An Improved Stochastic Model for Cybersecurity Risk Assessment

Oni Omoyemi Abimbola[1], Akinyemi Bodunde Odunola[2], Aladesanmi Adegboye Temitope[1], Ganiyu Adesola Aderounmu[2], Kamagat é Beman Hamidja[3]

[1] Information Technology and Communication Unit, Obafemi Awolowo University, Ile-Ife, Nigeria

[2] Department of Computer Science and Engineering, Obafemi Awolowo University, Ile-Ife, Nigeria

[3] LARIT-Abidjan Cocody Danga, C ôte d'Ivoire

Correspondence: Akinyemi Bodunde Odunola, Department of Computer Science and Engineering, Obafemi Awolowo University, Ile-Ife, Nigeria.

Received: November 8, 2019 Accepted: November 20, 2019 Online Published: November 22, 2019

doi:10.5539/cis.v12n4p96 URL: https://doi.org/10.5539/cis.v12n4p96

Abstract

Most of the existing solutions in cybersecurity analysis has been centered on identifying threats and vulnerabilities, and also providing suitable defense mechanisms to improve the robustness of the cyberspace network. These solutions lack effective capabilities to countermeasure the effect of risks and perform long-term prediction. In this paper, an improved risk assessment model for cyberspace security that will effectively predict and mitigate the consequences of risk was developed. Real-time vulnerabilities of a selected network were scanned and analysed and the ease of vulnerability exploitability was assessed. A Risk Assessment Model was formulated using the synergy of Absorbing Markov Chain and Markov Reward Model. The model was utilized to analyse cybersecurity state of the selected network. The proposed model was simulated using R- Statistical Package, and its performance was evaluated by benchmarking with an existing model, using Reliability and Availability as metrics. The result showed that the proposed model has higher reliability and availability over the existing model. This implied that there is a significant improvement in the assessment of security situations in a cyberspace network.

Keywords: cybersecurity, risk, absorbing markov chain, CVSS

1. Introduction

Cyberspace is a defining feature of modern life. Individuals and communities worldwide connect, socialize, and organise themselves in and through cyberspace (Tsakanyan, 2017). As Internet usage continues to expand, cyberspace will become increasingly woven into the fabric of everyday life across the globe (National Security Strategy, 2011). Cyberspace management involves the security of network critical infrastructure through cybersecurity procedures. Cyber Security (CS) is a whole set of procedures and systems protecting networks from intentional and unintentional damages or danger in cyberspace through services like confidentiality, integrity, authentication, and availability (Khan and Hussain, 2010).

Cybersecurity in cyberspace is a critical issue in today's dynamic network environment that communicates over the internet. The growing cyberspace requires the use of effective cybersecurity risk management techniques that will enable security practitioners to know the security status of a network. In cyberspace, a network provides diverse applications to end-users, and the ability to assess risk in cyberspace is very important to reduce the risk to a minimum level. To ensure that the overall security risk stays within acceptable limits, network practitioners need to ensure risks in the organisation are measured. To reduce the risks of cyber-attacks, an organisation needs to understand and assess them, make decisions about what types of barriers or protection mechanisms are necessary to defend against them, and decide where to place such mechanisms (Ye *et al*., 2006)

A cyberspace environment must be protected and resilient from attacks and also be an information pervaded environment that detects hostile behavior as it occurs. A cyberspace network administrator or practitioner should keep abreast of the state of the network in terms of knowing the risk impact of the probability of an attack occurrence and also providing remediation actions. To this effect, several decision-making support systems have been incorporated into cyberspace security management to provide potential approaches for optimization of remediation. Despite all these approaches, there has been a criticism of the quantitative attempts of risk evaluation due to the lack of data for validating the methods (Verendel, 2009). Also, security vulnerabilities that have been discovered but remain unpatched for a while still constitute a considerable risk to an organisation (Joh and Malaiya, 2010). Therefore, existing solutions lack the effective capability to countermeasure the consequences of risk by providing actions on how to make the make network resilience. It was noted that there is a need for the development of a framework that will capture the dynamic nature of the vulnerabilities, and evaluate the risk impacts on the network effectively.

Thus, an attempt was made in this paper to develop an improved risk assessment model for cyberspace security risk concerns that will effectively predict and mitigate the consequences of risk. A model was proposed to assess risk in a selected cyberspace network and predict cyberspace security resilience by projecting into the future risk.

The rest of this paper is arranged as follows: Section 2 discusses the related works, Section 3 describes the modeling process and Section 4 describes the expected result and the summary and conclusions are discussed in Section 5.

2. Related Works

There has been quite a good amount of existing work on cybersecurity risk management. Byres *et al*., (2007) described how the attack tree methodology may be applied to the common SCADA system to identify security vulnerabilities inherent in the specification and typical deployments. The study showed that attack trees are a promising technology for aiding control system security analysts in the understanding and protection of their systems. The methodology lacks pruning and trimming approach. (Conrad, 2005) used a Monte-Carlo approach for analysing the risks of Information Security Investments. This study captured uncertainty in security modeling parameters (vulnerabilities, the frequency of intrusion damage estimates, etc) and expresses its impact on the model’s forecast. However, the model is not suitable for long-term prediction. Frei *et al*., (2006) researched on large-scale vulnerability analysis. The study examined how vulnerabilities are handled in large scale by quantifying the performance of the security industry as a whole. Trends and the implications of vulnerabilities are discussed. The research quantified the gap between exploit and patch availability but the research did not consider the discovery and disclosure date. McQueen *et al*., (2006) worked on quantitative cyber risk reduction estimation methodology for a small SCADA Control System, however, the model is not suitable for prediction. Xie *et al*., (2008) used two-layer attack graphs to evaluate the network security vulnerabilities, where the upper layer is a host access graph and the lower layer comprises some host-pair attack graphs. However, the model lacks scalability defined the metrics available for measuring Security Risk. The study proposed a systematic and iterative research method to determine suited metrics in ISSRM domain. The study enriches the ISSRM domain model with suited metrics towards a measuring framework for security risk management but did not measure dependability metrics. Khan and Hussain (2010) used a unified model for the quantification of cybersecurity that considered most of the parameters and services in cybersecurity, but the model did not capture some important services and cannot apply to a real-life scenario. Joh and Malaiya (2011) formally defines risk measures and examines possible approaches for assessing risk using actual data. This model can be used for comparing the risk level for alternative systems. However, computational approaches need to consider governing probability distribution for the states of sojourn time. Abraham and Nair (2013) proposed cybersecurity analytics using a stochastic model for security quantification using Absorbing Markov Chains. The research utilized stochastic modeling techniques using attack graphs to define a complementary suite of quantitative metrics to aid network security. Houmb and Franqueira (2009) discussed a model for the quantitative estimation of the security risk level of a system by combining the frequency and impact of a potential unwanted event and is modeled as a Markov process. They estimate the frequency and impact of vulnerabilities using reorganised original CVSS metrics. And, finally, the two estimated measures are combined to calculate risk levels. Some other mechanisms that have been applied to cybersecurity risk management are Bayesian networks (Akinyemi *et al*., 2014; Akinyemi *et al*., 2015; Akinyemi *et al*., 2018a) , Bayesian attack graph (Akinyemi *et al*., 2018b), Non-linear Stochastic methods (Rajasooriya *et al*., 2017a; Rajasooriya *et al*., 2017b); Game theory (Akinwumi *et al*., 2017; Musman and Turner, 2018)etc. The proposed model utilized the probability characteristics of Absorbing Markov Chain to address how vulnerabilities can be exploited to infiltrate the cyberspace network by attackers.

