knowledge about system represents the attacker knowledge about system includes system hardware, software, employees and users information
- Critically of the area represents the parts of system that are more critical than other parts of system and they can be affected by threats
- Loss represents any loss that can occur in the system by effecting privacy, integrity, business repudiation and finance loss

The proposed threat classification models are usually limited on use of criteria so, they are sufficient for stable environment where security threats are stable. Nowadays, by developing computing and virtual environments, organizations are faced by huge dynamic environment that allows different threats to attack system constantly. In this situation, dynamic classification model allows organizations to understand threats and their influence on assets and also realize area which threat could affect.

Multi-dimensions model (Jouini *et al*., 2014) (Fig. 11) is a hybrid model for information system security threat classification to combine most criteria of threats classifications. In this model threat classification is based on five basic criteria as source, agent, motivation and impact. The first level of classification consists of threat's source. In addition, environmental threat is divided to internal and external threats. The human (insider or hacker), environment (flood, fire, earthquake, wind and etc.) and technological threats (power supplies) are known as a threat agent. Actually, threat agent is the actor that affects system by brings in threat to the system. The next level is threat motivation that is the main goal of attacker to attack system. Particularly, viruses, Trojans and worms are malicious threat that is caused by

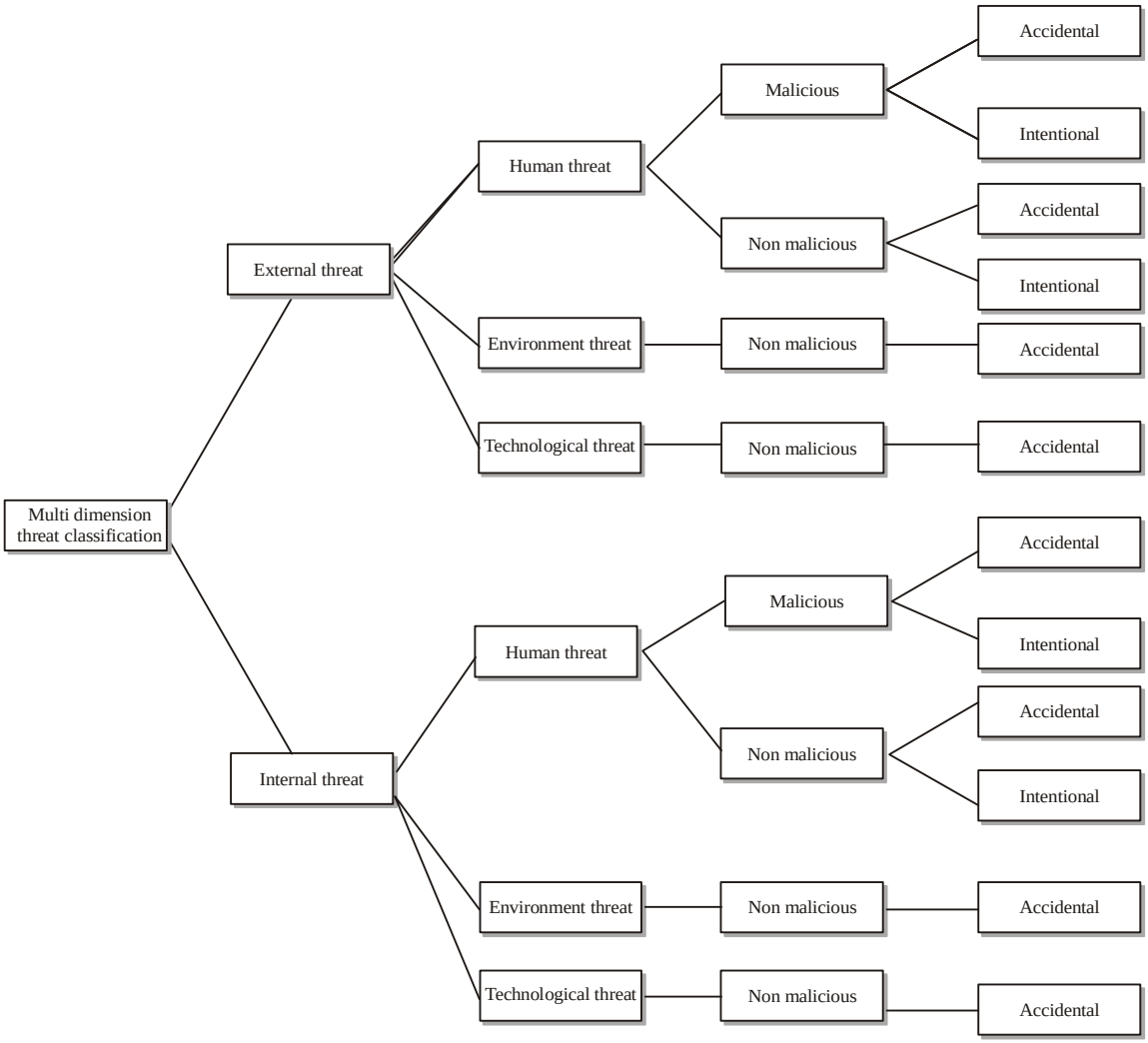

Fig. 11: Multi-dimensions model

attacker for disrupting or harming system. The vulnerabilities and errors are taking place in system because of poor security control or protocols and they are known as a none-malicious attack. The forth level of multi-dimensions model is related to user's intent that who caused the threat. International threat as a harmful decision (damage information deliberately, identity theft, ATM card crime) and accidental threat as a damage without awareness (operator mistake, coding error) are two kinds of this threat. The final part of this threat classification model is impacting threat. Each threat can cause one or many damaging impact to system same as information corruption, data loosing, disclosure of information, denial of use and data destruction.

This threat classification divides threats to different criteria to cover all security risks and allows organization to adopt large scale systems. For moving IT system to the cloud, new classes of threats have to be identified. Some of new available threats are inside trust boundary that should be considered by cloud's tenant and some else are related to cloud provider. Finally, all constraints and security issues propel managers and providers to design and adopt dynamic and hybrid threat classification model with their system to cover security risk and protect system from exploitation of vulnerabilities by threats.

