Novel Attack Tree Analysis Scheme to Assess the Security Risks on the Cloud Platform

Shin-Jer Yang, Ya-Hui Yeh

Dept. of Computer Science and Information Management, Soochow University, Taipei, Taiwan
cssjyang@scu.edu.tw, 03756014@mss.scu.edu.tw

Abstract

The security issues derived from cloud platforms are more serious, and this identifiable vulnerability risk classifies the threat paths and identifies and assesses the possible attack paths. Therefore, we employ the basis of Extended Attack Tree (EAT) Analysis and further propose the Novel Attack Tree (NAT) Analysis scheme to calculate the threat and vulnerability events that affect the Cloud Platform Service Security incidents through the characteristics of the NAT Analysis to defend and detect these security events.

This paper utilizes the NAT Analysis proves that it can effectively assess the risk value on the cloud platform. According to threat report of the Cloud Security Alliance (CSA), after it simulates the risk factors of the cloud platform to obtain the threat path, then performs quantitative analysis on the impact of assets with the NAT Analysis. Finally, it obtains the weight of the risk value and sorts the level according to the value and further illustrate the comparison with the EAT Analysis. The proposed NAT Analysis can improve an information security risk analysis that the EAT Analysis cannot fulfill, and it can also increase the availability of risk assessments and is expected to bring more secure cloud services to the Cloud platform.

Keywords: Novel attack tree analysis, Cloud security risk analysis, Information security, Cloud platform

1 Introduction

Technology breakthroughs allow services using "Cloud Computing" to move toward more diverse developments. "Cloud Computing" is a resource pool that is accessible through the Internet, which allows the user to access flexible and convenient computing resources based on the user's needs from the Cloud Service Provider (CSP) and the user's flexible requirements. With use of the cloud environment, with the increasing use of the cloud environment, the use habits of people on network services are changing, the use habits of people from web-based applications are more dependent and gradually follow the services provided by the cloud environment. To find a way to solve cloud platform security issues, the CSP also began to view the cloud platform information security risks caused by the threats and vulnerability seriously, facing endless cloud platform security issues, based on the above Attack Tree that extends the application of the described attack characteristics using a tree structure to assess the risk existing in the information system. The paper uses the Extended Attack Tree as the structure of risk analysis, further proposing a Novel Attack Tree (NAT) Analysis in this paper to assess the corresponding relationship of information security issues.

The scope of this study is information security risk analysis of cloud platforms, used in web-based systems as the Extended Attack Tree (EAT) Analysis risk assessments [1-2] cannot fulfill current cloud platform architecture and risk assessments, and further proposes an improvement strategy using the NAT Analysis, through the risk evaluation of simulating, deriving, quantifying, and analyzing the threats and vulnerabilities that impact the cloud platform. The proposed NAT Analysis is more appropriate for Information Security Risk Assessments and also strengthens the risk detection and defense on the Cloud Platform. The main purposes of this paper are as follows:

- EAT Analysis that targets the Attack Tree and web-based website system for risk assessment was improved, thereby proposing NAT Analysis that studies the risk of cloud platform information security and explaining and comparing the difference between NAT Analysis and EAT Analysis.
- With the cloud platform's resource sharing and virtualization technology characteristics, and through NAT Analysis targeting vulnerability, threats, and other risk factors affecting the cloud platform, risk identification and risk value weight quantification were carried out to analyze impacts arising from potential risk factors and establish a safe quantitative assessment model.

*Corresponding Author: Shin-Jer Yang; E-mail: cssjyang@scu.edu.tw
DOI: 10.3966/160792642019072004003

- The algorithm of NAT Analysis was applied to simulate and analyze information security risks, which serves as the cloud platform security assessment model implemented in this study: (a) Collect and study the cloud platform vulnerability, threats and other risk factors; (b) use Attack Tree+ Software from Isograph Company in order to simulate and drive at the NAT Attack Tree; (c) calculate risk weights and rank the risk values.
- Put forward key assessment indicators to analyze the empirical results.
- In summary, NAT Analysis is applied to analyze and evaluate research on security risks on the cloud platform.

The remainder of this paper is as follows. Section 1 describes the research background and purpose. In Section 2, we survey the related studies in BSI Standards ISMS and the Attack Tree as well as the research background and their application. Section 3 explains the security risk framework and proposes the design issues of the NAT Analysis. In Section 4, we set up simulation procedures and perform experiments that calculate the quantitative risk weight value analysis. Finally, we make a conclusion and indicate the future research direction in Section 5.

2 Related Works

2.1 Information Security Risk of Cloud Platform

Gartner International Research and Advisory pointed out that "Cloud services have large and scalable IT service resources that provide information to external users through Internet technology." The "National Institute of Standards and Technology (NIST)" described Cloud Computing as using a dynamic allocation method of resource pooling and can extend Computing Methods and MapReduce, Hadoop processing information capability and technology, and it achieves operating procedure analysis, distribution, and sorting through the high-speed network exchange server groups to provide highly efficient computing power [3]. How to ensure the quality assurance of service security and to protect the user's data security and confidentiality as the basis, etc., are playing a very important role in the trend of cloud information security development. The current top 10 cloud service security risks on the cloud services provision assessment are as follows [4-5]:

- Accountability and Data Ownership
- User Identity Federation
- Regulatory Compliance
- Business Continuity and Resiliency
- User Privacy and Secondary Usage of Data
- Service and Data Integration
- Multi-Tenancy and Physical Security
- Incidence Analysis and Forensic Support
- Infrastructure Security
- Non-Production Environment Exposure

Since its founding, Cloud Security Alliance (CSA) has successively published "Security Guidance for Critical Areas of Focus in Cloud Computing" and "Security as a Service Guidance" with the cloud information security threats brought forward by the CSA on the cloud computing, and the CSA report lists the top nine risks as including Data Theft, Loss of Data, Service Traffic Hijacking, Insecure Interfaces and API, Denial of Service, Malicious Insiders, and Use of Cloud Resources by Hackers, Lack of Foresight, Adjacent Vulnerability.