3. Methodolody

Figure 1 shows the framework of the proposed risk assessment model for cyberspace network security management that is capable of predicting and providing information for the optimization of remediation. The proposed model is based on the assumption that the vulnerabilities age. That is, when vulnerabilities are discovered, the exploit is not available until it is disclosed on the National Vulnerability Database (NVD). The proposed risk assessment of a cyberspace network when performed regularly by the network administrator will diagnose the network critical assets for risk assessment. The risk assessed will be scaled based on low, medium or high level. If high, the right approaches can be provided for remediation.

The processes involved in implementing this model are as follows:

i. Vulnerabilities and Attacks of a selected Cyberspace Network, that is OAUNET was analysed based on the National Vulnerability Database (NVD). The ease of exploitability of the risk on the network was evaluated using the Common Vulnerability Scoring System (CVSS) scoring model;

ii. An attack tree was generated using a formulated model; this was generated by combining the vulnerabilities present on the network configuration. This shows different scenarios whereby an attacker can gain access or reach a goal state.

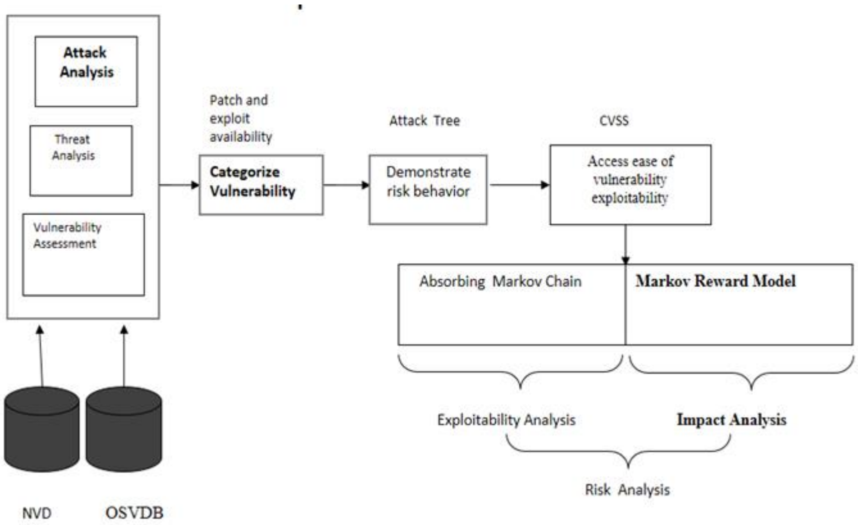


Figure 1. Proposed Model description

iii. Then, the Risk Assessment Model was formulated using the synergy of Absorbing Markov Chain and Markov Reward Model, to assess the cyberspace network security risk in terms of how resilient is the network based on the vulnerabilities risks level in the selected network.

- Absorbing Markov Chain (AMC) concept was used to estimate the probability and Expected Path Length (EPL). The probability analysis of the network's attack tree whereby an attacker will get to the target state and compromise the network was estimated using the transition probabilities of the Absorbing Markov Chain. This was calculated by normalizing the CVSS exploitability score over all the transitions starting from the attacker's source state. Also, the Expected Path Length (EPL) which indicates the number of steps an attacker will take to compromise the target state was also determined. In this research, it was interpreted that the EPL serves as the prediction of risk in a cyberspace network.
- Markov Reward Model (MRM) was used to estimate the degree of overall harm or loss that could occur as a result of the exploitation of a security vulnerability. The Markov Reward Model was used for evaluating the rewards associated with each vulnerability. When a vulnerability is exploited, it has associated reward which gives the impact.
- Finally, the model was extended to analyse and measure two key aspects, exploitability and impact properties associated with the cyberspace network security. An impact assessment (also known as impact analysis or consequence assessment) estimates the degree of overall harm or loss that could occur as a result of the exploitation of a security vulnerability.

iv. The Risk level (R) of the network was evaluated by synergizing both AMC and MRM.

v. Preventive measures that can be used to mitigate the consequences of these risk were proffered based on the Risk levels.

3.1 Data Collection from a Sample Network

The vulnerabilities dataset used for this research was collected using a sample network; Obafemi Awolowo

University Network (OAUnet). The description of the sample network, depicting the network infrastructure is as shown in Figure 2. The firewall rules that shows services running on each server host or machine and the actions that provide access to the cyberspace network services is as shown in Table 1. The critical information infrastructure in the network can be assessed through the domain name of the systems. Communication can take place in the system internally using the local area network and also externally using the internet. The systems that are interconnected in the network are a web server, DNS, e-portal, proxy, authentication and mail server. These servers are critical to the operation of the university that any disruption will cause a debilitating effect in the University.

