IOP Conf. Series: Materials Science and Engineering **732** (2020) 012037 doi:10.1088/1757-899X/732/1/012037

Cognitive artificial intelligence application to cyber defense

A D W Sumari[1,2,*], A Setiawan[1] and I N Syamsiana[1]

[1] Department of Electrical Engineering, State Polytechnic of Malang, Malang, East Java, Indonesia
[2] Faculty of Defense Technology, Indonesia Defense University, Sentul, West Java, Indonesia

*arwin.sumari@polinema.ac.id

Abstract. Predicting or estimating the occurrence of a cyberattack has been a challenge for various sectors including defense one. In this paper we propose a new method for making a prediction or an estimation of the occurrence of cyberattacks in terms of the attack type or category and when the attack(s) would be possible to occur. Our method based on Cognitive Artificial Intelligence (CAI) approach called as Knowledge Growing System (KGS). For this purpose, we did a simulation using random numbers which were generated based on the real data from UNSW-NB15. From the simulation results, we can conclude that CAI is able to deliver a prediction or an estimation of the occurrence of future possible cyberattacks.

1. Introduction

The existence of cyberspace because of the inventions in electronics, communications, and informatics technology has been attracted various parties to take advantages and utilize it for various needs. For some parties, cyberspace is said as a new domain for doing anything as the real ones such land, air, sea, and aerospace domains. From economy people view, cyberspace can give positive impacts to any party such as leverage the nation's or people's economy. For industry people, cyberspace can accelerate the industrial process, reduce the overhead, and increase the income. For military people, cyberspace is said as a new domain of warfare where such space can become combat area for conflicting parties. From those simple views, it can be seen clearly that cyberspace has two sides which can be utilized partly or whole for good and bad. The bad use of cyberspace is often materialized as cyberattacks with various reasons behind them. They can be from state actor, non-state actor, state-sponsored actor, or the combination of actors. Even though it was not admitted clearly, cyberattacks to some countries about 7 to 12 years ago can be categorize as cyberattacks from combined actors.

Cyberattack can occur anytime, anywhere, and without warning. On the other hand, predicting or estimating a cyberattack has also been a challenge knowing that the cyberspace and the actors involve with it are very dynamic. Tracking back the source(s) of the cyberattack(s) is time-consume and needs huge resources. In guarding systems which are vulnerable to cyberattacks, there are some approaches namely, reactive, active, and proactive defense [1]. Simply, reactive defense is carried out when an attack enters to the network or system, active defense is carried out when the attack is occurring, while proactive defense is carried out before an attack shows up in the network or system. Proactive defense can be said as an anticipation action by looking ahead what possible cyber threats which may evolve to become real cyberattacks in the future. In such defense, having knowledge of them is very necessary. It

is like having knowledge of the weather conditions as the basis to assess what would happen in the future such as rain, dray, or storm.

By having knowledge of possible cyberattacks in the future, then we can do assessment and carry out necessary as well as proper actions to defense the networks or systems. Thus, it can reduce time and resources. Having knowledge in advance by looking ahead the recent phenomenon for making anticipations is called as prediction or estimation. There are many prediction or estimation approaches that can be used. One of the approaches is based on Artificial Intelligence (AI). AI has been used for prediction tool such as in weather forecasting, etc. In this paper we will use AI for predicting or estimating the occurrence of possible cyberattacks in terms of the attack type or category and the possible time of the attack(s) would occur.

Artificial Intelligence (AI) is a technology that is used to emulate human intelligence in order to assist humans in doing their daily works safer, quicker, easier, more economics, and 24-hour ready. AI has been applied in many sectors especially in ones which are time-critical, high-risk, and carrying out continuous operation. Examples of the system such that are cyber defense system where its job not only monitors the flow of cyberattacks but also categorizes the types of cyberattack in 24 hours' continuous manner. The challenge has been facing by sectors is how to predict when the cyberattack can be probable occurred and what type(s) of cyberattack may probable come the system. Works on cyberattacks forecasting had also been done by some researchers such as employing multi-faceted machine learning by using unconventional signals to predict cyberattacks, using supervised learning on artificial neural network by using empirical data for predicting cyber intrusion, and probabilistic-based mathematical model to predict a cyberattack quantitatively [2-4].