2.2 Risk Management in Security

Security level is based on the importance of its classification in the Information Security Management System (ISMS) as follows [6]. Asset Identification, Confidentiality, Integrity, Availability, and Accountability (CIAA) of Asset Identification, identify a major threat and its vulnerability, assess the likelihood of threats and vulnerability, calculate and assess risk values based on defined standard risks. This study is based on BSI Standards ISMS, the most authoritative and representative standards of protecting information security internationally. An increasing number of security risks exist with the cloud environment, including deliberate attacks, invasion, Distributed Denial of Service (DDoS), fire and a wide range of threats, there are still security challenges and risk issues in cloud computing [7]. Since the cloud platform environment was not planned and installed according to the security system, under its limitation, information security defenses must be created through additional means and techniques, such as a strict management system and detection programming to achieve the protection defense mechanism.

However, the cloud computing must address several technology and security challenges to turn this vision into reality for enabling future Internet of services [8]. Hence, the previous authors survey details the security issues that arise due to the very nature of cloud computing. Also, the survey presents the vulnerabilities and threats that are very essential to support and improve more security and efficient quality of service (QoS) under cloud platform [9]. In [10], the proposed SOC platform with SLA (Service Level Agreement) is to handle and supervise all the security service processes under different levels of cloud security enforcements according to data center scales, business properties, and existing information security functions.

2.3 Introduction to Attack Tree

The Attack Tree is a concept of a multi-leveled Tree Structure, using a tree structure to perform

vulnerability events analysis of probable occurring information security risk combinations, and identifying the assumed problem occurrences of threat events. It uses graphs to display the combination of child nodes and root nodes, interacting with the display the path of the target which is being attacked, from the root node as the top of the tree down to the child node, the top root node represents the attacker's target, the leaf nodes of the tree's bottom level represents one or more activity paths; in the tree structure, the leaf node is the logical relation "OR," which represents when any one of the leaf nodes is "OR"; the upper root node identifies that the threat exists; the logical relation "AND" represents all leaf nodes must be "AND"; then the threat exists; the collection of events can be called the Attack Condition. Ping Wang [11] proposed an Attack Defense Tree (ADT) that considered the attack cost and defense cost, to solve the risk analysis issue through the indicator of effectiveness, to assess and mitigate the threats existing in cloud security risks.

3 Design Issues in Novel Attack Tree Analysis

This section examines the framework in security risks and also proposes a research method for the NAT Analysis.

Since the EAT Analysis cannot carry out complete detection and defense information risk analysis and assessment targeting the complex cloud environment, the NAT Analysis and EAT Analysis were compared in terms of their differences in functional benefits. The NAT Analysis proposed in this study has integrated the advantages of the EAT Analysis and has improved its shortcomings, making it applicable in more complex cloud platform information security risk analysis behaviors and giving it a complete assessment model. In addition, the NAT Analysis has also improved the EAT Analysis used purely in research on information security risk with a Web site as the risk assessment environment, as shown in Table 1.

Table 1. Comparative Features of NAT and EAT Analysis

Evaluation of indicators	NAT Analysis	EAT Analysis
Relevance	Analysis of the vulnerability and threats risk damage to the cloud platform.	By the relevance of the various stages of each attack, to evaluate the combination of threats.
Risk assessment objectives	In accordance with the collection of vulnerability and threats analysis and the vulnerability, threat paths identify the most value.	According to the goals, sub-goals, weakness, attacks on four levels and classifications.
Risk quantification assessment	NAT algorithm to calculate the threat path, and then according to the risk value to calculate the degree of risk impact.	Algorithm for attack path, calculate the combination of multiple threats.
Risk assessment range	Vulnerability intersects with the threat assessment.	Threat as a unit.
Risk analysis application	To Cloud Platform environment risk assessment, for the study of capital risk.	To Web-based site environment risk assessment, for the study of capital risk.

3.1 Evaluation Framework in Security Risk

The framework as shown in Figure 1 is to illustrate the following key five operational procedures in security risk for NAT.

Step 1: Risk Identification – The Step I should input the related risk factors.

Step 2: Risk Detection – This step is to examine the operational flow for designing the NAT algorithm.

Step 3: Risk Analysis – The Step 3 can derive the NAT Attack Tree based on the NAT algorithm listed in Step 2.

Step 4: Risk Processing - This step is to treat Security assessment.

Step 5: Monitoring Risk Management - This step is to monitor and control all the operations of other steps in security risk.