Vulnerability classification: The main effect of vulnerabilities is incurring high cost for businesses by undermining degree of integrity, confidentiality, safety, availability and reliability. Classification of vulnerability helps businesses to publish, identify and analysis known and unknown vulnerabilities. For this reason, an acceptable and sufficient classification method has to follow below principles (Jin *et al*., 2009):

- **Public acceptance:** A classification model should be accepted publicly
- **Comprehensibility:** A classification has to be understood by expert and ordinary users
- **Completeness:** A classification should classify most of known and unknown vulnerabilities

Table 2: Relation between threats, vulnerabilities and their counter measure

Threats	Vulnerabilities	Countermeasure
T1	V1, V2, V3, V4, V5, V6	Data Encryption, data signature, DLP as a service
T2	V1, V3, V5, V6	Identity and Access Management (IAM) services (CSA., 2012)
T3	V1,V3,V4	Authentication (Soares *et al*., 2013), Access control (Khan, 2012)
T4	V1, V2,V4, V5, V6, V7	Apply security patches, use an IPS for monitoring, configuring firewall, minimize IP spoofing
T5	V2,V5	Cryptography, separation of duties, logging and auditing, legal contracts and insider detection models (Kandias *et al*., 2012)
T6	V1, V3, V4, V5	Stop incursions, data protection policies, automating periodic check, security event management, monitoring technologies and authenticate identities
T7	V1, V4, V5	Stricter initial registration, credit card fraud monitoring, black list monitoring (CSA., 2010)
T8	V8	Trusted Third Party (TTP), Rating cloud service provider
T9	V2	Trusted Cloud Computing Platform (TCCP) (Santos *et al*., 2009), secure protocol and live migration

- **Determinism:** A classification should have comprehensive process
- **Mutual exclusion:** A classification has to classify vulnerabilities into minimum number of classes
- **Repeatability:** A classification model can be repeatable

Now-a-days, vulnerability is known as a new opportunity for attacker to access and exploit valuable business services. Cloud computing as a multi-tenancy and distributive environment increases substantially the possibility of vulnerability exploitation. In this situation, deploying online classification of vulnerability assists businesses to protect system from reported vulnerabilities. Web Services (WS) as a core cloud technology and XML implementation of Service-Oriented Architecture (SOA) plays an important role to classify and taxonomy vulnerabilities so we should have a closer look at SOA and WS based classification approaches. On the other hand, vulnerabilities those are associated with existing technologies of cloud computing same as SOA, WS and virtualization have significant impact on the cloud. The main goals of vulnerability analysis as avoiding, finding, fixing and monitoring vulnerability leads to vulnerability classification (Lowis and Accorsi, 2009).