This paper is arranged as follows. Our intention regarding the need of prediction or estimation means for proactive defense is already given in Section 1. In Section 2, some relevant materials will be given in Section 2 such as cyberattack categories and the basic of our proposed prediction tool. The example of the usage of our proposed prediction tool to a real data will be given in Section 3. We conclude our paper in Section 4.

2. Relevant theories

2.1. Cyberattack categories

Cyberattack is defined as an action which uses cyberspace as a medium to deliver an attack or attacks to computer networks or systems by means of malacious software. Meanwhile malacious software or simply malware is is (1) A virus or other malicious software that is attached to a program preloaded on a computer or external hard drive, (2) A Central Processing Unit (CPU) chip in a computer or handheld device that has a built-in back door, enabling an attacker to gain illegal entrance [5]. In our paper we adopt the categories of cyberattack from UNSW-NB15 data set [6]. Refer to [6], there are 9 categories of cyberattack, namely Analysis, Backdoors, Denial of Service (DoS), Exploit, Fuzzer, Generic, Reconnaissance, Shellcode, and Worm. The number of occured attacks from each category is summarized in table 8, the number of events for all categories of attack, while the number of events of the normal category access is 2,218,761. The total data sample is 2,540,044.

- Analysis is a kind of attack which does penetration to a computer network or system by performing port scanning, delivering spam, or using Hypertext Markup Language (HTML). Such attack is aimed to get information regarding holes in ports, or steal passwords by putting a trap via spams sent through emails or links in HTML.
- Backdoor is a kind of attack which gives a discretion to someone or something to illegally access a computer network or system as well as its data without detected. Such attack can be prepared from the beginning before the system is installed.
- DoS is a kind of attack which is carried out by flooding a network or computer server with messages repeatedly and making it busy so the legitimated users cannot access it temporarily for some time.

- Exploit is used by unlegitimated user to gain access to a computer network or system because he already knows that there is a hole which can be utilized for his own interests.
- Fuzzer commonly is used by pen-tester as a part of stress test to a computer network by feeding random data to observe if it experiences errors or probably hangs up. This method is also used by unlegitimated users to cause a computer network or system, or it softwares stops operating or suspended for some time.
- Generic is a kind of attack which works against all block ciphers (with a given block and key size), without consideration about the structure of the block-cipher [6].
- Reconnaissance is an activity to obtain information about a computer network or system as well as its activities and all resources it has. The information includes vulnerability points which can be utilized to gain access to such network or system.
- Shellcode can be a medium by unlegitimated user to have knowledge about a computer network or system's vulnerability by injecting a certain payload. If it is succeeded, then the unlegitimated user can explore the weaknesses of such network or system.
- Worm is a kind of attack which is hidden within an official-like letter through email or link in a web site. Once it is clicked, it automatically spreads itself to all the computers in the network or to all targeted files in the computer.

Table 1. Number of events for all attack categories.

No.	Attack Categories	Number of events
1	Analysis	2,677
2	Backdoor	2,329
3	DoS	16,353
4	Exploit	44,525
5	Fuzzer	24,246
6	Generic	215,481
7	Reconnaissance	13,987
8	Shellcode	1,511
9	Worm	174
	Total	**321,283**

2.2. Artificial intelligence application for proactive defense

AI technology has been explored and applied in many sectors but not many of such technology applied in defense sector especially in cyber defense. In today's paradigm, conventional warfare is not common knowing that new technology has given a new lethal weapon called cyber weapon which is materialized in form of cyberattacks. Paralyze a nation's defense system can easily be done by just clicking some buttons, where these buttons give commands to deliver cyber weapon such the ones shown in Table 8. Cyber weapon can be grouped into three categories. The first one is in the form of software which is called malicious software (malware), the second one is in the form of hardware which is called as malicious hardware, and the third one is in the form of attacks to brainware or cognitive attack [7]. In this case we are talking about malware as cyber weapon. Even though there are hard cases of cyber weapon usages which caused computer networks in some countris stop working for almost a month, the probability of a warfare in and through cyberspace between state actors is very low. But, non-state actors and state-sponsored actors have to be taken into account because they have high probabiliy to deliver cyber weapon which may attack the defense system. This matter has to be anticipated before the cyberattacks occur.