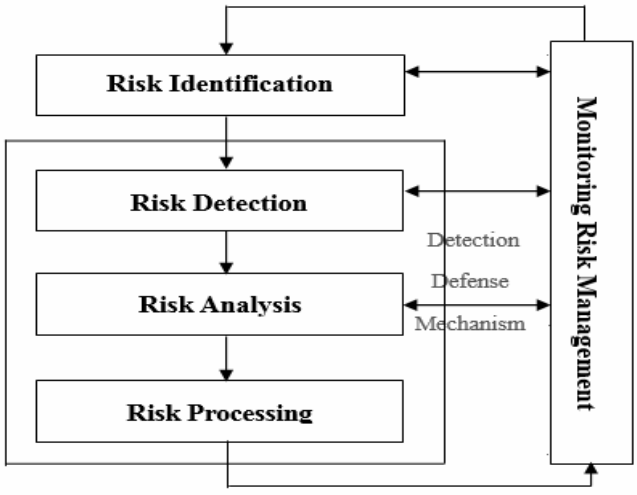

Figure 1. NAT analytical work flow chart

3.2 Operations Principle in NAT Analysis

In response to the resource sharing and technical structure complexity of the cloud platform, the Novel Attack Tree (NAT) is used as the basis to extend the application to the risk analysis on the cloud platform. Attack Countermeasure Trees (ACT) proposed in Arpan Roy [12] use model and analysis. ACT can develop countermeasures at any node of the tree, not just at the leaf nodes in defense, and can also use its minimum subsets facing an attack scenario to perform probabilistic analysis on the probability of an attack and impact at the target nodes [13-16]. This methodology of this paper combines the theory and feature of risk management, simulates risk factors in the cloud platform and designs the threat defense algorithm of NAT, and then quantifies the probable combinations of various threats and risk values as the target of risk assessments. Based on the Figure1, it is necessary to propose the treatment and controlling of defense countermeasures on the security risk for the NAT as depicted in Figure 2. This Figure 2 is to achieve the task of minimizing the security risk through the task of monitoring risk management.

Figure 2. NAT operation diagram of analytical method

3.3 Design of NAT Analysis Algorithm

The Targeting the Attack Tree and EAT Analysis is the bases, and the Attack Countermeasure Trees (ACT) proposed by A. Roy uses a combination of a model and analysis network to establish attack countermeasure technology, with the ability to use minimum subsets in ACT in the face of attack scenarios. The minimum subsets attack strategy tree uses the BSI risk management framework and procedure as references and adopts Plan, Do, Check and Action modes to import management system norms into cloud platform vulnerability and treats, while placing the detection mechanism and risk processing design in the cloud platform security assessment processes and continually maintain improvement by applying NAT Analysis on the cloud platform for information security risk analysis and security assessment uses. Hence, the NAT Analysis algorithm can be designed as follows.

3.4 Assessment of Risk Quantification

A risk value involves the use of a system impact caused by threat success probability and threat *i* to calculate the vulnerability incidence of each node (L_i) and threat incidence (T_i) risk value. Vulnerability corresponding to threat is the degree of impact on the cloud platform likely caused by the establishment of risk analysis and detection, which are: known vulnerability L and the potential vulnerability in the cloud platform system *PL, known threat T* and the potential threat *PT* in the cloud platform system becoming any node *i* with the equation computed as: known vulnerability L multiplied by potential vulnerability *PL* equals vulnerability incidence (L_i), and known threat T multiplied by Potential Threat *PT equals* threat incidence (T_i). The calculations of the impact and degree of effect caused on the cloud platform at any node *i* are shown in Equations (1) and (3). In addition, the calculations of total vulnerability (L_t) and total threat (T_t) are shown in Equations (2) and (4).

$$L_j = L * PL_j \tag{1}$$

$$L_t = \sum_{j=1}^{n} L_j \tag{2}$$

$$T_j = T * PT_j \tag{3}$$

$$T_t = \sum_{j=1}^{n} T_j \tag{4}$$

Equation (1) and (3) is the calculation for the possibility and degree of threat impact of vulnerability incidence (L_i) and threat incidence (T_i) at every node. The assessment in Equations (2) and (4) is based on the risk value of the cloud platform and calculates the risk value of the impact and degree of effect caused on the cloud platform. Additionally, according to the risk management BSI security management steps, the threat impact level is established as the security assessment model of the NAT Analysis.

3.5 Simulations Procedure Design

The NAT Analysis algorithm was used to define the risk detection mechanism, simulate, derive and establish the Attack Tree structure, listing the vulnerability and threat, and reporting all the risks to setup a risk attack diagram. By simulating the vulnerability incidence (L_i) and threat incidence (T_i) of every node, the outputted simulation results include: likelihood, impact, node path and risk. Risk analysis was further carried out as the security assessment model.

The design overview of the empirical simulation procedures in this paper is as depicted in Figure 3, and the procedures are briefly explained below:

(1) Risk Identification: Input parameter setting in the simulation procedure: This paper collected, compiled and identified the risk factors in the corresponding vulnerability and threat table in order to carry out simulation

Algorithm Novel-Attack-Tree ()

Input :

String source; //Source vertices
String[] include node; // Node threats processing
String[] promising; // Judgement the threat
int *i*; // Impact on any node *i*
int *r*; // Node threat by rate
int *x*; // System impact rate
int *L*; // Known vulnerability
int *PLi*; // Potential vulnerability node *i*
int *T*; // Known threat
int *PTi*; // Potential threat on node *i*

An Novel Attack Tree P with *r* being the root
// Risk suffering the threat of rate and impact of the vulnerability.

