Security threat probability computation using Markov Chain and Common Vulnerability Scoring System

Ngoc T. Le, Doan B. Hoang
University of Technology Sydney, Faculty of Engineering & IT
Virtual Infrastructure and Cyber Security (VICS)
15 Broadway NSW 2007 Australia
NgocThuy.Le@student.uts.edu.au, Doan.Hoang@uts.edu.au

***Abstract* - Security metrics have become essential for assessing the security risks and making effective decisions concerning system security. Many security metrics rely on mathematical models, but are mainly based on empirical data, qualitative method, or compliance checking and this renders the outcome far from accurate. This paper proposes a novel approach to compute the probability distribution of cloud security threats based on Markov chain and Common Vulnerability Scoring System (CVSS). The paper gives an application on cloud systems to demonstrate the use of the proposed approach.**

Keywords - Security threats, quantitative security metrics, Markov Chain.

I. INTRODUCTION

To ascertain the security of a cloud system, it is necessary to develop meaningful metrics to measure appropriately the system's security level or status. Lord Kelvin considered that when you can quantify or measure what you are talking about, and show it by figures and numbers, you can know apart of it; however, in case you can not quantify it, you can not show it in numbers, your knowledge is of a meagre and unsatisfactory kind [1]. This idea is the source of inspiration and motivation for scholars who generate security metrics that can express in numbers. There are many security metrics proposed to satisfy the need for measuring the security of cyber space from industrial organizations and researchers. The Center for Internet Security (CIS) published a number of security metrics in management, operation, and technique [2]. The National Institute of Standards and Technology (NIST) developed security metrics in implementation, effectiveness, and impact [3]. Other metrics have been proposed in Risk assessment and network security evaluation [4-6].

There are several security metrics related to the computation of probability of security threats. Mean Failure Cost is one of the sound approaches to quantitative security metrics when it takes various security components like stakeholders, security requirements, security threats into account [7]. The probability distribution of security threats is central to this metric, but, this computation is mainly based on empirical or qualitative data. Some security metrics, related to successful attacks, are specific to a particular kind of attacks and hence they cannot be generalized. Realistically, to assess security of a system, all aspects of security threats are essential, and a security model should take all security threat angles into account.

To our best knowledge, we hardly found a model that computes the probability distribution of security threats. The paper proposes a security threat model based on Markov theory to calculate the probability distribution of security threats in cloud systems. For this purpose, the Common Vulnerability Scoring System (CVSS) will be applied to compute the probability of each attack paths. For evaluating the proposed method, cloud security threats reported by Cloud Security Alliance (CSA) will be investigated.

Major contributions of this paper are as follows:

- It proposes the security threat model that takes all known and major cloud security threats into account.
- It applies Markov chain and CVSS to the proposed model to predict the probability distribution of security threats.
- It demonstrates the use of the model and its computational method on a cloud security system.

The remainder of the paper is organized as follows. Section 2 provides the background of metrics related to security threats and Markov chain in security metrics. Section 3 analyses the relationship between security threats and vulnerabilities. Section 4 proposes the security threat model based on Markov chain. In section 5, the calculation of probability distribution of security threats will be expressed. It also discusses the application of the proposed metric. The conclusion with suggestion for future work will be concluded in section 6.

II. RELATED WORK

This section discusses related work concerning security metrics related to security threats.

A. A security metric related to probability distribution of security threats.

Ben et al. introduced a security metric called Mean Failure Cost (MFC) is a metric that measure the security of a IT system through quantifying variables including stakeholders, the loss resulting from security threats [7]. It includes several desirable features: it identifies stakeholders and provides the cost for each as a result of a security failure; it measure the cost financial loss in a unit investigated time ($/h). Despite these appropriate considerations, MFC has a major drawback in that the security threats probability distribution is based on simple empirical data, while security threats are changeable, dynamic, and specific to different IT systems. Due to the stochastic nature of threats, modelling their probability distributions has become a necessity for any security measuring and predicting system. Relevant and sound classification of threats in terms of deployed vulnerabilities, attack motivation perspectives, and likelihood of successful attacks are essential to facilitate the identification of potential

security threats and the development of security countermeasures.