Fortunately, the defense sector inherently already has a mechanism for anticipation of possible future threats to the their systems specifically and to the nation generally. This mechanism is called as contingency plan which contains such as the list of possible threats, the resources which are already prepared, the stakeholders involve when the contingency occurs, and the steps when performing the contingency. For setting up the proper plan, the planners should have knowledge about the future

possible threats. In the case of cyberattack, given so many data of cyberattacks a tool which can help them to extract knowledge from the data is a necessity. Therefore we propose AI approach as predictor or estimator for proactive defense. Differ from AI approaches have been done by other researchers such as machine learning or artificial neural networks which have knowledge from past data or experiences, our AI approach uses new data as the basis for having knowledge of possible future cyberattacks. Our approach is called as Cognitive AI (CAI).

2.3. Cognitive approach for artificial intelligence

As mentioned by Herbert Simon in Sumari and Sutikno, AI has two purposes [8]. The first one is to augment human thinking and the second one is to understand how human thinks. Most of AI applications are for augmenting human thinking and just a little are for the second purpose. Originally from the psychology perspective, human becomes intelligent because of knowledge generated within his brain. The knowledge generation, which is taken from contructivism theory of psychology field, can be done in two ways namely, learning from past data or experience and learning by interaction with phenomenon. We made an important note for the latter mechanism. In this mechanism, the generated knowledge comes from new data, that is when human is making interaction with the phenomenon. At first, he does not have knowledge at all about the phenomenon because he just see, hear, smell, taste, or touch it. After making interaction, he gets knowledge about it and this is what is called as new knowledge which grows for nothing.

The latter mechanism has been researched which gave a birth a new perspective in AI called Knowledge Growing System (KGS) in 2009 [9-11]. KGS simply is a system that is capable of growing its own knowledge as the accretion of information it receives as the time passes. At the end of the learning phase the system's brain will generate new knowledge regarding the phenomenon and can use this knowledge to make prediction or estimation of possible future the same or similar phenomenon. Knowledge generation represents cognitive characteristic shown by human brain. KGS emulates this characteristic and answers the second purpose of AI as mentioned by Herbert Simon. This is the reason we call KGS as the main engine of CAI [12].

In most cases in real life human thinks probabilistically. Human is always faced with situations where there are many data with many alternatives as options that can be choosed or selected as the decision. This condition has been handled by KGS. The main component of KSG is information-inferencing fusion method called as ASSA2010. This method has been submitted for patent of Intellectual Property Right (IPR) since the beginning of 2019 [13]. Taken from Sumari and Ahmad, ASSA2010 is briefly explained follows [14].

Let us assume that $\delta = 1, \ldots, i, \ldots, n$ is the number of sensor or multi-sensor, $\lambda = 1, \ldots, j, \ldots, m$ is a collection of hypotheses or multi-hypothesis of phenomenon regarding the information supplied by the multi-sensor. At the end of the computation, λ is also functioned as the numbers of fused information from multi-sensor that explain a collection of individual phenomenon based on the multi-hypothesis.

Notation $P\left(\upsilon_j^i\right)$ represents the probability hypothesis *j* is true given information sensed and perceived by sensor *i*. The Degree of Certainty (DoC) represented by $P\left(\psi_1^j\right)$ defines that hypothesis *j* is selected based on the fusion of the information delivered from multi-sensor, that is, from $P\left(\upsilon_j^1\right)$ to $P\left(\upsilon_\delta^j\right)$ where $j = 1, \ldots, \lambda$. The subscript "1" in notation $P\left(\psi_1^j\right)$ means that the computation results are DoC at time 1 or the first observation time. This number is required if we want to have the next observation to be computed. The information fusion to obtain a collection of DoC is given in (1).