Output :

To complete NOVEL-Attack-Tree Analysis.
// Node path *PGate.*

Method:

For *i* =1 ,..., *n* //Assume *n* nodes (or events) in a NAT
include node [*L*, *T*, (*i*)]
call procedure Defense-detection (*L*, *T*, (*i*))
void check node (*i*) {node (*Pr*);
if (promising (*i*)) {
//Determines whether the left node as a threat
let source vertices be the *x*
for each node = 1/*x* in Novel Attack Tree do
check node (*Pr*); // Check each child node the risk of rate
else { int *r* = *i*
if *r* is the OR node the source vertices of *i* the minimum subsets
//To calculate the minimum subsets of threats OR associated node
return (*Pr*) = OR node
if *r* is the AND node source vertices of *i* the minimum
subsets //Calculate the minimum subsets of threat AND associated.
return (*Pr*) = AND node
While *x* is not a source vertices //Most recursive scan a threat by node
let *r* be a vertices of *x* with maximum (*Pr*)
then *r* = *x*
}END if
return promising (*i*); END For
}END
Procedure Defense detection [*L*, *T*, (*i*)]
void sum_of_ sub_goals (index *i*, int *L*, int *T*){
if (promising (*i*)) //Probing to see whether *i* threat paths.
if (*P* == 1) cout << include[*i*] ;
//Lists all the risk-reward
else {
String[] include[*i*] >="*L*";
//Determine vulnerability incidence, expand the left Leafs.
sum_of_subsets (*i*);
String[] include[*i*]< = "*T*";
//Determine threats incidence, expand the right Leafs.
sum_of_subsets (*i*);
}END if
return promising (*i*);
}END Procedure Defense detection
}

END Novel-Attack-Tree

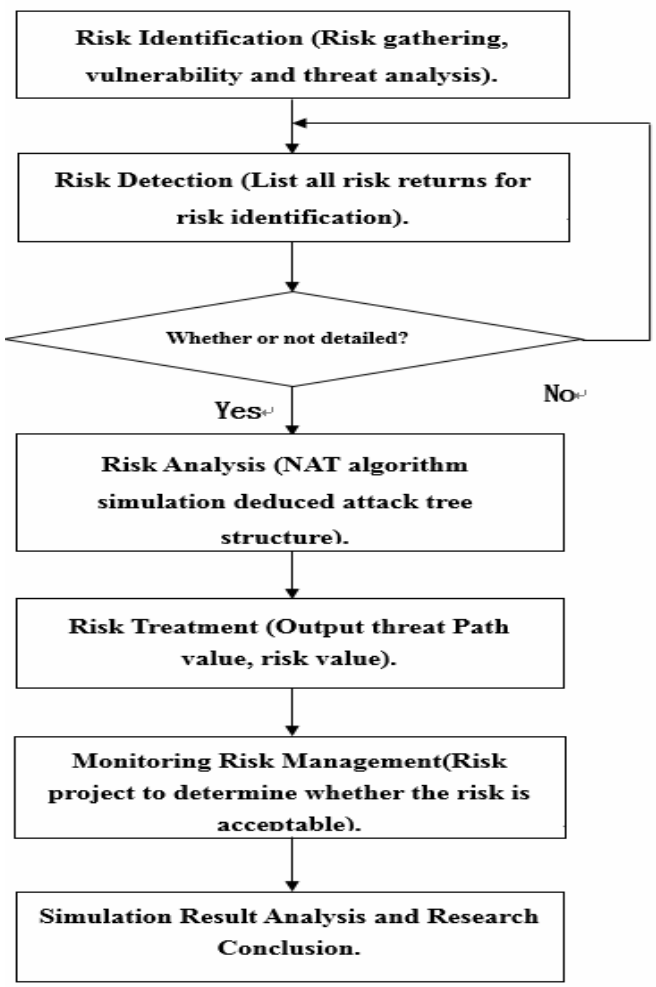

Figure 3. Simulations Procedure Chart

(2) Risk Detection: The minimum subsets between vulnerability and threats were calculated. After listing and reporting all the risks, the threat incidence and vulnerability incidence were confirmed to be risks identified.

(3) Analysis: According to the algorithm of NAT Analysis the NAT Attack Tree structural diagram was derived to establish a risk attack diagram. The vulnerability and threats that existed in each risk item underwent analysis.

(4) Risk Treatment: The targets, paths, vulnerability, threats and other risks likely to cause an impact on the cloud platform underwent security assessment processing in two stages through Attack Tree+ Software simulation output results and based on the weight design: 1. The first stage is to sequence high-risk event nodes arranged by likelihood and impact; 2. The second stage includes two key assessment indicators: node path and risk.

(5) Monitoring Risk Management: After conducting a security assessment by risk analysis, the quantified risk level is identified individually, and whether information security risk can be accepted by the cloud platform is determined.

(6) Simulation Result Analysis and Research Conclusion.