B. Markov theory in security metrics

For a Markov process, the conditional probability distribution of future states of the process (conditional on both past and present states) depends only on the present state, not on the sequence of events that preceded it. Based on this property, several studies have deployed Markov for modelling security metrics. In [8], Ariel et al. used Discrete Markov Chain Model to predict next honeypot attacks. In [9], to detect anomaly attacks in an intrusion detection system (IDS), Patcha et al. used Hidden Markov Chain to model this system. In [10], Bharat et al. used Semi Markov Model (SMM) to quantify the security state for an intrusion tolerant system. In this work, Discrete Time Markov Chain (DTMC) steady-state probability was applied to compute the mean time to security failure (MTTSF). In [11], Anderson et al. proposed a malware detection algorithm based on the analysis of graphs that represent Markov chains from dynamically collected instruction traces of the target executable. In [12], Jaafar et al. used attack path concept and time is used to calculate transition probabilities. In terms of security metrics, most research used Markov Model in predicting security attacks or malware propagations. To our best knowledge, we have hardly found studies that take the consideration of applying Markov chain for computing the probability distribution of security threats.

III. THE RELATIONSHIP BETWEEN CLOUD SECURITY THREATS AND VULNERABILITIES

In this section, we explore the relationship between security threats and vulnerabilities to identify potential attacks.

A security threat is considered as a potential attack leading to a misuse of information or resources, and vulnerability is defined as the flaws in a cyber space that can be exploited by hackers. As a result, a security threat is a potential attack that may or may not happen, however it has the potential to cause damages. First, we clarify the cloud security threats based on the Cloud Security Alliance (CSA) report [13]. The report released *twelve* critical security threats specifically related to the shared, on-demand for cloud computing with the highest impact on enterprise business.

- Data Breaches (DB). These are security incidents in which confidential or protected information is released, stolen or unauthorizedly used by an attacker.
- Weak Identity, Credential and Access Management (IAM). Attacks may occur because of inadequate identity access management systems, failure to use multifactor authentication, weak password use, and a lack of continuous automated rotation of cryptographic keys, passwords, and certificates.
- Insecure interfaces APIs (Application Programming Interface). The security of fundamental APIs is vital key role in availability of cloud services. From authentication and access control to encryption and activity monitoring, these interfaces must be designed to protect against both accidental and malicious attempts to circumvent policy.
- System Vulnerabilities (SV). These are exploitable bugs in programs that attackers can use to infiltrate a computer system for stealing data, taking control of the system or disrupting service operations. Vulnerabilities within the components of the operating system - kernel, system libraries and application tools - put the security of all services and data at significant risk.
- Account Hijacking (AH). It is a traditional threat with attack methods such as phishing, fraud, and exploitation of software vulnerabilities.
- Malicious Insiders (MI). It is defined as a malicious insider threat created by people in organizations, who has privileged access to the system and intentionally misused that access in a manner that negatively affected the confidentiality, integrity, or availability of the organization's information system.
- Advanced Persistent Threats (APTs). These are parasitical-form-cyber-attacks that infiltrate systems to establish a foothold in the computing infrastructure of target companies from which they smuggle data and intellectual property.
- Data Loss (DL). For reasons like the deletion by the cloud service provider or a physical catastrophe accidently including earthquake or a fire leading to the permanent loss of customer data. Providers or cloud consumers have to take adequate measures to back up data, following best practices in business continuity and disaster recovery - as well as daily data backup and possibly off-site storage.
- Insufficient Due Diligence (IDD). An organization that rushes to adopt cloud technologies and chooses cloud service providers (CSPs) without performing due diligence exposes itself to a myriad of commercial, financial, technical, legal and compliance risks.
- Abuse and Nefarious Use of Cloud Services (ANU). Poorly secured cloud service deployments, free cloud service trials, and fraudulent account sign-ups via payment instrument fraud expose cloud computing models such as IaaS, PaaS, and SaaS to malicious attacks.
- Denial of Service (DOS). DOS attacks are meant to prevent users of a service from being able to access their data or their applications by forcing the targeted cloud service to consume inordinate amounts of finite system resources so that the service cannot respond to legitimate users.
- Shared Technology Vulnerabilities (STV). Cloud service providers deliver their services by sharing infrastructure, platforms or applications. The infrastructure supporting cloud services deployment may not have been designed to offer strong isolation properties for a multitenant architecture (IaaS), re-deployable platforms (PaaS) or multi-customer applications (SaaS). This can lead to shared technology vulnerabilities that can potentially be exploited in all delivery models.