$$P\left(\psi_1^j\right) = \frac{\sum_{i=1}^{\delta} P\left(\upsilon_j^i\right)}{\delta} \tag{1}$$

where $P\left(\psi_1^j\right) \in \Psi$ and it is called as New Knowledge Probability Distribution (NKPD). This is a collection of information that can be furthered extracted to obtain inference or new knowledge. The inference or new knowledge at this point can be obtained by applying (2).

$$P\left(\psi_1^j\right)_{estimate} = \odot\left[P\left(\psi_1^j\right)\right] \quad (2)$$

where $\odot[\ldots] = \max[\ldots]$. $P\left(\psi_1^j\right)_{estimate}$ is the inference of $P\left(\psi_1^j\right) \in \Psi$ which later become new knowledge of KGS. The growing of knowledge over time is obtained by employing time parameter. The advancement of ASSA2010 method that already involves time parameter gave rise to new method called Observation Multi-time ASSA2010 (OM-ASSA2010) method and knowledge distribution resulted from the application of this method is called as New Knowledge Probability Distribution over Time (NKPDT). The quality of the grown knowledge is measured using (3).

$$DoC = \left|P\left(\theta_j\right)_{estimate} - \phi_1^j\right| \times 100\% \quad (3)$$

with $P\left(\theta_j\right)$ is information-inferencing of $P\left(\psi_\gamma^j\right)$ after several observation time to the phenomenon and ϕ_1^j is the knowledge probability of the most correct fused-information j which represents the phenomenon at observation time γ_1 . In the case of knowledge extraction, (1) can be used to assess how good is the extracted knowledge compared to the true phenomenon being observed. The extracted knowledge of the phenomenon which is represented by NKPD or NKPDT will be used as the basis for making prediction or estimation of possible future cyberattacks.

3. Results and discussion

3.1. Predicting the cyberattack using cognitive artificial intelligence

Proactive defense is an activity to do deterrence action to future possible attacks before they are really materialized. In defense or military terminology it is said as pre-emptive strike to deny the adversary's intention to perform attacks. As like pre-emptive strike, proactive defense needs comprehensive information as the basis for creating a plan. Such information has to be obtained through prediction or estimation regarding what the adversary will be trying to do with all resources it has. For the case we are raising in this paper, such information can be what kind of attack categories which will be the most possible one to enter the protected or defended system, and when the most possible time the attacks will occur. As the nature of KGS-based CAI which will use new data as the basis for obtaining knowledge which will be translated as the prediction or estimation.

CAI system will use the latest data as shown in Table 8 to make prediction or estimation of what and when future possible attacks would occur. Because the system has not interacted with the environment, therefore we had to create such environment by making simulated data based on the data in Table 8 for *n* times in the future. The simulated data are random integer numbers which were created by using a random generator tool provided by random.org web site [15]. Because each attack category is specific, therefore each one will be equipped with its own simulated data. For generating random numbers, we made assumptions to obtain the lower and higher bounds for each attack category. The lower bound is set to be 0.5*the_attack_number_of_event, while the high bound or the maximal one is set to be 1.5*the_attack_number_of_event.

As an example, the number of event of Analysis is 2,677. Then its lower bound is 1,339 and its higher one is 4,061. The random numbers obtained for the next 10 times of interaction time are 3,664, 2,458, 1,913, 3,895, 2,851, 3,815, 1,435, 1,398, 3,784, and 3,213. Other categories will have their own lower and higher bounds as well as their randomized numbers as shown in Table 2. The data in such table is assumed as the number of events of all attack categories after observed by the system for 10 interaction times. We can do simulation with more interaction times, but we think that 10 times should be enough to show the performance of our proposed method. The next step is to convert the number of events of each category into inputs which are recognized by the system, that is binary ones. The convertion is done by using threshold value which is different for each category. To obtain a fair data convertion, we use average value of each category as the threshold values. The converted data is shown in table 2 dan table 3.

Table 2. Number of events for all attack categories after 10 observation times.