3.6 Empirical Analysis

(1) Risk Analysis of Simulated Cloud Platform Threat Factors

The difference between the risk factors of vulnerability and threats: Vulnerability is defined as the unlawful acquisition of internal information, system security loopholes and flaws exploited intentionally or unintentionally, loopholes being undetected or potential vulnerability unrepaired, resulting in exploitation by threats and consequentially leading to an external attack event. The identification of threats refers to a system being subject to attack or cyber espionage, zero-day attack actions, or Distributed Denial of Service (DDoS), causing network outages or even virtual machine service failures or malfunction and resulting in disastrous immediate restoration failure. In order to ensure accurate determination standards for subsequent NAT simulation derivation of information society risk assessment, a risk level rating of the cloud platform information security risk level was established, with its risk levels (1~5; 1 is the lowest; 5 is the highest) to score its impact on cloud platform information security level, as shown in Table 2.

Table 2. Cloud platform risk analysis

Project		Events	Risk Level
EV01	Vulnerability	Unauthorized Access to Management Interface	4
EV14	Threat	Management Interface Compromise	
EV02	Vulnerability	Weak Authentication Scheme	5
EV15	Threat	Cloud provider malicious insider	
EV03	Vulnerability	Weak Credential-Reset Mechanisms	5
EV16	Threat	Data Leakage on Up/Down	
EV04	Vulnerability	Vulnerabilities of Shared Network	2
EV17	Threat	Compromise Service Engine	
EV05	Vulnerability	Computational Resource Vulnerabilities	2
EV18	Threat	Resource Exhaustion	
EV06	Vulnerability	Injection Vulnerabilities	3
EV19	Threat	Distributed Denial of Service	
EV07	Vulnerability	Internet Protocol Vulnerabilities	3
EV20	Threat	Web Services Routing Issues	
EV08	Vulnerability	Session Riding and Hijacking	3
EV21	Threat	Undertaking Malicious Probes or Scans	
EV09	Vulnerability	Metering and Billing Evasion	1
EV22	Threat	Economic Denial of Service	
EV10	Vulnerability	Data Recovery Vulnerabilities	3
EV23	Threat	Intercepting Data in Transit	
EV11	Vulnerability	Storage-Related Vulnerabilities	1
EV24	Threat	Isolation Failure	
EV12	Vulnerability	Denial of Service by Account Lockout	4
EV25	Threat	WSDL Scanning and Enumeration	
EV13	Vulnerability	Weak Credential-Reset	5
EV26	Threat	Loss of Encryption keys	

(2) Derivation of NAT Analysis

The bottom of the simulation environment in this paper is virtual host VirtualBox 5.0, with the Windows 10 operating system and the reinstalled simulation tool is Isograph Company's target development of the

reliability-series Attack Tree+ Software 3.0 version of the world's most widely used threat analysis software [17]. First, in the simulation environment, vulnerability, threats and other risk factors whose information security risk deems hazardous were inputted into the simulation environment, thereby logically deriving the cloud platform risk threat path diagram through the NAT Analysis algorithm. The likelihood of vulnerability and threats was then obtained. Through the simulation tool of Attack Tree+ Software 3.0, the risk value of each node was computed, as depicted in Figure 4 and Figure 5.