A security threat usually exploits one or more vulnerabilities in components of a system to compromise it. The relationship between security vulnerabilities and these recognized threats is thus essential for the threat model. Hashizume et al. [14] identified *seven* major security vulnerabilities in cloud computing.

- Insecure interfaces and APIs (V1). Cloud providers offer services that can be accessed through APIs (SOAP, REST, or HTTP with XML/JSON). The

security of the cloud depends upon the security of these interfaces. Vulnerabilities are weak credential, insufficient authorization checks, and insufficient input-data validation. Furthermore, cloud APIs are still immature which means that they are frequently changed and updated. A fixed bug can introduce another security hole in the application.

- Unlimited allocation of resources (V2). Inaccurate modeling of resource usage can lead to overbooking or over-provisioning.
- Data-related vulnerabilities (V3). This is one of the biggest cloud challenges involving data issues. Data can be co-located with the data of unknown owners (competitors, or intruders) with a weak separation. Data may be located in different jurisdictions which have different laws. Incomplete data deletion – data cannot be completely removed. Data backup is done by untrusted third-party providers. Information about the location of the data usually is unavailable or not disclosed to users. Data is often stored, processed, and transferred in clear plain text.
- Vulnerabilities in Virtual Machines (V4). Beside data-related, vulnerability in Virtual Machines is a big challenge in cloud security. It includes several aspects. Possible covert channels in the colocation of VMs. Unrestricted allocation and de-allocation of resources with VMs. Uncontrolled Migration - VMs can be migrated from one server to another server due to fault tolerance, load balance, or hardware maintenance. Uncontrolled snapshots – VMs can be copied in order to provide flexibility, which may lead to data leakage. Uncontrolled rollback could lead to reset vulnerabilities - VMs can be backed up to a previous state for restoration, but patches applied after the previous state disappears. VMs have IP addresses that are visible to anyone within the cloud - attackers can map where the target VM is located within the cloud.
- Vulnerabilities in Virtual Machine Images (V5). Uncontrolled placement of VM images in public repositories. VM images are not able to be patched since they are dormant artefacts.
- Vulnerabilities in Hypervisors (V6). These vulnerabilities stem from is the complexity of the hypervisor code.
- Vulnerabilities in Virtual Networks (V7). The vulnerabilities are associated with the sharing of virtual bridges by several virtual machines.

We identify and tabulate the connection between security threats and vulnerabilities in Table 1. It is seen that a security threat may have several security vulnerabilities and one vulnerability may be exploited by several security threats. For example, in terms of threat Data Breaches (DB), five vulnerabilities are involved in this security threat: Insecure interfaces and APIs (V1), Data-related vulnerabilities (V3), Vulnerability in Virtual Machines (V4), Vulnerabilities in Virtual Machine Image (V5), and Vulnerabilities in Virtual Networks (V7). Ristenpart et al. [15] indicated the confidential information can be extracted from VMs co-located in the same server. An attacker may use several attacks to collect data by exploiting vulnerabilities in brute-forcing, measuring cache usage, and load-based co-residence detection data processing techniques in cloud systems. Therefore, data leak depends