Attack Category/Time	**t+1**	**t+2**	**t+3**	**t+4**	**t+5**	**t+6**	**t+7**	**t+8**	**t+9**	**t+10**
Analysis	3,664	2,458	1,913	3,895	2,851	3,815	1,435	1,398	3,784	3,213
Backdoor	2,603	2,438	2,149	2,058	3,040	2,832	2,802	2,780	2,334	2,694
DoS	15,932	10,823	14,316	10,355	21,019	21,791	15,241	20,285	10,224	19,473
Exploit	28,674	42,487	50,880	42,946	28,622	54,099	31,638	55,161	29,398	23,363
Fuzzer	14,009	34,807	14,072	14,143	15,588	21,198	19,803	35,607	18,358	32,717
Generic	214,776	182,342	123,537	138,120	136,080	230,496	157,090	315,967	222,522	161,058
Reconnaissance	7,323	10,642	16,271	15,964	14,862	15,267	19,452	20,379	7,136	7,287
ShellCode	1,348	1,658	2,038	1,367	1,119	1,279	1,850	907	1,802	1,177
Worm	101	127	209	179	205	139	92	147	100	213

Table 3. Data inputs to CAI-based system for predicting the possible time of attacks.

Attack Category/ Time	**t+1**	**t+2**	**t+3**	**t+4**	**t+5**	**t+6**	**t+7**	**t+8**	**t+9**	**t+10**
Analysis	1	0	0	1	1	1	0	0	1	1
Backdoor	1	0	0	0	1	1	1	1	0	1
DoS	0	0	0	0	1	1	0	1	0	1
Exploit	0	1	1	1	0	1	0	1	0	0
Fuzzer	0	1	0	0	0	0	0	1	0	1
Generic	1	0	0	0	0	1	0	1	1	0
Reconnaissance	0	0	1	1	1	1	1	1	0	0
ShellCode	0	1	1	0	0	0	1	0	1	0
Worm	0	0	1	1	1	0	0	0	0	1
NKPD	**0.065**	**0.087**	**0.096**	**0.087**	**0.111**	**0.133**	**0.065**	**0.152**	**0.074**	**0.13**

Table 4. Data inputs to CAI-based system for predicting the possible attacks in 10 times.

Attack Category/ Time	Analysis	Back-door	DoS	Exploit	Fuzzer	Generic	Recon-naissance	Shell-Code	Worms
t+1	0	0	0	1	0	1	0	0	0
t+2	0	0	0	1	1	1	0	0	0
t+3	0	0	0	1	0	1	0	0	0
t+4	0	0	0	1	0	1	0	0	0
t+5	0	0	0	1	0	1	0	0	0
t+6	0	0	0	1	0	1	0	0	0
t+7	0	0	0	1	0	1	0	0	0
t+8	0	0	0	1	1	1	0	0	0
t+9	0	0	0	1	0	1	0	0	0
t+10	0	0	0	0	1	1	0	0	0
NKPD	**0**	**0**	**0**	**0.417**	**0.117**	**0.467**	**0**	**0**	**0**

3.2. Discussion

Based on the computation results in form of NKPDs as shown in table 10 dan table 11, it can be obtained two kinds of graphics as depicted below. Figure 1 shows the dynamics of attack for each category of attack from 10 observation times, and Figure 2 shows the number of events for each category of attack from 10 observation times. As shown in Figure 1, the dynamics of each attack category is variative. At the same t_1, some attack categories have t similar behaviors while others do not. Meanwhile Figure 2 shows the collection of all number of events for all categories. The question is what knowledge can be obtained by the CAI system which can be used as the basis for making a plan for proactive defense.