Berghe *et al*. (2006) proposed a vulnerability classification model on the base of system components relation and their influence on vulnerabilities. Seacord and Householder (2005) suggested a classification view based on attributes and values to protect system from vulnerability exploitation. Parrend and Frenot (2008) deployed java Service Oriented Programming (SOP) platform to classify vulnerabilities on the base of vulnerability's categorizes and goal of attacks that are based on these vulnerabilities. The ATLIST as a vulnerability analysis method was represented by Lowis and Accorsi (2009) to detect known vulnerabilities rather than new vulnerabilities. However, for categorizing vulnerabilities in cloud computing the three different services of cloud computing as SaaS, PaaS, IaaS (SPI model) have to be considered. On the base of SPI model, insecure interface, unlimited allocation of resources, data related vulnerabilities, virtual machine, SOA and WS are the main impressive vulnerabilities in cloud computing (Hashizume *et al*., 2013).

Cloud computing as a combination of different technologies is faced by huge amount of threats and vulnerabilities that force organization to consider more complex classification mechanisms than traditional method. Furthermore, traditional web services and virtualization techniques offer some solutions that are unfledged for computing environment. Nevertheless, numerating cloud's vulnerabilities may not enough and based on existing new threats and security techniques can identify more vulnerability to make system more robust.

Implementing countermeasure: The main goal of countermeasure as an action, device, procedure, technique or other measure, is reducing vulnerability and protecting assets against threats (Laorden *et al*., 2010). Regardless cloud computing services, data confidentiality, integrity and availability as the main security challenges of cloud computing present the base of countermeasures to protect critical information. On the other hand, each security countermeasure is based on the measured threat, being offered as a service in the cloud. Countermeasure as a service is identified on the base of relationship between threats and vulnerabilities (Table 2).

Determine the result: Estimating and ranking the severity of threats and vulnerabilities to inform decision about what to do to protect system from harmful effects is the last step of proposed model. Having a system to ranking threats and vulnerability is needed to save time and prevent system from more serious security risks. The result of this step can be a list or database of threat and vulnerability profiles that consist of sorted security risks.

Threat ranking: Ranking threats as a complex task is depended on various factors same as existing vulnerabilities, likelihood of attacks and potential impact of attacks. The first step for ranking threats is considering different risk factors that are posed by identified threats. On the base of threat model, various criteria have to be considered as the main exploitation factors of risks. For instance, Microsoft Threat Modeling introduces Damage potential, Reproducibility, Exploitability, Affected users and Discoverability (DREAD) as different influencing agents of a threat (Malik *et al*., 2008). The equation that is used to compute a risk value has been shown as follows:

$$\text{Risk value} = (D+R+E+A+D)/5$$

The amount of risk value is a number between 0 and 10. It means the higher number is more serious risk. The Open Web Application Security Project (OWASP) as a universal

risk rating system estimates all risks for all organization accurately. This model introduces a rating system to estimate the severity of all security risks on the base of likelihood, impact and combination of them to determine threats as the main factor of security risk. The equation that is used in OWASP is shown as follows:

$$\text{Risk} = \text{Likelihood} \times \text{Impact}$$

In this rule the risk consists of threat agents and their impact on system. The likelihood factor is estimated from a successful attack to exploit vulnerabilities. The amount of likelihood is low, medium or high (0-9). The impact as an effect of successful attack, divided to technical and business. These impacts are related to each other and each one has a set of options with different impact rating from 0-9. In the final stage, impact and likelihood estimations are putting together to calculate the overall accuracy for the risk. The OWASP by defining a dynamic system is more suitable for web services. On the other hand, this model is not based on some predefined threats same in DREAD or Trike. In any case, the customizability and adoptability of this model help businesses to produce result based on their perception about more risky threats.

Vulnerability ranking: Estimating and ranking vulnerability as a complex multi-step mechanism allows businesses to protect system from harsh attacks. The Common Vulnerability Scoring System (CVSS) (Hanford, 2007) is a universal open and standardized method for rating IT vulnerabilities. The CVSS offers evaluation metrics; base metric, temporal metric and environment metric for evaluating security status. Base metric provides original and basic attribute of vulnerabilities, environment metric evaluate vulnerabilities' metrics that are depended on the environment and temporal metric deploys dynamic aspect of vulnerabilities.