TABLE 1: RELATIONSHIP BETWEEN SECURITY THREATS AND VULNERABILITIES

	Threat	Description	Vulnerabilities	Incidents
1	DB	Data Breaches	V1, V3, V4, V5, V7	An attacker can use several attack techniques involved like SQL, command injection, and cross-site scripting. Virtualization vulnerabilities can be exploited to extract data.
2	IAM	Weak Identity, Credential and Access Management	V1, V3	An attacker can leverage the failure to use multifactor authentication, or weak password uses.
3	API	Insecure interfaces APIs	V1	An attacker can take advantage of weakness in using APIs like SOAP, HTTP protocol. Bugs in APIs can be also exploited.
4	SV	System Vulnerabilities	V4, V5, V6, V7	An attacker can attack via vulnerabilities in Virtual Machine images, in Hypervisors, and in Virtual Networks.
5	AH	Account Hijacking	V1	To get access system, attackers can use the victim's account
6	MI	Malicious Insiders	V5, V7	An attacker can generate a VM image embracing malwares then propagate it.
7	APT	Advanced Persistent Threats	V1, V4, V5, V6, V7	An attacker can use several kinds of vulnerabilities from specific virtual cloud or APIs to infect bugs permanently in the target system for mainly scavenging data.
8	DL	Data Loss	V3, V4, V7	An attacker can use data-driven attack techniques to gain confidential information from other VMs co-located in the same server. Or using the risk of data backup, storing process to scavenge data.
9	IDD	Insufficient Due Diligence	V4, V6	An attacker can leverage weaknesses in complying rules in using cloud system like configuration of VMs, data and technology shares.
10	ANU	Abuse and Nefarious Use of Cloud Services	V4	An attacker can attack through use and share of servers, data of customers by using anonymous account.
11	DOS	Denial of Service	V1, V2	An attacker can request more IT resources, so authorized users cannot get access the cloud services.
12	STV	Shared Technology Vulnerabilities	V4, V6	An attacker can sniff and spoof virtual networks or use the flexible configuration of Virtual Machines or hypervisors to exploit.

not only on data-related vulnerabilities but also from virtualization vulnerabilities.

Table 1 indicates that the Data-related vulnerability (V3) involves in three security threats. First, it may cause the threat Data Breaches (DB) when an attacker uses several techniques like SQL injection, cross-site scripting to attack the cloud system. Second, it may lead to the threat Weak Identity, Credential and Access Management (IAM) where an attacker may leverage the data that is often stored, processed, and transferred in clear plain text to gain access to the cloud system. Third, it may cause the threat Data Loss (DL) when an attacker exploits several involved vulnerabilities like different located data, incomplete data deletion, and data backup.

IV. MARKOV MODEL FOR SUCCESSFUL ATTACKS

We introduce a Markov process to describe a cloud attack model and use the CVSS to determine the transition matrix of the proposed Markov.

A security threat is a stochastic process. We model it as a Markov chain. The probability of transition from one state to others is based on the vulnerabilities present in the current state. An attacker exploits various vulnerabilities to arrive at a security threat state and eventually reaches the final failure state. At this stage, we mainly focus on a first level of abstraction with visible and quantifiable states and construct 3 states, namely the secure state (S), the threat state (T), and the failure state (F). Figure 1 depicts the proposed Markov model for modeling security threats and attacks with state transition probabilities where α denotes the transient probability from state S to state T, β denotes the transient possibility from T back to S, γ denotes the probability to change the state from T to F, δ denotes the transient probability from F state back to T state, ε denotes the possibility from F state back to S state. The model takes all elements of an attack model into account including attack, defense and recovery factors of the system. We do not present the direct transition probability from state S to state F for several reasons. First, we are investigating the impact of security threat on failure system and how an attacker takes advantages from security threats. An attacker tries to exploit vulnerabilities to change from secure state to threat state. Second, the system collapsed (goes directly from S to F) mainly in case of natural disasters or similar catastrophes. This model is simple and practical for our consideration. Even with this 3-state model, it is difficult to derive a set of data for its complete description. We refine the model in several steps for our investigation.

Figure 2 shows the attack model with the defense elements absorbed into the failure state. It means there is no the transient probability from F to T or from F to S. when the process reaches F, it stays there with probability 1. This means, recovery process is not taken into account.