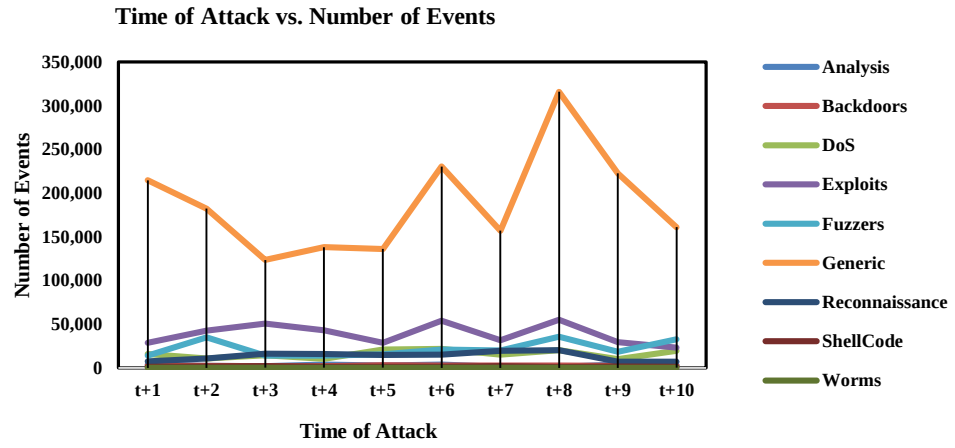

Figure 1. Dynamics of attack for each category of attack for 10 observation times.

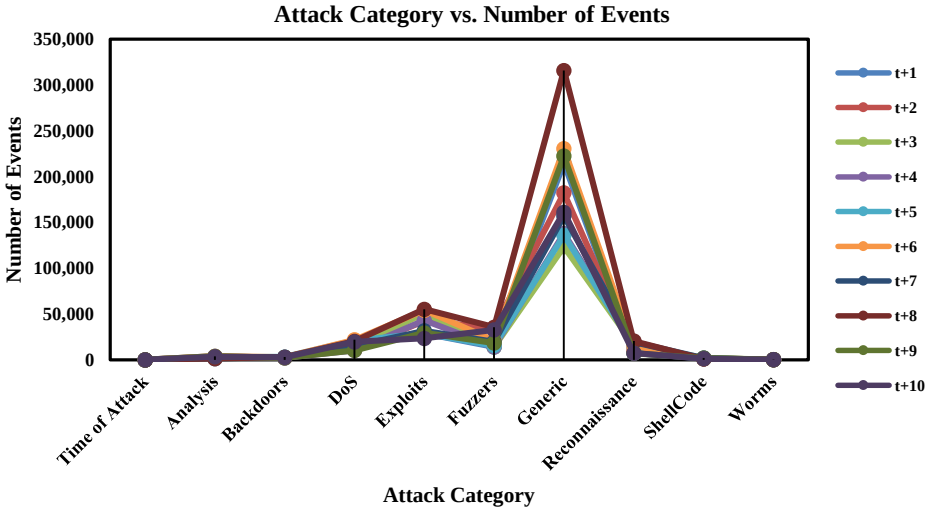

Figure 2. The number of events for each category of attack from 10 observation times.

The knowledge can be obtained from figure 1 is the most probable time of attack by all attack categories would be in its peak which may occur in a certain time *t* in the future. The attack would be done simultaneously which may deliver severe impact to the computer network or systems. As depicted in Figure 3, it can be seen the dynamics of cyberattacks from time to time. The attack would be in its lowest at t_7 and quickly toward its highest at the next *t*, that is t_8, then also quickly decrease at the next *t*. The DoC of the system that simultaneous cyberattack would be at its highest at the next t_{i*8} where i=1,...,n is shown obtained from (2) and (3) as follows. From the computation we obtain $P\left(\psi_1^j\right)_{estimate} = 0.152$ and $DoC = 15.2\%$. Meaning that the CAI system predicts that the most probable simultaneous attack at its highest would occur at time t_8 or its multiplication such as t_{16} and t_{24}. On the other hand, the network or system has to be hardened when approaching such certain times.