Applying CVSS to a business process cannot fully deliver optimal security measure for dynamic environments same as SOA and Web-Services (Zhao *et al*., 2011). VRank and hybrid ranking have been developed to satisfy business requirements. The VRank (Jiang *et al*., 2012) as a dynamic framework is able to integrate existing vulnerability databases with the specific detail context of business process. Accordingly, the VRank provides more specific vulnerability assessment for SOA. The hybrid ranking model proposes a combination of CVSS rating and numerical estimation of vulnerability that influence the global network (Zhao *et al*., 2011). By developing dynamic environments estimating vulnerability in an influential level and aggregating other rating models with high-level rating technics provides a hybrid model to precise measurement of vulnerabilities more economic and efficient.

CONCLUSION

This study reviewed the different existing threat modeling approaches and proposes a dynamic threat modeling method to be adopted by cloud computing. The proposed threat model allows organization to identify threats and vulnerabilities, justify countermeasures and document the more effected security risks. Unlike other models, proposed dynamic model is not based on some predefine threats. On the other hand, we plan to deploy a novel model to define new threats which are more critical than expected threats in static models. Eventually, in this research we effort to expand a dynamic threat model by respecting cloud essence as a reliability, mobility, scalability and flexibility. By considering the contribution of cloud computing in IT industries, it's obvious that cloud computing is a leading and innovative strategy to attract much attentions. However, developing and designing in-depth security techniques same as threat modeling is needed to satisfy cloud users and providers.

ACKNOWLEDGMENTS

First I would like to thank to my supervisor Dr. Norziana BteJamil for guidance and advances. She inspired and contributed me greatly to work in this study. Beside, I should like to thank the authority of University Tenaga Nasional (UNITEN) for providing good environment and facilities to complete this research. Special thanks to Assoc. Prof. Abdul Rahim Bin Ahmad, for sharing their invaluable assistance. Finally, I would specially thank to my family that support me for completing this study. Without helps of the person that mentioned above, I couldn't be success to publish this paper.

REFERENCES

Alhabeeb, M., A. Almuhaideb, P.D. Le and B. Srinivasan, 2010. Information security threats classification pyramid. Proceedings of the IEEE 24th International Conference on Advanced Information Networking and Applications Workshops, April 20-23, 2010, Perth, WA., pp: 208-213.

Amadi-Echendu, J.E., 2004. Managing physical assets is a paradigm shift from maintenance. Proceedings of the IEEE International Engineering Management Conference, Volume 3, October 18-21, 2004, Singapore, pp: 1156-1160.

Berghe, C.V., J. Riordan and F. Piessens, 2006. A vulnerability tax-onomy methodology applied to web services. Proceedings of the 10th Nordic Workshop on Secure IT Systems, October 20-21, 2005, Tartu, Estonia.

Bertino, E., L. Martino, F. Paci and A. Squicciarini, 2010. Security for Web Services and Service-Oriented Architectures. Springer, New York, USA., ISBN: 978-3-540-87742-4, Pages: 226.

CSA., 2010. Top threats to cloud computing V1.0. Cloud Security Alliance (CSA), March, 2010, pp: 1-14. https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf

CSA., 2012. Identity and access management. Cloud Security Aliance (CSA), September 2012, pp: 1-45. https://downloads.cloudsecurityalliance.org/initiatives/secaas/SecaaS_Cat_1_IAM_Implementation_Guidance.pdf

Chao, D., Y. Danfeng, Y. Yun and Y. Fangchun, 2009. A domain-oriented distributed vulnerability scanning mechanism. Proceedings of the 2nd IEEE International Conference on Broadband Network and Multimedia Technology, October 18-20, 2009, Beijing, China, pp: 831-836.

Demchenko, Y., C. Ngo, M.X. Makkes, R. Strijkers and C. de Laat, 2012. Defining inter-cloud architecture for interoperability and integration. Proceeding of the 3rd International Conference on Cloud Computing, GRIDs and Virtualization, July 22-27, 2012, Nice, France, pp: 174-180.

Dong, G., Z. Liu and D. Zhao, 2009. A security domain isolation and data exchange system based on VMM. Proceedings of the 3rd International Conference on Signal Processing and Communication Systems, September 28-30, 2009, Omaha, NE., pp: 1-5.