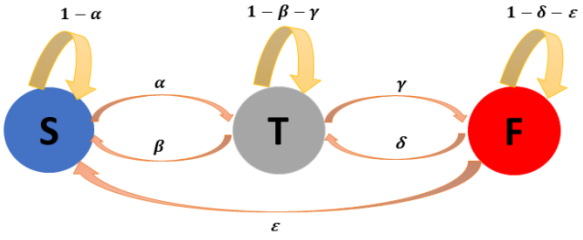

Fig. 1. Diagram of attack model with defense and recovery

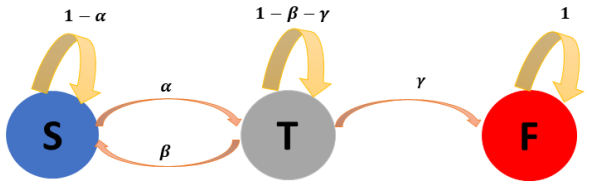

Fig. 2. Diagram of attack model with defense and without recovery

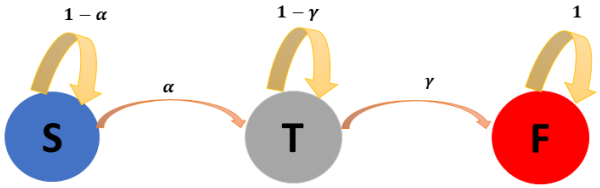

Fig. 3. Diagram of attack model without defense and recovery

Figure 3 shows the attack model with the defense efforts absorbed both at the threat state and the failure state. We focus on this kind of abstraction of this model. The aim is to compute the successful chance of attacks by an attacker deploying vulnerabilities of a threat. We do not take into account the recovery element of the system at this stage of investigation as it can be incorporated at a later stage. Furthermore, recovery efforts largely depend on the manager of the system and relevant data is not often disclosed. The probability from S to T also means the overall probability that includes the defense element that system tries to change state from T back to S.

We are interested in finding the transition probability from state S to state F in the attack sequence. Chapman–Kolmogorov equation [16] is available to find the transient probability between two states after a number of jump-steps. Once the distribution of probability on the states of a Markov chain is discrete and this space is homogeneous, it can be showed by matrix multiplication. Therefore, to derive the transition probability between two states in a number of steps, Chapman–Kolmogorov equation can be used as follows:

$$P_{ij}^{m+n} = \sum P_{ik}^{m} P_{kj}^{n} \qquad (1)$$

Where, P is the probability matrix of transition of state space. P_{ij}^{m+n} is the transition probability from state i to state j after $(m+n)$ steps via any state k.

V. DISTRIBUTION OF SECURITY THREAT PROBABILITIES

To compute the distribution of security threat probabilities based on Markov chain, 3 phases can be presented as follows: modeling security threat model as the Markov chain; building transition probability matrix; computing the transition probability from state S to state F via each threat T.

Phase 1: modeling security threat model as the Markov chain. Figure 4 shows attack model that expands the general model in the figure 3 with twelve attack paths. This is modeled as a Markov chain with fourteen states including a security state, a failure state, and twelve threat states. The security is defined as a state of system that has no failure or security threats. The failure is a state when the system fails to meet its minimum requirements because of security issues that an attacker could exploit security vulnerability of specific threat. Each security threat is expressed by possible attack path that an attacker can utilize a set of vulnerabilities of a specific threat. These paths are possible ways to reach

failure system target. In this model, we assume that the probability of attack path is overall probability that includes defense element. This is a simplification as it is possible that the system can move from one threat state to other determined threat states to reach the failure state.