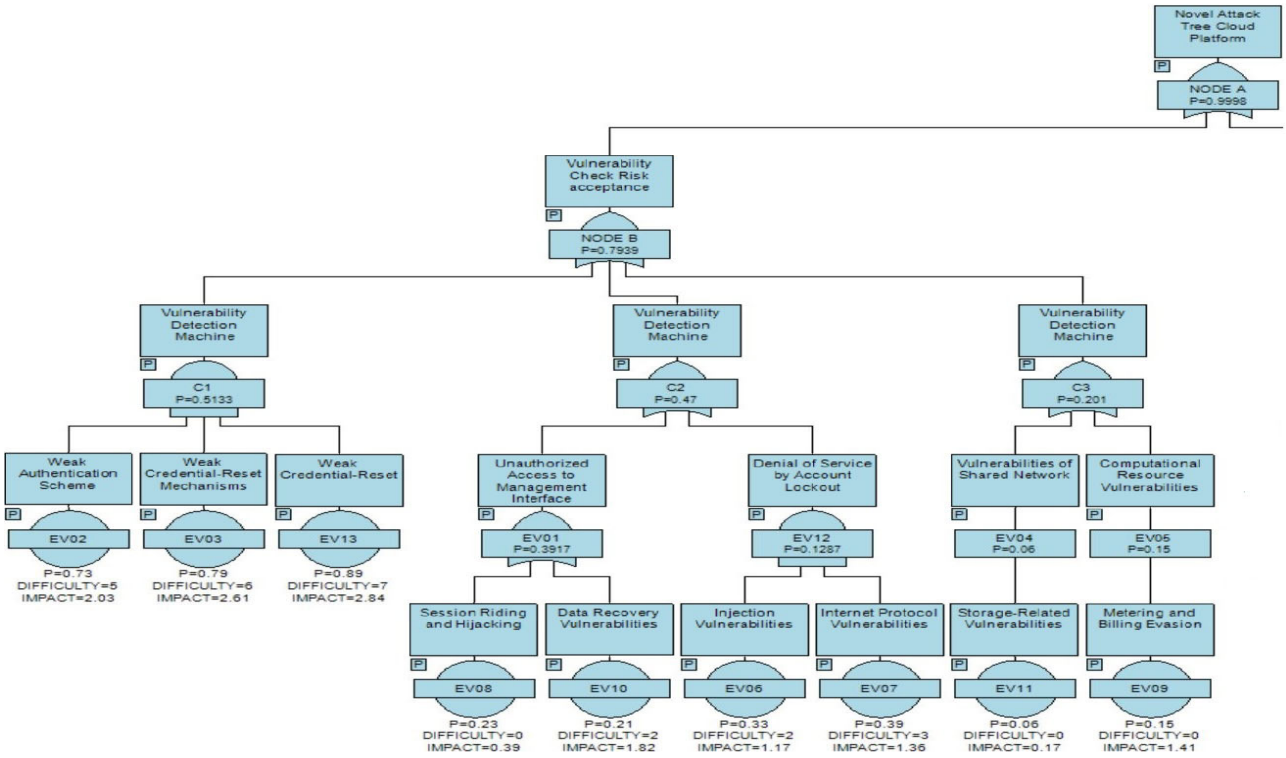

Figure 4. NAT Vulnerabilities are derived

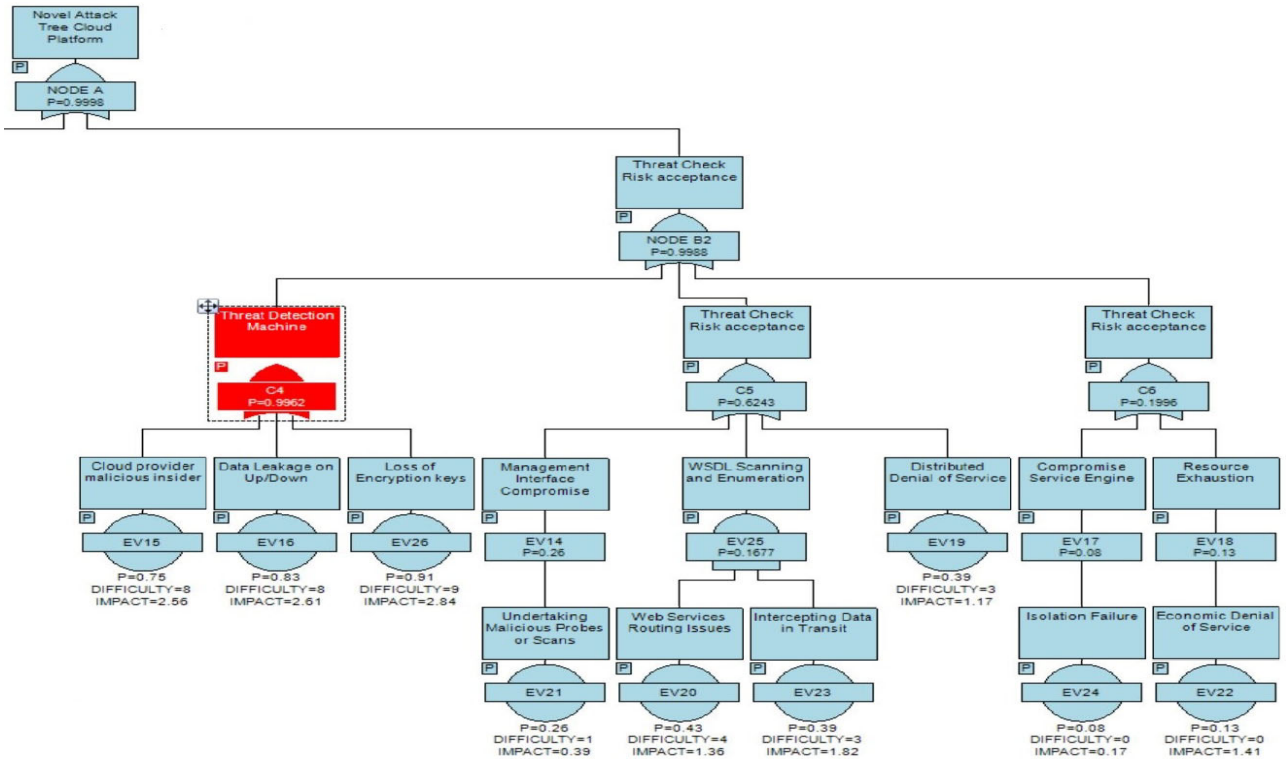

Figure 5. NAT Threats are derived

4 Results Analysis

According to Figure 4 and Figure 5 derived from Attack Tree+ Software 3.0 tool, the simulation results indicate that the node may generate a higher degree of impact, with Threat Node B2 key node having the highest impact value (0.5878) when the system calculates a higher impact value on key node. Node B2 causes a greater risk than Node B1 (impact value: 0.4122), and Importance on Node B2 exceeds Node B1, which means the risk threat is greater than the vulnerability, as depicted in Figure 6.