Geric, S. and Z. Hutinski, 2007. Information system security threats classifications. J. Inform. Organiz. Sci., 31: 51-61.

Grobauer, B., T. Walloschek and E. Stocker, 2011. Understanding cloud computing vulnerabilities. IEEE Secur. Privacy, 9: 50-57.

Hamza, Y.A. and M.D. Omar, 2013. Cloud computing security: Abuse and nefarious use of cloud computing. Int. J. Comput. Eng. Res., 3: 22-27.

Hanford, S., 2007. Common Vulnerability Scoring System (CVSS-SIG): New version of common vulnerability scoring system released. http://www.first.org/cvss

Hashizume, K., D.G. Rosado, E. Fernandez-Medina and E.B. Fernandez, 2013. An analysis of security issues for cloud computing. J. Internet Services Applic. 10.1186/1869-0238-4-5

He, Z. and G. Liang, 2012. Research and evaluation of network virtualization in cloud computing environment. Proceedings of the 3rd International Conference on Networking and Distributed Computing, October 21-24, 2012, Hangzhou, pp: 40-44.

Jehangir, A. and S.M.H de Groot, 2012. Securing inter-cluster communication in personal networks. Proceedings of the 4th Annual International Conference on Mobile and Ubiquitous Systems: Networking and Services, August 6-10, 2007, Philadelphia, PA., pp: 1-6.

Jiang, J., D. Liping, E. Zhai and Y. Ting, 2012. VRank: A context-aware approach to vulnerability scoring and ranking in SOA. Proceedings of the IEEE 6th International Conference on Software Security and Reliability, June 20-22, 2012, Gaithersburg, MD., USA., pp: 61-70.

Jin, S., Y. Wang, X. Cui and X. Yun, 2009. A review of classification methods for network vulnerability. Proceedings of the IEEE International Conference on Systems, Man and Cybernetics, October 11-14, 2009, San Antonio, pp: 1171-1175.

Jouini, M., L.B.A. Rabai and A.B. Aissa, 2014. Classification of security threats in information systems. Procedia Comput. Sci., 32: 489-496.

Kallath, D., 2005. Trust in trusted computing the end of security as we know it. Comput. Fraud Secur., 2005: 4-7.

Kandias, M., N. Virvilis and D. Gritzalis, 2012. The insider threat in cloud computing. Proceedings of the 6th International Workshop on Critical Information Infrastructure Security, September 8-9, 2011, Switzerland, pp: 99-103.

Kenyon, H., 2010. Closing an overlooked vulnerability. Government Computer News, June 9, 2010, pp: 25-27. https://www.drivesaversdatarecovery.com/images/pdf/GCN+09_06_10.pdf

Khan, A.R., 2012. Access control in cloud computing environment. ARPN J. Eng. Applied Sci., 7: 613-615.

Laorden, C., B. Sanz, G. Alvarez and P.G. Bringas, 2010. A threat model approach to threats and vulnerabilities in on-line social networks. Proceedings of the 3rd International Conference on Computational Intelligence in Security for Information Systems, November 11-12, 2010, Leon, Spain, pp: 135-142.

Lohman, T., 2011. DDoS is cloud's security achilles heel. http://www.computerworld.com.au/article/401127/ddos_cloud_security_achilles_heel/

Lohr, H., T. Poppelmann, J. Rave, M. Steegmanns and M. Winandy, 2010. Trusted virtual domains on OpenSolaris: Usable secure desktop environments. Proceedings of the 5th ACM Workshop on Scalable Trusted Computing, October 4-8, 2010, Chicago, IL., USA., pp: 91-96.

Lowis, L. and R. Accorsi, 2009. On a classification approach for SOA vulnerabilities. Proceedings of the 33rd Annual IEEE International Computer Software and Applications Conference, Volume 2, July 20-24, 2009, Seattle, WA., pp: 439-444.

Malik, N.A., M.Y. Javed and U. Mahmud, 2008. Threat modeling in pervasive computing paradigm. Proceedings of the Mobility and Security, New Technologies, November 5-7, 2008, Tangier, pp: 1-5.

McRee, R., 2008. PTA: Practical threat analysis. Information Systems Security Association, September 2008, pp: 37-40.