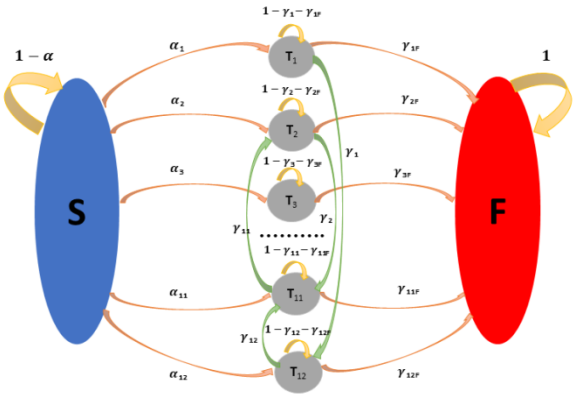

Fig. 4 Security threat model with attack process

Phase 2: building transition probability matrix. The probability of each attack path is considered as the probability of changing state security to failure caused by each security threat. This means when an attacker attacks the cloud system successfully there will be a transition probability from a security to failure state as called potential successful attack or probability of security threats. In other words, an attacker leverages security vulnerabilities of each security threat (the attack path) to attack to reach the failure state of the cloud system. From the attack model (see the figure 4) we arrive at a transition probability P_{ij} matrix with fourteen states including security, failure, and twelve threat states.

$$P = \begin{bmatrix} 1-\alpha & \alpha_1 & \cdots & \alpha_{12} & 0 \\ 0 & 1-\gamma_1-\gamma_{1F} & \cdots & \gamma_1 & \gamma_{1F} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1-\gamma_{12}-\gamma_{12F} & \gamma_{12F} \\ 0 & 0 & \cdots & 0 & 1 \end{bmatrix}$$

In which, α is the sum of probability of all attack paths from S state to T states. And γ_F is the sum of the probability of all threat states to failure state. Once the system is in the security state, it will remain in his state with probability (1-α) and once the system is in the failure state, the probability is 1 (the absorbing state). The probabilities of attack paths representing from S to T states are $\alpha_1, \alpha_2, \alpha_3$ etcetera. The probabilities of attack paths representing from threats states to the failure state are $\gamma_{1F}, \gamma_{2F}, \gamma_{3F}$ etcetera. And there are the probabilities from one state to other states. However, for the purpose of demonstrate the model, it is assumed that there is one path from one threat state to another threat state. These probabilities are presented as $\gamma_1, \gamma_2, \gamma_3$ etcetera.

Phase 3: computing the transition probability from state S to state F via threats T_i. According attack paths theory, each attack path represents the path that the attacker will take advantage to reach the failure state (F) from a threat state (T) by exploiting the set of vulnerabilities (v_{ij}) of each security threat. For example, we assume that attack path 1 represents the path that the attacker exploits vulnerability of threat 1 (Data Breaches-DB). Thus, there is a distribution of probability of attack paths when attackers may choose one path to attack in the space of attack paths. To quantify this distribution, we use the concept weight of each path. CVSS [17] can be used to weigh each path from S to T, from T to F, or between threats to calculate transition probabilities. The weight associated with the transition from S to T_i is determined by computing the ratio between vulnerability scores from S to T_i and all vulnerability scores from S to all threats. By using (2), the transition probabilities (α_i) from S to T_i can be calculated. Similarly, the transition probabilities (γ_{iF}) from T_i to F can be computed using (3). To compute the transient probability S to F via T_i, ($P(SF)_i$), (1) can be used to compute in a number of jump-steps. However, at this stage, with purpose of demonstrate the threat model based on Markov chain, we simulate to compute $P(SF)_i$ in two jump-steps using (4). Therefore, the probability between threats may not be considered.

$$\alpha_i = \frac{\sum_j v_{ij}}{\sum_{k,l} v_{kl}} * \alpha \quad (2)$$

$$\gamma_{iF} = \frac{\sum_j v_{ij}}{\sum_{k,l} v_{kl}} * \gamma_F \quad (3)$$

$$P^2(SF)_i = P^2 = \alpha_i * \gamma_{iF} \quad (4)$$

In which, i is index of an attack path, v_{ij} is the vulnerability score of vulnerability j associated path i, k∈P is the set of attack paths.