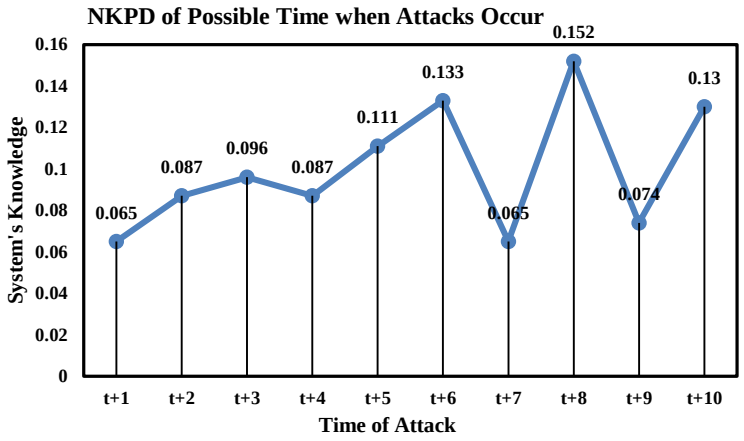

Figure 3. The CAI system's knowledge as the basis for proactive defense decision in term of time of a simultaneously attack.

$$P\left(\psi_1^j\right)_{estimate} = \odot\,[0.065,0.087,0.096,0.087,0111,0.133,0.065,0.152,0.074,0.13] = 0.152$$

$$DoC = \left|P\left(\theta_j\right)_{estimate} - \phi_1^j\right| \times 100\% = |0.152 - 0|x100\% = 15.2\%$$

From another perspective, the knowledge can be obtained from Figure 2 is the most probable attack category which would attack the computer network or system in the future. The knowledge obtain by CAI system is depicted in Figure 4. It can be seen that after 10 observation times, CAI system has a certainty that there would be three categories of attack which would become threats in the future that is, Exploit, Fuzzer, and Generic. By using the same formulas as above, the most probable attack with the highest probability is Generic where $P\left(\psi_1^j\right)_{estimate} = 0.467$ with $DoC = 46.7\%$.

The knowledge obtained by CAI system as depicted in Figure 3 and Figure 4 followed with the dicussion of the results, give us three kinds of prediction as follow.

- The most probable time when a simultaneously cyberattack as its highest, namely at time t_8 or its multiplication.
- The most probable attack category with the highest attack probability which would occur at anytime.
- Other attack categories with high probabilities which would attack the computer network or system at anytime besides the highest one.

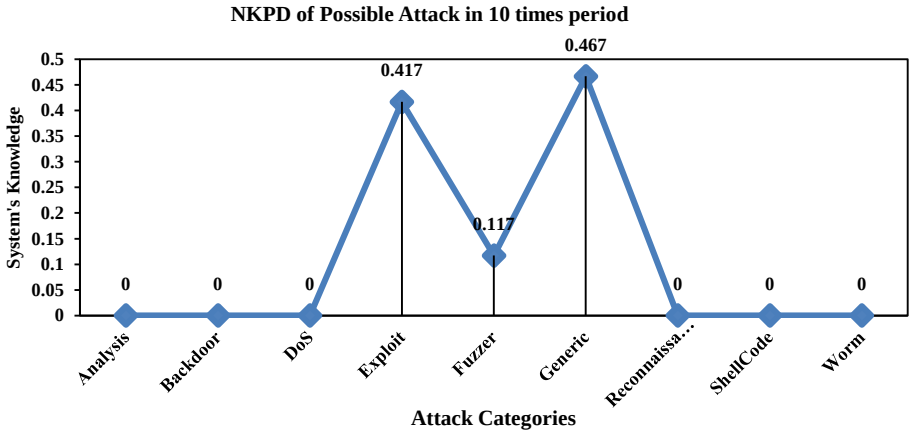

Figure 4. The CAI system's knowledge as the basis for proactive defense decision in term of attack category.

Based on these predictions, we can deliver some recommendations for proactive cyber defense such as follows.

- Hardening the computer network or system to anticipate the attacks from Exploit, Fuzzer, and Generic.
- Add more hardening mechanism especially to anticipate cyberattacks at time t_8 or its multiplication.
- Develop new approach for protecting the block ciphered-based systems, fix all vulnerable holes, and monitor any attempt of pen-testing by unlegitimated accesses.