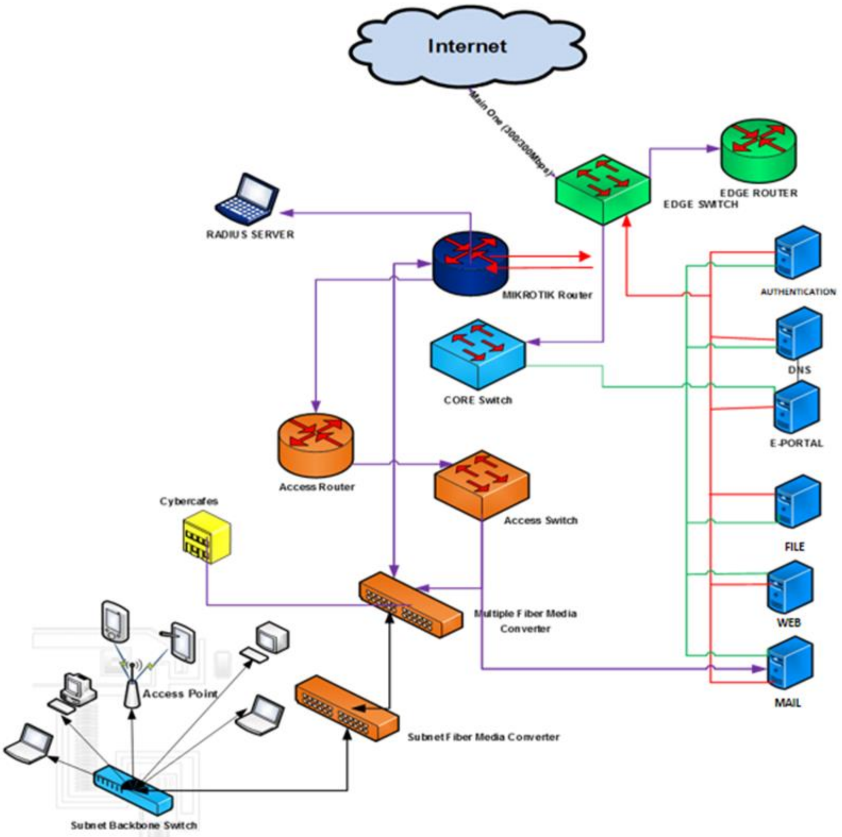


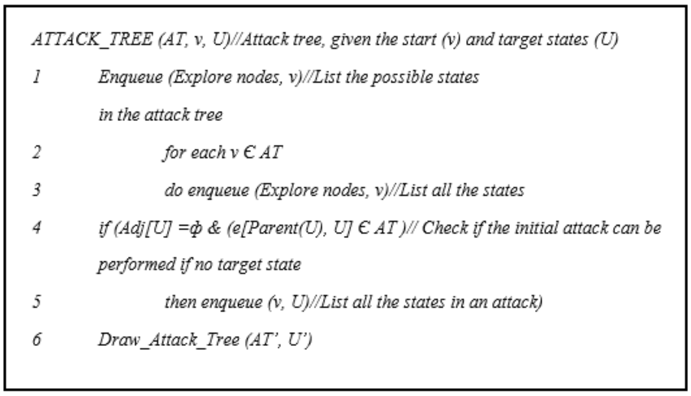
Figure 2. Sample Network Model

Table 1. Sample Network Security Firewall

S/N	Host	Services	Action
1	Authentication (Host1)	Apache	Allow
2	DNS (Host 2)	Linux	Allow
3	E-Portal(Host3)	Ftp	Allow
4	File (Host4)	SSL	Allow
5	Web(Host5)	Linux	Allow
6	Mail(Host6)	Ftp	Allow

3.2 Attack Tree Generation Algorithm

The formulated algorithm for generating the attack tree is shown in Algorithm 1. The model builder takes as input the network topology, services running on each host and a set of attack rules based on the vulnerabilities associated with the different services. This study used the Navigator Network Analysis software to generate the visualization and reachability of hosts which depict the attack scenario steps based on the vulnerabilities associated with the different services. This allows the study to capture the various security metrics leading to useful insights into the current security state of the network.



```
ATTACK_TREE (AT, v, U)//Attack tree, given the start (v) and target states (U)
    Enqueue (Explore nodes, v)//List the possible states
    in the attack tree
        for each v Є AT
        do enqueue (Explore nodes, v)//List all the states
    if (Adj[U] =ф & (e[Parent(U), U] Є AT )// Check if the initial attack can be
    performed if no target state
        then enqueue (v, U)//List all the states in an attack)
    Draw_Attack_Tree (AT', U')
```

Algorithm 1. Attack Tree generation Algorithm

3.3 Proposed Model Formulation

The major aim of this work is to assess cyberspace network security risk in terms of how resilient is the network based on the vulnerabilities risks level in the selected network i.e. OAUNET. The concepts employed were the combination of the efforts of Absorbing Markov Chain and Reward Model to know the overall exposure of the machines in the selected network to risk.

3.3.1 Absorbing Markov Chain Absorbing Markov Chain

This is used to calculate the transition probabilities from state i to state j. This depicts the different paths an attacker can take to reach the absorbing state. When the attacker gets to the absorbing state, it stays there and does not come out again. The Absorbing Markov Chain incorporates the vulnerability age that follows the Weibull distribution. Weibull distribution is used for life data analysis due to its versatility, flexibility, and simplicity. The Absorbing Markov Chain follows the Weibull distribution which is given by three parameters, the shape, the scale, and the location parameter. As the shape parameter increases, the probability distribution functions converge. Hence, Weibull distribution gives the best fit for life data analysis. The proposed Absorbing Markov Chain was used to generate the probability of an attack in the state i exploiting state j using the scoring rules in Figure 3.

3.3.2 Markov Reward Model

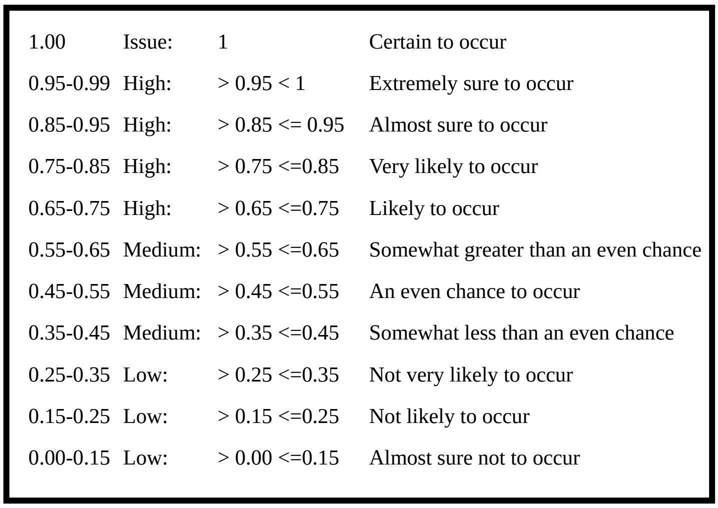
This shows the accumulated rewards associated with the vulnerability being exploited by the attackers. This is the rewards of being in a particular state. The rewards of the vulnerabilities being exploited by an attacker to transit from one state i to another state j are used to evaluate the impact of the vulnerability risk. By combining the output of individual effort of Absorbing Markov Chain and Markov Reward Model, the output gives the vulnerability risk level or vulnerability risk impact of the selected cyberspace network. The vulnerability risk level *(Rv*) was evaluated by combining the Absorbing Markov Chain and the rewards associated with it. The synergized model was realized by multiplying the transition probability *Pr(i,j)* with the reward rate (Impact) of the vulnerabilities on each state. The variable Impact (I) records the reward associated with the vulnerabilities on a network. The detailed model is as shown in Algorithm 2.

4. Results

R programming language which is an open-source was used as the tool to simulate and analyse the performance of the proposed model. The results obtained from the simulation of the risk assessment model of cyberspace network security situation are presented as follows:

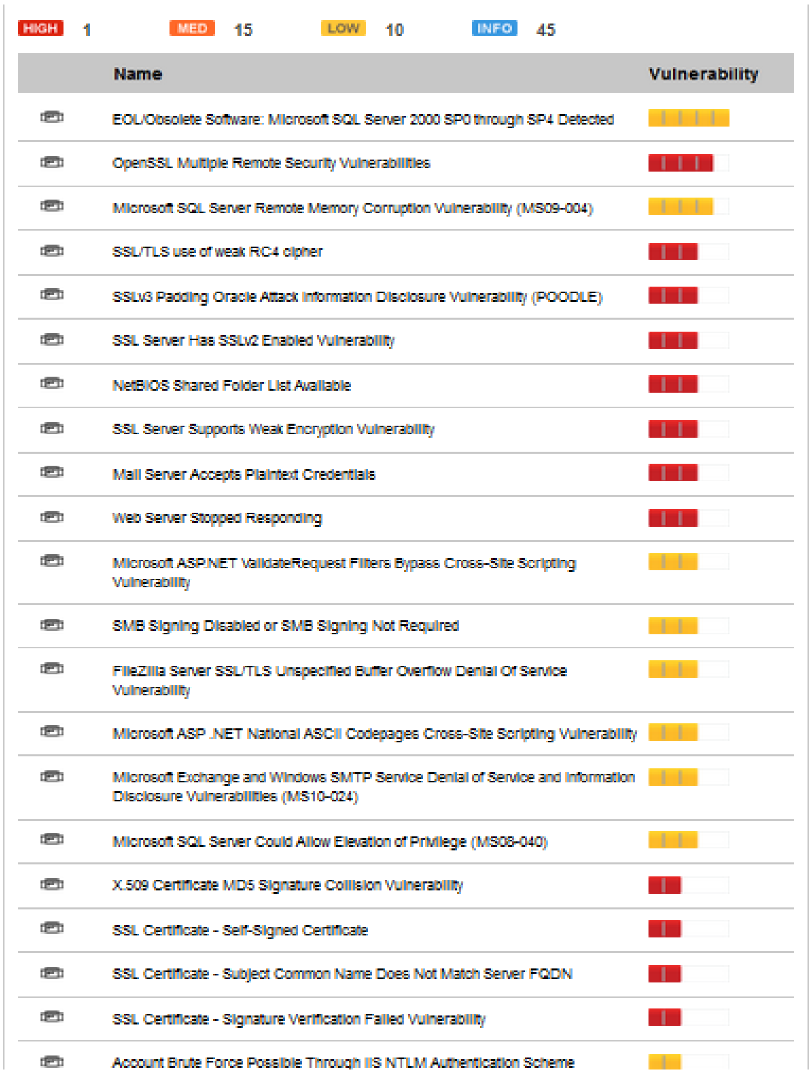
4.1 Data Collection Result

The scan result of the sample network is as shown in Figure 4. The result shows the vulnerability identification number as specified by the National Vulnerability Database (NVD) and also the nature of the characteristics of the vulnerability. Also, the exploitability analysis which focuses on assessing the evolving security state of the network was conducted. The exploitability score and date of disclosure collected is shown in Table 2.



1.00	Issue:	1	Certain to occur
0.95-0.99	High:	> 0.95 < 1	Extremely sure to occur
0.85-0.95	High:	> 0.85 <= 0.95	Almost sure to occur
0.75-0.85	High:	> 0.75 <=0.85	Very likely to occur
0.65-0.75	High:	> 0.65 <=0.75	Likely to occur
0.55-0.65	Medium:	> 0.55 <=0.65	Somewhat greater than an even chance
0.45-0.55	Medium:	> 0.45 <=0.55	An even chance to occur
0.35-0.45	Medium:	> 0.35 <=0.45	Somewhat less than an even chance
0.25-0.35	Low:	> 0.25 <=0.35	Not very likely to occur
0.15-0.25	Low:	> 0.15 <=0.25	Not likely to occur
0.00-0.15	Low:	> 0.00 <=0.15	Almost sure not to occur

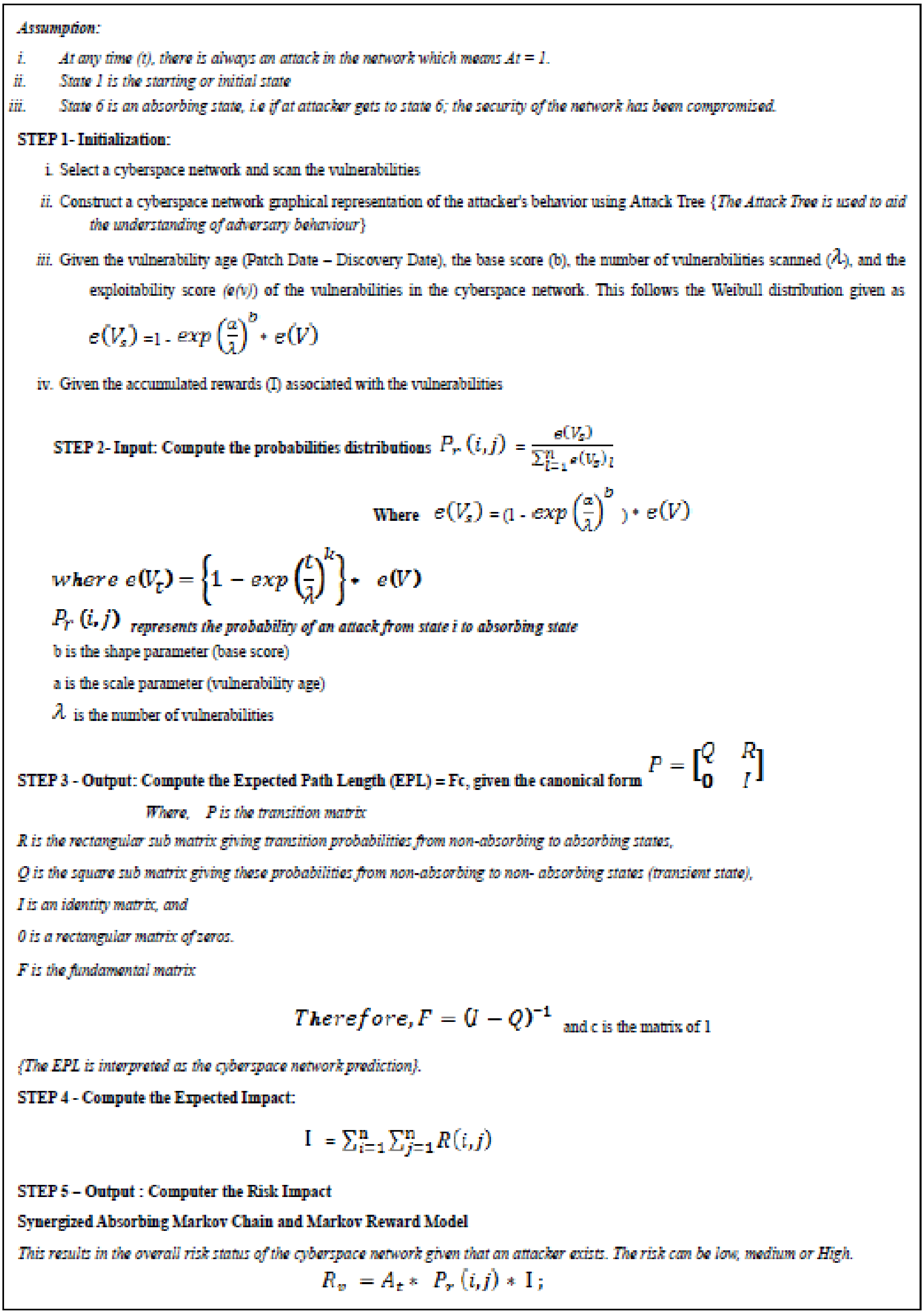
Figure 3. Scoring rules for probability distributions



HIGH 1 MED 15 LOW 10 INFO 45

Name	Vulnerability
EOL/Obsolete Software: Microsoft SQL Server 2000 SP0 through SP4 Detected	🟨🟨🟨🟨🟨
OpenSSL Multiple Remote Security Vulnerabilities	🟥🟥🟥🟥
Microsoft SQL Server Remote Memory Corruption Vulnerability (MS09-004)	🟨🟨🟨🟨
SSL/TLS use of weak RC4 cipher	🟥🟥🟥
SSLv3 Padding Oracle Attack Information Disclosure Vulnerability (POODLE)	🟥🟥🟥
SSL Server Has SSLv2 Enabled Vulnerability	🟥🟥🟥
NetBIOS Shared Folder List Available	🟥🟥🟥
SSL Server Supports Weak Encryption Vulnerability	🟥🟥🟥
Mail Server Accepts Plaintext Credentials	🟥🟥🟥
Web Server Stopped Responding	🟥🟥🟥
Microsoft ASP.NET ValidateRequest Filters Bypass Cross-Site Scripting Vulnerability	🟨🟨🟨
SMB Signing Disabled or SMB Signing Not Required	🟨🟨🟨
FileZilla Server SSL/TLS Unspecified Buffer Overflow Denial Of Service Vulnerability	🟨🟨🟨
Microsoft ASP .NET National ASCII Codepages Cross-Site Scripting Vulnerability	🟨🟨🟨
Microsoft Exchange and Windows SMTP Service Denial of Service and Information Disclosure Vulnerabilities (MS10-024)	🟨🟨🟨
Microsoft SQL Server Could Allow Elevation of Privilege (MS08-040)	🟨🟨🟨
X.509 Certificate MD5 Signature Collision Vulnerability	🟥🟥
SSL Certificate - Self-Signed Certificate	🟥🟥
SSL Certificate - Subject Common Name Does Not Match Server FQDN	🟥🟥
SSL Certificate - Signature Verification Failed Vulnerability	🟥🟥
Account Brute Force Possible Through IIS NTLM Authentication Scheme	🟨🟨