TABLE 2. VULNERABILITY SCORES

Vulnerability	Acronym	Exploitability score
CVE-2017-14925	V1	8
CVE-2014-4064	V2	2
CVE-2015-5255	V3	3
CVE-2015-4165	V4	5
CVE-2016-0264	V5	7
CVE-2015-1914	V6	5
CVE-2017-6710	V7	7

To calculate probability distribution of security threats, we need to determine elements of the Markov transition matrix based on the vulnerabilities associated with a threat. From the security state S, the total probability that the system moves to one of the threat states is assumed α (α = 0.0318 [18]). We can determine the transition probability that the system moves from S to T_i as the ratio of the sum of vulnerability scores of threats associated with T_i over the total CVSS scores of all threats.

Table 2 shows the CVSS scores [17] associated with relevant vulnerabilities considered in this paper. According to CVSS this number is out of ten score. For example, V1 scores eight out of ten because the severity of this vulnerability is very high once it is related to cloud data breaches vulnerabilities. In addition, to go to state T_1 from S, an attacker needs to exploit the certain set of vulnerabilities associated with the security threat state T_1. In this case, vulnerabilities one, three, four, five, and seven will be exploited (see Table 1). Therefore, the number of vulnerability scores for the attack path one is (W_1=V_1+V_3+V_4+V_5+V_7=30) and the total number of all

vulnerability score from S to any T_i (W=177). We can estimate the transition probability from S to T_1 ($\alpha_1 = 30/177 * \alpha = 0.00539$). Similarly, other transition probability from S to T_i will be computed by using (9). We assume that the transition probability from state T_i to F is highly likely with probability $\gamma_{iF} = 0.95$ for any attack paths (see Figure 4). By computing α_i and γ_{iF}, the transition probability matrix P is obtained. Then by using (1) and (4), we have the probabilistic distribution of twelve security threats expressed in Table 3.

TABLE 3 PROBABILITY DISTRIBUTION OF TWELVE SECURITY THREATS

	Threats	Formula	Probability (*10^{-3})
1	DB	$\alpha_1 * \gamma_{1F}$	5.120339
2	IAM	$\alpha_2 * \gamma_{2F}$	1.877458
3	API	$\alpha_3 * \gamma_{3F}$	1.365424
4	SV	$\alpha_4 * \gamma_{4F}$	4.096271
5	AH	$\alpha_5 * \gamma_{5F}$	1.365424
6	MI	$\alpha_6 * \gamma_{6F}$	2.389492
7	APT	$\alpha_7 * \gamma_{7F}$	5.461695
8	DL	$\alpha_8 * \gamma_{8F}$	2.560169
9	IDD	$\alpha_9 * \gamma_{9F}$	1.706780
10	ANU	$\alpha_{10} * \gamma_{10F}$	0.853390
11	DOS	$\alpha_{11} * \gamma_{11F}$	1.706780
12	STV	$\alpha_{12} * \gamma_{12F}$	1.706780

The computation of a security threat probability distribution is essential for creating security metrics [19] especially in security risk metrics [20]. The above approach showed that it is effective for cloud computing. Apparently, this method can also be tailored in other cyber systems such as Internet of Things (IOTs) and software-defined systems/services [21]. This computation can support security managers to make security decisions. For example, as seen in table 3, the probabilities of security threats DB or APT is quite high. Hence, the security action plan can focus on deteriorating the impact of these kinds of threat. In case of reducing the damage in overall, we can apply several specific countermeasures or security standard compliance to decrease the probability of each threat.

VI. CONCLUSION

This paper introduced a security threat model based on graph theory. For this purpose, we applied Markov chain to this model with three states to identify the attack paths through various security threats. Twelve security threats reported by CSA and seven security vulnerabilities scored by CVSS were investigated to support to demonstrate the security threat model to compute the probability distribution of security threats. Our future work is to develop novel quantitative security metrics, that use this computation of probability distribution of security threats, to measure security domains in a cloud system for determining the overall security level.

REFERENCES

[1] W. Thomson, "Lord Kelvin: Electrical units of measurement. Popular lectures and addresses," ed: Macmillan, London, 1889.

[2] C. f. I. Security, "The CIS security metrics," ed, 2010.