4. Concluding remarks

We have presented the application of CAI-based system for predicting or estimating the occurences of cyberattacks in the future by using simulated random data based on UNSW-NB15 data. The CAI-based system with the knowledge it obtains after interacting with the phenomena for 10 observation times, is able to deliver three prediction or estimation namely, (1) the most probable time when a simultaneously cyberattacks would occur at its highest, (2) the most probable attack category with the highest probability to attack, and (3) the most dangerous attack category which would do attacks at anytime in the future. All these predictions or estimations can be used as the basis for delivering recommendations to all related actors and this mechanism is called as proactive cyber defense.

The prediction or estimation for the most probable attack category with the highest probability of attack in the future was easy to do because the number of events of such attack category is the highest among others. The prediction or estimation will be a challenge if the number of events of all attack categories are almost similar one to another. The distinguishing factor of CAI to other AI methods is CAI obtains knowledge by performing forward learning, namely learning by interaction.

Acknowledgment

The first author with humble would like to deliver his gratitude to the late Prof. Dr-ing. Ir. Adang Suwandi Ahmad, DEA, IPU (1948-2019) for his great idea in developing Cognitive Artificial Intelligence (CAI) at the first place. He was one of AI experts in the world and his contributions are invaluable in the field of AI.

References

[1] CapcoMedia 2018 *Active, Proactive or Reactive? Assessing Your Cyber Security Posture Capco* [Online] retrieved from https://www.capco.com/-/media/CapcoMedia/PDFs/cyber_security_posture_v4.ashx

[2] Okutan A, Werner G, Yang S J and McConky K 2018 Forecasting cyberattacks with incomplete, imbalanced, and insignificant data *Cybersecurity* **1**(15) 1-16
[3] Rege A, Obradovic Z, Asadi N, Parker E, Pandit R, Masceri N and Singer B 2018 predicting adversarial cyber intrusion stages using autoregressive neural networks *IEEE Intelligent System*
[4] Jaganathan V, Cherurveettil P and Sivashanmugam P M 2015 Using a prediction model to manage cyber security threats *The Scientific World Journal* 1-5
[5] PCmac *Malicious hardware* [Online] retrieved from https://www.pcmag.com/encyclopedia/term/59521/malicious-hardware
[6] Moustafa N and Slay J 2015 UNSW-NB15: a comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set) *in 2015 military communications and information systems conference (MilCIS) IEEE* 1-6
[7] Sumari A D W and Sutikno S 2019 Cyber-physical systems threats, risks, and vulnerabilities: the challenge to indonesia defense sector *Proc. of the 3rd Indonesia International Defense Science Seminar 2019 (Bogor)* 347-364
[8] Sumari A D W 2019 Cognitive artificial intelligence: a new perspective in artificial intelligence *Guest Lecturer Applied Master on Electrical Engineering Study Program, State Polytechnic of Malang Malang, March 20*
[9] Sumari A D W, Ahmad A S, Wuryandari A I, and Sembiring J 2010 Constructing brain-inspired knowledge-growing system: a review and a design concept *Proc. of the Second International Conference on Distributed Framework and Applications 2010 (Yogyakarta)* 95-102
[10] Sumari A D W, Ahmad A S, Wuryandari A I, and Sembiring J 2012 Brain-inspired knowledge growing-system: towards a true cognitive agent *International Journal of Computer Science & Artificial Intelligence* **2**(1) 26-36
[11] Sumari A D W, Ahmad A S, Wuryandari A I, Sembiring J, and Sahlan F 2010 An introduction to knowledge-growing system: a novel field in artificial intelligence *Jurnal Ilmiah Teknologi Informasi (JUTI)* **8**(2) 11-20
[12] Sumari A D W and Ahmad A S 2017 Knowledge-growing system: the origin of the cognitive artificial intelligence *Proc. of the 6th International Conference on Electrical Engineering and Informatics 2017 (Langkawi)* 1-7
[13] Sumari A D W and Ahmad A S 2019 Metode komputasi untuk sistem berpengetahuan tumbuh terinspirasi cara manusia berpikir *Patent Registration Number P00201202101 March 12*
[14] Sumari A D W and Ahmad A S 2017 Cognitive artificial intelligence: brain-inspired intelligent computation in artificial intelligence *Proc. of Computing Conference 2017 (London)* 135-141
[15] Random.org [Online] retrieved from https://www.random.org/