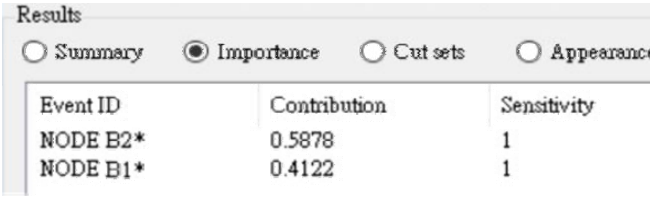

Figure 6. The key node's impact values

The simulation results in the first stage are used to analyze the risk range value corresponding to its equivalent level according to weight value analysis. The simulation results are used to evaluate and sequentially list high-risk events based on the threat impact level assessment. The threat weight of Risk No. EV26 / EV13 causing an impact ranks number one (4.83), EV16 / EV03 threat weight ranks number two (4.80) and EV15 / EV02 threat weight ranks number three (4.77). The assessment in this stage facilitates risk security control and tracking, as depicted in Table 3.

Table 3. Calculation result of weights risk factor

Events	Likelihood	Impact	Weights	Risk level
EV14 / EV01	0.68	2.96	3.64	4
EV15 / EV02	0.75	4.02	4.77	5
EV16 / EV03	0.83	3.97	4.80	5
EV17/ EV04	0.25	2.37	2.62	2
EV18 / EV05	0.31	1.38	1.69	2
EV19 / EV06	0.39	3.52	3.91	4
EV20 / EV07	0.43	1.36	1.79	2
EV21 / EV08	0.26	1.39	1.65	2
EV22 / EV09	0.13	2.41	2.54	3
EV23 / EV10	0.34	1.82	2.16	3
EV24 / EV11	0.08	0.17	0.25	1
EV25 / EV12	0.65	2.76	3.41	4
EV26 / EV13	0.91	3.92	4.83	5

The two key assessment indicators in Stage 2 are risk and node path, which are used to analyze the simulation result content descriptions. The simulation results show the risk data of each node, with Node A (threat path value (0.973) and risk value (7.6483) as the primary target subject to risk threat on the cloud platform. Node B2 (threat path value (0.825) and risk value (6.0398) is the key threat node, as depicted in Table 4.

Table 4. Risk value results for each node

Node	Risk Threat Path Values	Risk Values
A	0.973	7.6483
B1	0.628	4.5879
B2	0.825	6.0398
C1	0.457	1.7296
C2	0.304	2.8838
C3	0.257	3.2751
C4	0.785	5.8530
C5	0.577	2.0960
C6	0.125	1.2575

Targeting the detection and defense level filtering conditions greater than or equal to the risk value, the risk factor failed to meet the various security indicators in the assessment. Based on the simulation results of the risk factor threat path value and risk value of each node, Threat Path [C4, B2, A] has the largest path value (0.785), indicating this path brings the greatest hazard on assets. The greatest threats of cloud platform information security come from information leakage, encryption key failure, risks arising from the cloud supplier's internal security loophole and other factors, which have the greatest impacts. Therefore, a security assessment and defense mechanism needs to be established to prevent information security risk paths that lead to unacceptable damage, thereby achieving risk monitoring and management and providing a reliable security guarantee, as depicted in Table 5.

Table 5. Cloud platform for risk analysis

Risk Threat Path	Events	Risk Threat Path Values	Risk Values	Overall Orders
[C1, B1, A]	EV02 EV03 EV13	0.457	1.7296	3
[C2, B1, A]	EV01 EV12 EV05	0.304	2.8838	4
[C4, B2, A]	EV15 EV16 EV26	0.785	5.8530	1
[C5, B2, A]	EV14 EV19 EV25	0.577	2.0960	2

5 Conclusion

According to the results, the threat impact level and key assessment indicators were analyzed. Pre-defined risk standards were used to reach security criteria and identify major paths, confirm assets and evaluate the likelihood of hazards. The final results in this paper include five points described as follows.

(1) On the evaluation and analysis of threat handling

the related risk factors between each vulnerability and threat in respective stages either reject or accept a service on the key path. The related threat combinations between attack threats need not be cross-matched. NAT Analysis is superior to EAT analysis on the cloud platform in terms of risk analysis and assessment.

(2) The algorithm derives at potential risk factors and quantified risk values to analyze results obtained. For impacts arising from possible damage on the cloud platform, detection and defense judgments were proposed to help identify the cloud platform risk orientation.

(3) The threat impact level assessment of each risk item is listed in sequence. The cloud platform impact, and effects and hazards that cause damage, are further prevented, and a complete security control mechanism is established to minimize risk occurrences.

(4) Among the key assessment indicators, the threat path value is the highest. For risk factors under the threat nodes assessed, data leakage, encryption key failure and CSP internal security loophole have the greatest impacts. As for precautionary measures adopted, security measures should strengthen information encryption capacity and enhance control authorization monitoring level in order to achieve risk monitoring and management.

(5) The result analysis shows the greatest threat comes from information and authorization security risk factors (i.e., CSP security norms ranging from information security control to certification mechanism should strengthen complete operational security, Business Continuity Management (BCM) and Disaster Recovery Planning (DRP) in order to serve as a basis for thorough evaluations of the security auditing system.

The CSP risk assessment reference and improvement measures on the key vulnerability of deficiency in further research, the NAT Analysis can be used in the technical complex cloud platform service environment, to detect vulnerabilities with the safety assessment model and the impact possible from the potential threat risks. The proposed NAT Analysis can further enhance the regulations of detection and prevention, reduce the harm from threats, and extend the risk analysis to the security assessment of the Internet of Things, to provide the reference guidance to the industry, and utilize it as an academic research for future related topics. Hence, the main contributions of this paper are that NAT Analysis, from detecting the impact of possible vulnerability on the cloud platform to impacts arising from potential threat risks and evaluating impacts arising from possible damage, such as confidentiality integrity, usability, and responsibility, identifies major threats, vulnerability, and other risk factors. The proposed NAT helps CSP with proper cloud platform preventive norms, reduce hazards brought about by risk factors, and provides CSP risk monitoring and management references.