Figure 4. The Vulnerabilities scanned from Sample Network



Assumption:

i. *At any time (t), there is always an attack in the network which means At = 1.*
ii. *State 1 is the starting or initial state*
iii. *State 6 is an absorbing state, i.e if at attacker gets to state 6; the security of the network has been compromised.*

STEP 1- Initialization:

i. Select a cyberspace network and scan the vulnerabilities

ii. Construct a cyberspace network graphical representation of the attacker's behavior using Attack Tree {*The Attack Tree is used to aid the understanding of adversary behaviour*}

iii. Given the vulnerability age (Patch Date – Discovery Date), the base score (b), the number of vulnerabilities scanned (λ), and the exploitability score *(e(v))* of the vulnerabilities in the cyberspace network. This follows the Weibull distribution given as $e(V_s) = 1 - exp\left(\frac{a}{\lambda}\right)^b * e(V)$

iv. Given the accumulated rewards (I) associated with the vulnerabilities

STEP 2- Input: Compute the probabilities distributions $P_r\,(i,j) = \frac{e(V_s)}{\sum_{i=1}^{n} e(V_s)_i}$

Where $e(V_s) = (1 - exp\left(\frac{a}{\lambda}\right)^b\;) * e(V)$

$$where\ e(V_t) = \left\{1 - exp\left(\frac{t}{\lambda}\right)^k\right\} *\ e(V)$$

$P_r\,(i,j)$ ***represents the probability of an attack from state i to absorbing state***

b is the shape parameter (base score)

a is the scale parameter (vulnerability age)

λ is the number of vulnerabilities

STEP 3 - Output: Compute the Expected Path Length (EPL) = Fc, given the canonical form $P = \begin{bmatrix} Q & R \\ \mathbf{0} & I \end{bmatrix}$

Where, P is the transition matrix

R is the rectangular sub matrix giving transition probabilities from non-absorbing to absorbing states,

Q is the square sub matrix giving these probabilities from non-absorbing to non- absorbing states (transient state),

I is an identity matrix, and

0 is a rectangular matrix of zeros.

F is the fundamental matrix

$$Therefore, F = (I - Q)^{-1}$$ and c is the matrix of 1

{The EPL is interpreted as the cyberspace network prediction}.

STEP 4 - Compute the Expected Impact:

$$\mathrm{I} = \sum_{i=1}^{n} \sum_{j=1}^{n} R(i,j)$$

STEP 5 – Output : Computer the Risk Impact

Synergized Absorbing Markov Chain and Markov Reward Model

This results in the overall risk status of the cyberspace network given that an attacker exists. The risk can be low, medium or High.

$$R_v = A_t * P_r\,(i,j) * \mathrm{I}\,;$$

Algorithm 2. Proposed Model

Table 2. Exploitability Score and Disclosure Date

Service Name	CVE-ID	Exploitability Score	Host	Disclosure Date
Apache	CVE-2014-1878	10	Host 1	07/08/2013
Linux	CVE-2013-1324	8.6	Host 2	11/13/2013
Ftp	CVE-2013-4782	10	Host 3	07/08/2013
SSL	CVE-2014-0063	7.9	Host 4	02/17/2014
Linux	CVE-2014-0038	3.4	Host 5	02/06/2014
Ftp	CVE-2014-0098	10	Host 6	03/18/2014

4.2 Attack Tree Generation

Figure 5 gives the graphical representation of the attack scenario that shows the visualization and reachability of a network, assuming that the starting state is 1 and the absorbing state is 6. The graphical representation is the attack tree that was generated by combining the relationships between the vulnerabilities present in the network. This shows the scenario whereby an attacker can gain root access to root access, which is machine 6.

The Attack scenario was generated based on the inter-relationships between the vulnerabilities present on the networks. The vulnerabilities are unique and publicly known and are denoted by a CVE (Common Vulnerability and Exposure) identifier. For instance, Apache web-server has vulnerability CVE-2014-1878 and publicly disclosed on 07/08/2013 which allows remote attackers to execute arbitrary code.

The network is comprised of 6 machines that are interconnected together and operating internally behind a firewall. Host 1 is running Apache Web-server. The presumed aim of the attacker will be to infiltrate the network and gain root access on Host 6. To achieve this, the attacker will attempt to exploit the apache web-service since that is the only port (80) accessible from the firewall. Once this is exploited, access will be gained and the attacker will then need to slowly work through the network to achieve the target goal as shown in Figure 4.

4.3 Simulation Results

The simulation results of the proposed model are as follows:

4.3.1 Assessment Using Absorbing Markov Chain

Based on the Attack tree generated for the cyberspace security network, a simulation of the Absorbing Markov Chain was conducted. The attack tree incorporated the exploitability level and base score that was formulated. The transition probability generated based on the exploitability score is shown in Figure 6. The Absorbing Markov Chain was used to estimate the number of steps an attacker will take to infiltrate a network. The number of steps is called the expected path length and this is indicated in Table 3.

4.3.2 Assessment Using Markov Reward Model

The consequence or impact analysis was estimated using Markov Reward Model. The impact is the accumulated rewards associated with the vulnerabilities present in the cyberspace network machines. This is as shown in Figure 6. In this result, it was observed that the impacts increases as the number of vulnerability increases and this is an indication that the attacker with “technical skills will rather exploit the machines with quite several vulnerabilities, for instance, OpenSSL, Filezilla, SQL server, ASP.Net, and PHP vulnerabilities with greater impact. Figure 7 shows the graph of the impact based on the number of vulnerabilities.