Msanjila, S.S. and H. Afsarmanesh, 2007a. Modelling trust relationships in collaborative networked organisations. Technol. Transfer Commer., 6: 40-55.

Msanjila, S.S. and H. Afsarmanesh, 2007b. Towards Establishing Trust Relationships among Organizations in VBEs. In: Establishing the Foundation of Collaborative Networks: IFIP TC 5 Working Group 5.5 Eighth IFIP Working Conference on Virtual Enterprises September 10-12, 2007, Guimaraes, Portugal, Camarinha-Matos, L.M., H. Afsarmanesh, P. Novais and C. Analide (Eds.). Springer-Verlag, Berlin, Germany, ISBN: 978-0-387-73798-0, pp: 3-14.

Narayan, A., S. Rao, G. Ranjan and K. Dheenadayalan, 2012. Smart metering of cloud services. Proceedings of the IEEE International Systems Conference, March 19-22, 2012, Vancouver, BC., pp: 1-7.

Parrend, P. and S. Frenot, 2008. Classification of component vulnerabilities in Java Service Oriented Programming (SOP) platforms. Proceedings of the 11th International Symposium, Component-Based Software Engineering, October 14-17, 2008, Karlsruhe, Germany, pp: 80-96.

Prasad, N.R., 2007. Threat model framework and methodology for Personal Networks (PNs). Proceedings of the 2nd International Conference on Communication Systems Software and Middleware, January 7-12, 2007, Bangalore, pp: 1-6.

Rai, P.K. and R.K. Bunkar, 2014. Study of security risk and vulnerabilities of cloud computing. Int. J. Comput. Sci. Mobile Comput., 3: 490-496.

Rouse, M., 2009. Virtual machine escape. http://whatis.techtarget.com/definition/virtual-machine-escape

Ruf, L., A. Thorn, T. Christen, B. Gruber and R. Portmann, 2003. Threat modeling in security architecture: The nature of threats. https://www.isss.ch/fileadmin/publ/agsa/ISSS-AG-Security-Architecture__Threat-Modeling_Lukas-Ruf.pdf

Ryan, M.D., 2013. Cloud computing security: The scientific challenge and a survey of solutions. J. Syst. Software, 86: 2263-2268.

Santos, N., K.P. Gummadi and R. Rodrigues, 2009. Towards trusted cloud computing. Proceedings of the Conference on Hot Topics in Cloud Computing, June 14-19, 2009, Berkeley, CA, USA.

Seacord, R.C. and A.D. Householder, 2005. A structured approach to classifying security vulnerabilities. Technical Note CMU/SEI-2005-TN-003, Camegie Mellon Software Engineering Institute, Pittsburgh, PA., USA., January 2005.

Sladic, G., M. Vidakovic and Z. Konjovic, 2011. Agent based system for network availability and vulnerability monitoring. Proceedings of the IEEE 9th International Symposium on Intelligent Systems and Informatics, September 8-10, 2011, Subotica, pp: 53-58.

Soares, L.F.B., D.A.B. Fernandes, M.M. Freire and P.R.M. Inacio, 2013. Secure user authentication in cloud computing management interfaces. Proceedings of the IEEE 32nd International Performance Computing and Communications Conference, December 6-8, 2013, San Diego, CA., USA., pp: 1-2.

Takabi, H., M. Amini and R. Jalili, 2007. Trust-based user-role assignment in role-based access control. Proceedings of the IEEE/ACS International Conference on Computer Systems and Applications, May 13-16, 2007, Amman, pp: 807-814.

The Open Group, 2009. Risk Taxonomy. The Open Group, London, UK., ISBN: 1-931624-77-1, Pages: 39.

Tianyi, Z., L. Weidong and S. Jiaxing, 2011. An efficient role based access control system for cloud computing. Proceedings of the 11th IEEE International Conference on Computer and Information Technology, August 31-September-2, 2011, Paphos, Cyprus, pp: 97-102.

Wang, S., Y. Gong, G. Chen, Q. Sun and F. Yang, 2013. Service vulnerability scanning based on service-oriented architecture in web service environments. J. Syst. Architecture, 59: 731-739.

Zhao, F., H. Huang, H. Jin and Q. Zhang, 2011. A hybrid ranking approach to estimate vulnerability for dynamic attacks. Comput. Math. Applic., 62: 4308-4321.