[3] E. Chew, M. Swanson, K. Stine, N. Bartol, A. Brown, and W. Robinson, "Performance measurement guide for information security". 2008.

[4] Huang, Kaixing, et al. "Application of Bayesian network to data-driven cyber-security risk assessment in SCADA networks." Telecommunication Networks and Applications Conference (ITNAC), 2017 27th International. IEEE, 2017.

[5] Hadaad, Nabeel, Luke Drury, and Ronald G. Addie. "Protecting services from security mis-configuration." Telecommunication Networks and Applications Conference (ITNAC), 2015 International. IEEE, 2015.

[6] Hu, Qinwen, Muhammad Rizwan Asghar, and Nevil Brownlee. "Evaluating network intrusion detection systems for high-speed networks." Telecommunication Networks and Applications Conference (ITNAC), 2017 27th International. IEEE, 2017.

[7] A. B. Aissa, R. K. Abercrombie, F. T. Sheldon, and A. Mili, "Defining and computing a value based cyber-security measure," Information Systems and e-Business Management, vol. 10, no. 4, pp. 433-453, 2012.

[8] A. Bar, B. Shapira, L. Rokach, and M. Unger, "Identifying Attack Propagation Patterns in Honeypots Using Markov Chains Modeling and Complex Networks Analysis," in Software Science, Technology and Engineering (SWSTE), 2016 IEEE International Conference on, 2016, pp. 28-36: IEEE.

[9] A. Patcha and J.-M. Park, "An overview of anomaly detection techniques: Existing solutions and latest technological trends," Computer Networks, vol. 51, no. 12, pp. 3448-3470, 2007/08/22/ 2007.

[10] B. B. Madan, K. Goševa-Popstojanova, K. Vaidyanathan, and K. S. Trivedi, "A method for modeling and quantifying the security attributes of intrusion tolerant systems," Performance Evaluation, vol. 56, no. 1, pp. 167-186, 2004.

[11] B. Anderson, D. Quist, J. Neil, C. Storlie, and T. Lane, "Graph-based malware detection using dynamic analysis," Journal in computer Virology, vol. 7, no. 4, pp. 247-258, 2011.

[12] J. Almasizadeh and M. A. Azgomi, "A stochastic model of attack process for the evaluation of security metrics," Computer Networks, vol. 57, no. 10, pp. 2159-2180, 2013.

[13] C. S. ALLIANCE. (2016). The Treacherous Twelve - Cloud Computing Top Threats in 2016. Available: https://cloudsecurityalliance.org/media/news/cloud-security-alliance-releases-the-treacherous-twelve-cloud-computing-top-threats-in-2016/

[14] K. Hashizume, D. G. Rosado, E. Fernández-Medina, and E. B. Fernandez, "An analysis of security issues for cloud computing," Journal of Internet Services and Applications, vol. 4, no. 1, p. 5, 2013.

[15] T. Ristenpart, E. Tromer, H. Shacham, and S. Savage, "Hey, you, get off of my cloud: exploring information leakage in third-party compute clouds," in Proceedings of the 16th ACM conference on Computer and communications security, 2009, pp. 199-212: ACM.

[16] S. M. Ross, Introduction to probability models. Academic press, 2014.

[17] NVD. (2018). National Vulnerability Database. Available: http://nvd.nist.gov/

[18] M. Jouini and L. B. A. Rabai, "Mean Failure Cost Extension Model towards Security Threats Assessment: A Cloud Computing Case Study," JCP, vol. 10, no. 3, pp. 184-194, 2015.

[19] N. T. Le and D. B. Hoang, "Cloud Maturity Model and metrics framework for cyber cloud security," Scalable Computing: Practice and Experience, vol. 4, pp. 277-290, 2017.

[20] T. G. Lewis, "Critical infrastructure protection in homeland security: defending a networked nation," John Wiley & Sons, 2014.

[21] D. B. Hoang and S. Farahmandian, "Security of Software-Defined Infrastructures with SDN, NFV, and Cloud Computing Technologies," in Guide to Security in SDN and NFV: Springer, 2017, pp. 3-32.