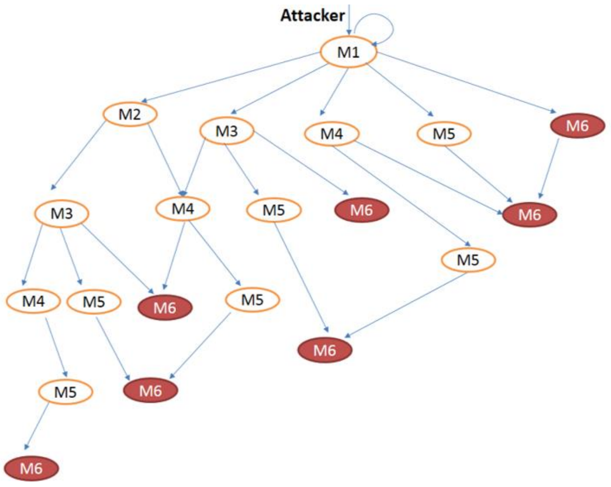


Figure 5. Attack Scenario

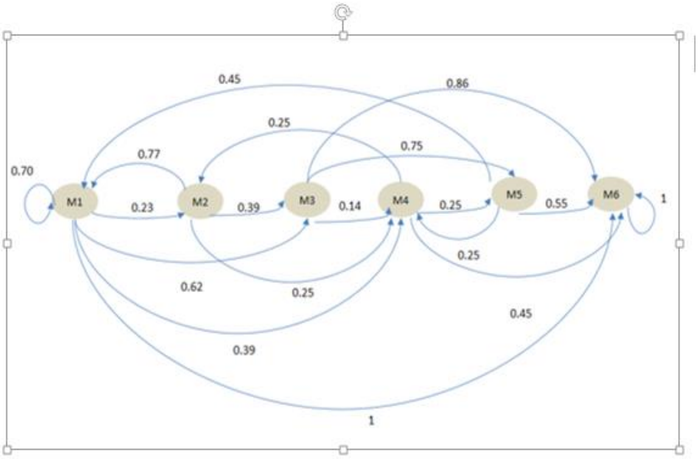
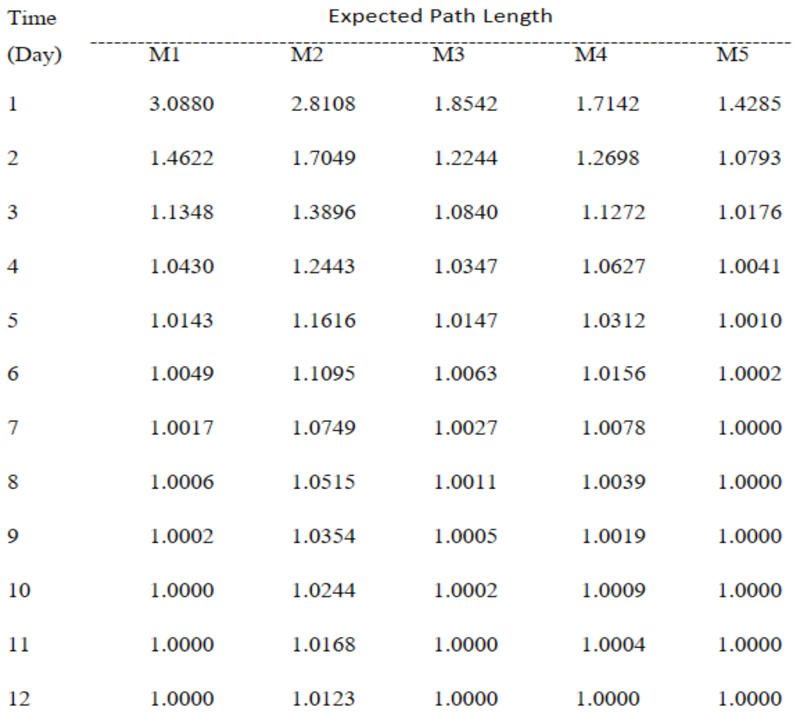


Figure 6. Transition of Attackers from one state to another

4.3.3 Assessment Using the Combined Features of the Developed Model

The synergy of Absorbing Markov Chain and Markov Reward Model analyses the overall risk level of the selected cyberspace network security. The probability distribution generated by R-software package using Absorbing Markov Chain was synergized with the Expected Impact gotten using Markov Reward Model. The product of this model generated the risk level of the machines on the network as shown in Figure 8. The risk assessment output obtained from the synergy of Absorbing Markov Chain and Markov Reward Model was presented based on the vulnerability risk level. Tables 4and 5 shows the risk assessment results on each machine and the decision on the protection and resilience actions respectively.

Table 3. Expected Path Length using Absorbing Markov Chain



Time	Expected Path Length				
(Day)	M1	M2	M3	M4	M5
1	3.0880	2.8108	1.8542	1.7142	1.4285
2	1.4622	1.7049	1.2244	1.2698	1.0793
3	1.1348	1.3896	1.0840	1.1272	1.0176
4	1.0430	1.2443	1.0347	1.0627	1.0041
5	1.0143	1.1616	1.0147	1.0312	1.0010
6	1.0049	1.1095	1.0063	1.0156	1.0002
7	1.0017	1.0749	1.0027	1.0078	1.0000
8	1.0006	1.0515	1.0011	1.0039	1.0000
9	1.0002	1.0354	1.0005	1.0019	1.0000
10	1.0000	1.0244	1.0002	1.0009	1.0000
11	1.0000	1.0168	1.0000	1.0004	1.0000
12	1.0000	1.0123	1.0000	1.0000	1.0000