In the future, the NAT Analysis shall serve as references for academic research on cross-cloud platform service environment related issues, as well as serving as the information security reference standard for Information and Communication Technologies (ICT) industrial development or cloud platform assessment.

Acknowledgements

The partial work of this paper is funded and supervised by the Ministry of Science and Technology in Taiwan under Grant MOST 106-2410-H-031-017-.

References

[1] S.-J. Yang, S.-P. Peng, Extended Attack Tree Analysis Method to Assess the Security Risks on the Website, *Journal of Information Management*, Vol. 20, No. 1, pp. 1-38, January, 2013.

[2] S.-J. Yang, Y.-L. Lin, An Approach to Assessment Model and Metric Tool of Information Security in Designing EIP, *Journal of Information Management*, Vol. 21, No. 2, pp. 107-138, April, 2014.

[3] ENISA, Cloud Computing: Benefits, Risks and Recommendations for Information Security, https://drive.google.com/drive/folders/0Byla-W9pHwmLdi1fa2RdkJyWk0?zx=8nfo4b o3wjik

[4] Y.-L. Tsai, OWASP Top 10 Cloud Services Security Risk, Taiwan Computer Emergency Response Team/Coordination Center, http://blog.yilang.org/2012/07/owasp.html

[5] CSA, Top Threats to Cloud Computing, https://drive.google.com/drive/folders/0BylaW9pHwmLdi1fa2RZdkJyWk0?zx=8nfo4bo3wjik

[6] The BSI, BSI Standard 100-1 Information Security Management Systems (ISMS), https://www.bsi.bund.de/EN/Publications/BSIStandards/BSI Standards_node.html

[7] M. A. Jinnah Campus, D. Road, Cloud Computing: Security Issues and Challenges, *Journal of Wireless Communications*, Vol. 1, pp. 10-15, 2016.

[8] R. Moreno-Vozmediano, R. S. Montero, I. M. Llorente, Key Challenges in Cloud Computing to Enable the Future Internet of Services, *Journal of IEEE Internet Computing*, Vol. 17, No. 4, pp. 18-25, July, 2013.

[9] M. Ali, S. Khan, A. Vasilakos, Security in Cloud Computing: Opportunities and Challenges, *Journal of Information Sciences*, Vol. 305, pp. 357-383, June, 2015.

[10] S.-J. Yang, Using SLA Strategy to Design an SOC Platform in Data Center on the Cloud Computing, *Journal of Internet Technology*, Taipei, Vol. 14, No. 5, pp. 751-758, September, 2013.

[11] P. Wang, W.-H. Lin, P. T. Kuo, H. T. Lin, Threat Risk Analysis for Cloud Security Based on Attack-Defense Trees, *International Conference on Computing Technology and Information Management* (ICCM), Seoul, South Korea, 2012, pp. 106-111.

[12] A. Roy, D. Kim, K. S. Trivedi, Cyber Security Analysis using Attack Countermeasure Trees, The Annual Cyber Security and Information Intelligence Research Workshop (CSIIRW), pp. 21-23, April, 2010.

[13] B. Kordy, S. Mauw, S. Radomirović, P. Schweitzer, Foundations of Attack Defense Trees, Formal Aspects of Security and Trust of the Series, *Lecture Notes in Computer Science*, Vol. 6561, pp. 80-95, 2010.

[14] W. Yi, M. B. Blake, Service-Oriented Computing and Cloud Computing Challenges and Opportunities, *Journal of IEEE Internet Computing*, Vol. 14, pp. 72-75, November, 2010.

[15] A. Roy, D. Kim, K. S. Trivedi, Cyber Security Analysis Using Attack Countermeasure Trees, *Proceedings of the ACM Sixth Annual Workshop on Cyber Security and Information Intelligence Research* (CSIIRW), Oak Ridge, TN, 2010, pp. 28.

[16] L. Wei, H. Zhu, Z. Cao, X. Dong, W. Jia, Y. Chen, Security and Privacy for Storage and Computation in Cloud Computing, *Journal of Information Sciences*, Vol. 258, pp. 371-386, February, 2014.

[17] Isograph, Attack Tree, https://www.isograph.com/software/attacktree.

Biographies

Shin-Jer Yang is currently a full Professor in the Department of Computer Science and Information Management, Soochow University, Taipei, Taiwan. Professor Yang is the author/coauthor of more than 112 refereed technical papers (Journals and Conferences) on Wired/Wireless Networking and Services, Cloud Computing Applications, Internet Technologies and Applications, and Network Management and Security. Also, he takes in charge of more than 25 research projects. His research interests include Wired/Wireless Networking Technologies and Applications, Cloud Computing and Applications, Network Management and Security, and Information Management.

Ya-Hui Yeh is a System Engineer in the Department of Network Maintenance and Operation, Taiwan Security Company, Taipei, Taiwan. Her research interests include Network Management, Network and Information Security, and Cloud/Web Applications Design.