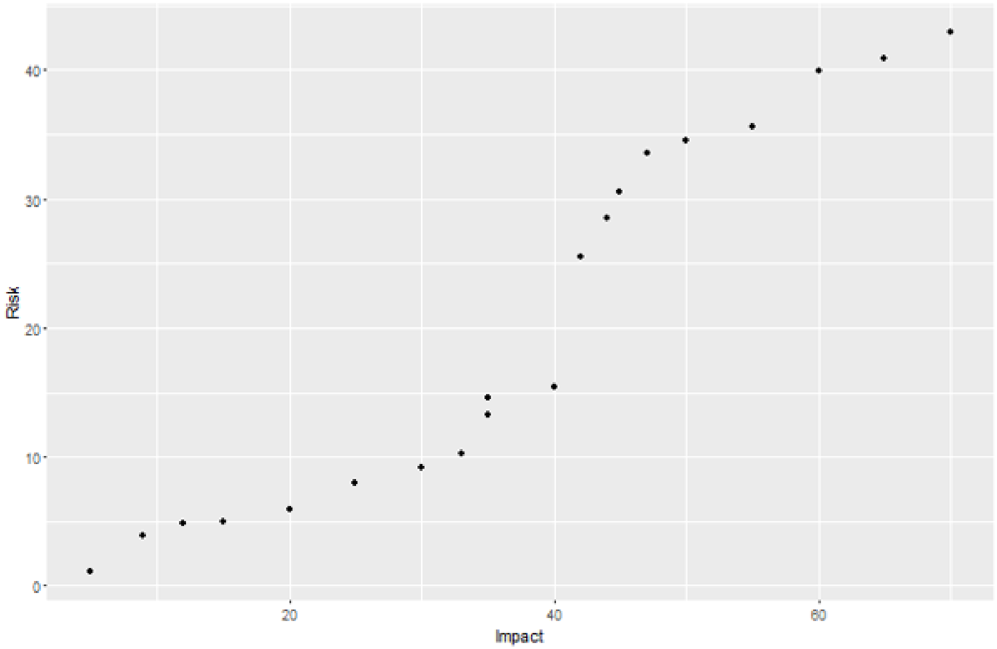


Figure 7. Simulation result of Expected Impact based on the vulnerabilities

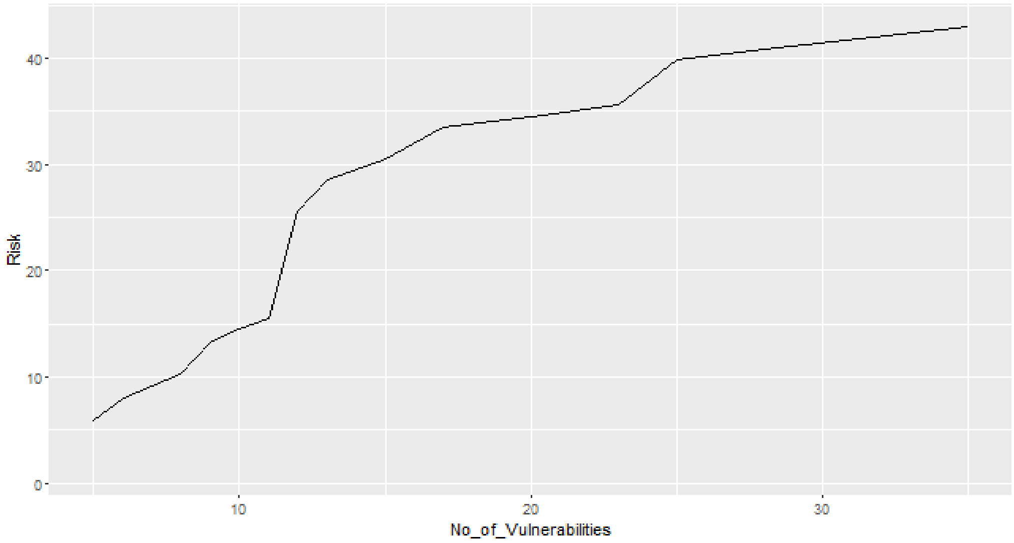


Figure 8. Simulation result of the Risk Level

Table 4. Risk Assessment Results

Machine	Probability	Impact	Risk Impact	Decision
M1	0.7	59.9	41.9 (Medium)	Control
M2	0.23	66.4	15.2(Low)	Accept
M3	0.62	84.4	52.3(Medium)	Control
M4	0.39	52.9	20.6(Low)	Accept
M5	0.45	54.9	24.7(Low)	Accept
M6	1	79	79.0(High)	Transfer/Reject

Table 5. Decisions on protections and resilience actions

Risk Impact	Remediation
Low: 0.0 – 39	Absorb / Accept / Tolerate
Medium: 40 – 69	Install the latest version of the update Shutdown ports that are not needed Ensure a security policy in place.
High: 70 - 100	Firewall Policies Patch Installation Whitelisting and Execution control Disable open and unused services

4.4 Model Evaluation Results

A simulation was done in R package, to evaluate the performance of the proposed risk assessment model. The result is presented in Table 6. Also, a quantitative evaluation was performed by benchmarking the performance of the proposed model with an existing Absorbing Markov Chain model using Reliability and Availability as a performance metric.

4.4.1 Reliability

This shows the strength of the model, that is, how reliable the model developed is. The reliability of the model was generated by employing the Mean-Time-To-System-Failure (MTTSF) of the developed model. The developed model gives 86.7% reliability, while the reliability of the existing model gives 57.8%. This means that the reliability performance comparison of the developed model gives a 28.9% increase over the existing model. Thus, higher reliability was achieved in the developed model. This implies that the synergized model has a better performance of the trust. The MTTSF result is shown in Figure 9.

4.4.2 Availability

This shows the readiness of usage. This used the product of the average number of times state i is visited and the mean sojourn time in the state. The result is shown in Figure 10. It is obvious in this performance evaluation result that the availability of the proposed model is 93%, while the availability of the existing model is 81%. This means that the developed model has a better performance in increasing the effectiveness of the assessment model in terms of availability requirement.

Table 6. Evaluation Results of the Existing and Proposed Models

Time (Days)	Reliability	Reliability	Availability	Availability
	(Existing)	(Proposed)	(Existing)	(Proposed)
1	1.2	3	2.7	3.9
2	1.9	3.5	3.2	4.4
3	2.3	3.9	3.9	5.1
4	2.8	4.6	4.6	5.8
5	3.8	5.9	5.7	6.9
6	4.6	6.2	6.2	7.4
7	5.2	7.6	7.1	8.2
8	5.6	8.8	7.6	8.9
9	6.7	9.2	9.2	9.6
10	7.2	10.3	9.7	10.2
11	7.9	11.2	10.2	10.9
12	8.6	12.5	10.9	11.7
Total	57.8	86.7	81	93

5. Conclusion

This study used a stochastic model to access the security state of a selected cyberspace network. An improved risk assessment model was formulated by employing the concepts of Absorbing Markov Chain and Reward Model to know the overall exposure to the risk of the machines in the selected cyberspace network. The risk was scaled and it was observed that machine 6 has the highest exposure level to cyberspace risk in the selected network. The individual effort of Absorbing Markov Chain and its Rewards were analysed which gives the insight to understand the security status of the sample network. In comparison with the existing model, the proposed risk assessment model is higher in all measures. The proposed model has higher reliability of 28.9% and higher availability of 12% over the existing model. The results from the performance evaluation show that there is an improvement in the assessment of security situations in a cyberspace network using the synergy of Absorbing Markov Chain and Markov Reward Model. However, it is recommended for future work that zero-day exploit which are the vulnerabilities that are discovered but not yet fixed and also the resilience and the robustness of the network components should be considered.

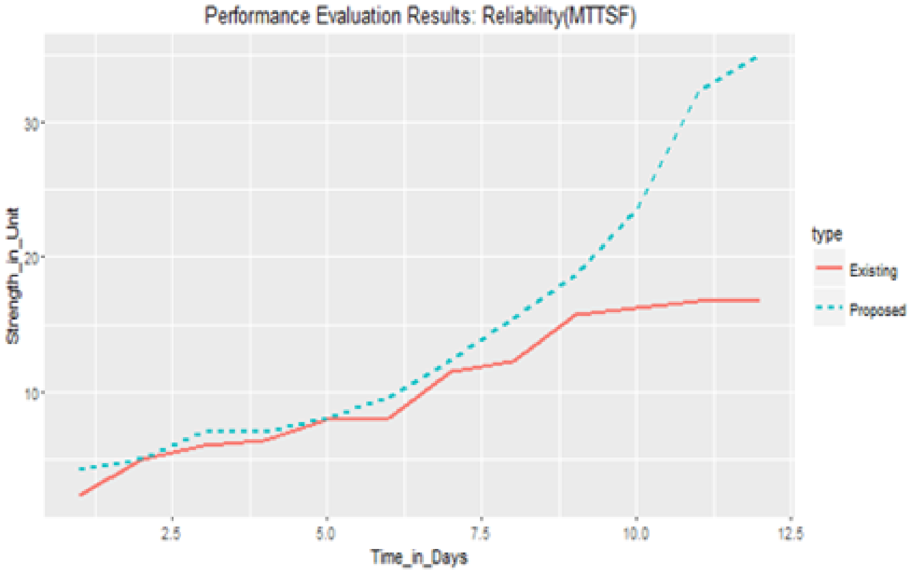


Figure 9. Comparisons of the Reliability of Proposed and Existing Models

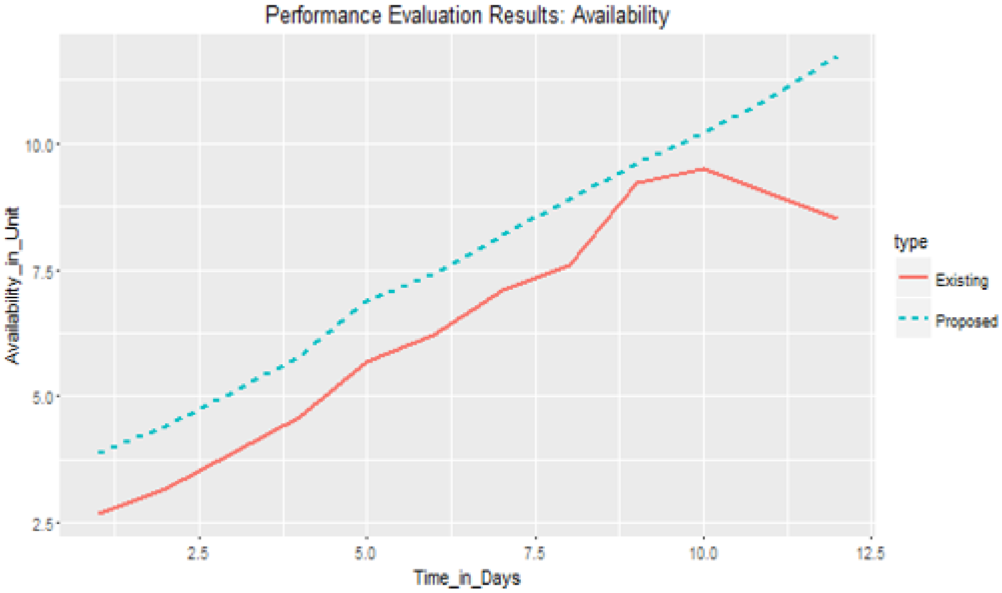


Figure 10. Comparisons of the Availability of Proposed and Existing Models

Acknowledgements

This Research was funded by the TETFund Research Fund" and Africa Centre of Excellence OAK-Park, Obafemi Awolowo University, Ile-Ife, Nigeria.

References

Abraham, S., & Nair, S. (2014). Cyber Security Analytics: A Stochastic Model for Security Quantification Using Absorbing Markov Chains. *Journal of Communications*, *9*(12), 899-907. https://doi.org/10.12720/jcm.9.12.899-907

Akinwumi, D. A., Iwasokun, G. B., Alese, B. K., & Oluwadare, S. A. (2017). A review of game theory approach to cyber security risk Management. *Nigerian Journal of Technology (NIJOTECH), 36*(4), 1271-1285. https://doi.org/10.4314/njt.v36i4.38

Akinyemi, B. O, Jekoyemi, O. V, Aladesanmi, T. A., Aderounmu, G. A., & Kamagate, B. H. (2018b). A Scalable Attack Graph Generation for Network Security Management. *Journal of Computer Science and Information Technology, 6*(2), 30-44. https://doi.org/10.15640/jcsit.v6n2a4

Akinyemi, B. O., Amoo, A. O., & Aderounmu, G. A. (2015). Performance Prediction Model for Network Security Risk Management. *Communications on Applied Electronics (CAE), 2*(8), 1-7. https://doi.org/10.5120/cae2015651816

Akinyemi, B. O., Amoo, A. O., & Olajubu, E. A. (2014). An Adaptive Decision-Support Model for Data Communication Network Security Risk Management. *International Journal of Computer Applications, 106*(8), 1-7. https://doi.org/10.5120/18537-9752

Akinyemi, B. O., Oyebade, A. I., Amoo, A. O., Oyegoke, T. O., Aladesanmi, T. A., & Aderounmu, G. A. (2018a). System Simulation of A Bayesian Network-Based Performance Prediction Model for Data Communication Networks. *International Journal of Computer, 31*(1), 119-136.

Byres, E., Leversage, D., & Kube, N. (2007). Security incidents and trends in SCADA and process industries. *The industrial Ethernet book, 39*, 12-20.

Conrad, J. R. (2005). *Analyzing the Risk of Information Security Investment with Monte-Carlo Simulation.* Paper presented at the Fourth Workshop on Economics of Information Security, Harvard University, Cambridge, June 2-3, 2005. Retrieved from http://infosecon.net/workshop/ pdf/13.pdf

Frei, S., May, M., Fiedler, U., & Plattner, B. (2006). Large-Scale Vulnerability Analysis. *Proceedings of the 2006 SIGCOMM workshop on Large-scale attack defense (SIGCOMM'06)*, 131-138. https://doi.org/10.1145/1162666.1162671

Houmb, S. H., & Franqueira, V. N. L. (2009). Estimating ToE Risk Level Using CVSS. *Proceedings of the Fourth International Conference on Availability, Reliability and security*, 718-725. https://doi.org/10.1109/ARES.2009.151

Joh, H. C., & Malaiya, Y. K. (2011). Defining and Assessing Quantitative Security Risk Measures Using Vulnerability Lifecycle and CVSS. *Proceedings of the International Conference. Security and Management (SAM'11)*, 10-16.

Joh, H., & Malaiya, Y. K. (2010). A Frameworks for Software Security Risk Evaluation using the Vulnerability Lifecycle and CVSS Metrics. *Proceedings of International Workshop on Risk and Trust in Extended Enterprises*, 430-434.

Khan, M. A., & Hussain, M. (2010). Cyber Security Quantification Model. *The journal of Bahria University Information Communication and Technologies (BUJICT*), *3*(1), 39-44. https://doi.org/10.1145/1854099.1854130

McQueen, M., Boyer, W. F., Flynn, M. A., & Alessi, S. (2006). Quantitative Risk Reduction Estimation Tool for Control Systems – Suggested Approach and Research Needs. *Proceedings of the International Workshop on Complex Network and Infrastructure Protection*, 1-21.

Musman, S., & Turner, A. (2018). A game theoretic approach to cyber security risk management. *Journal of Defense Modeling and Simulation: Applications, Methodology, Technology, 15*(2), 127-146. https://doi.org/10.1177/1548512917699724

National Security Strategy. (2011). *Strategy for Operating in Cyberspace.* Department of Defense, United States of America July, 2011. 1-19. Retrieved from https://csrc.nist.gov/CSRC/media/Projects/ISPAB/documents/DOD-Strategy-for-Operating-in-Cyberspace.pdf

Rajasooriya, S. M., Tsokos, C. P., & Kaluarachchi, P. K. (2017a). Stochastic Modelling of Vulnerability Life Cycle and Security Risk Evaluation. *Journal of information Security, 7*, 269-279. https://doi.org/10.4236/jis.2016.74022

Rajasooriya, S. M., Tsokos, C. P., & Kaluarachchi, P. K. (2017b). Cyber Security: Nonlinear Stochastic Models for Predicting the Exploitability. *Journal of Information Security, 8*, 125-140. https://doi.org/10.4236/jis.2017.82009

Tsakanyan, V. T. (2017). The role of Cybersecurity in world politics. *Vestnik RUDN. International Relations, 17*(2), 339-348. https://doi.org/10.22363/2313-0660-2017-17-2-339-348

Verendel, V. (2009). Quantified security is a weak hypothesis: a critical survey of results and assumptions. *Proceedings of 2009 workshop on new security paradigms workshop*, 37-49. https://doi.org/10.1145/1719030.1719036

Xie, A., Cai, Z., Tang, C., Hu, J., & Chen, Z. (2008). Evaluating Network Security with Two-Layer Attack Graphs. *Proceedings 2008 IEEE Annual Computer Security Applications Conference*, 127-138. https://doi.org/10.1109/ACSAC.2009.22

Ye, N., Newman, C., & Farley, T. R. (2006). A System-Fault-Risk Framework for cyber-attack classification. *Information Knowledge Systems Managemen*t, 135-151.