APT'sTTP: Deep Learning with Metaheuristics for Targeted Asset Prediction and Prioritization (TAPP) in Industrial Control System

Diana Arulkumar and K. Kartheeban

Abstract In cyberdomain, advanced persistent threat's tactics techniques and procedures (APT'sTTPs) are related to gain threats information. APT'sTTPs describe the threats behavior and pattern of attack in the adversary. Effective identification of APT'sTTPs in timely manner leads to construction of effective strategy for diagnosis of cyber threats actors (CTAs) in the form of attack vector. Through effective process, appropriate prevalence and regularities are evolved for APT'sTTPs for CTAs. However, the existing techniques focused on classification of attacks influenced by attackers alone but fails to examine the hackers target assets. To highlight the goal of this paper, to prioritize and predict the target assets in industrial control system (ICS) using deep learning integrated with metaheuristics ABC optimization method. For identification of TTP utilized in the industrial application, a brain-inspired model of deep neural network (DNN) approach has been used. Those TTP is evaluated for the collection of cyber assets process adopted in people, technology, and infrastructure (PPTI). The Deep Neural Network (DNN) once trains the 15 TTP helps to map and prioritize the inventory asset. For prioritizing an asset in the forum, a bio-inspired intelligence of metaheuristics ant bee colony (ABC) optimization approach has been adopted as ABC for targeted asset prediction and prioritization (ABCTAPP). Analysis of results illustrated that input capture (IC) and Service Certifying Organization (SCO) exhibit higher utilization of 93%. Further, hackers target host address and IP protocol in industrial applications.

Keywords Tactics techniques and procedures (TTPs) · Deep neural network (DNN) · Ant bee colony for targeted asset prediction and prioritization (ABCTAPP)

D. Arulkumar (✉) · K. Kartheeban
Kalasalingam Academy of Research and Education, Krishnankoil, Tamil Nadu, India

K. Kartheeban
e-mail: K.Kartheeban@klu.ac.in

S. Bhaumik et al. (eds.), *Proceedings of International Conference on Industrial Instrumentation and Control*, Lecture Notes in Electrical Engineering 815,
https://doi.org/10.1007/978-981-16-7011-4_36

1 Introduction

In recent years, cyberattack has been emerging at drastic pace. As per [1], in the year of 2017, average cyberattack cost is recorded as 153 million USD. The increased number of malware and sophistic, an enhancement in security of the network particularly cyberthreats related to CTAs is required. At these circumstances, information related to cyberthreat plays major role in indication of attack and vulnerabilities employed in the CTA at particular campaign. The major limitation related to present Cyber Telephony Integration (CTI) is limited sharing of information with respect to static- and heuristics based signature approach those are not able to defend any dynamic and complex nature of threats. Generally, this CTI is classified into four categories such as technical, strategic, operational, and tactical threat intelligence [2]. The strategic-based CTI is related to identification and analysis of risks associated with collected information for making decision for gathered information. The CTI belonging to operational has minimal vulnerabilities and attacks at zero day, dark web, or collection of hackers in closed forums. The CTI with tactical is related to CTAs and APT'sTTPs which involves CTA operand and training with integral part. The representation of APT'sTTPs based on the characteristics of CTA interacts with affected network and operating system. CTA offers substantial effort in the development of operational module by means of customized software tools for attack campaigns. Based on this, it is difficult for CTA to cope with changes in the APT'sTTPs due to minimal attack or new attack emerged in specified time [3]. Hence, it is necessary for the identification of attack in APT'sTTPs with incident of attack for prevention of loss in the organization. The recent prevalent incident of cyberattack and behavior of CTAs are extracted for establishment of relation between APT'sTTPs attack pattern [4].

The CTI employs several technical resource factors such as intrusion detection system and firewalls. Those indicators are the signatures involved in attack such as IP address, file hashes, Command and Control (C&C) domains, and viral signatures. The indicators are ineffective in the identification of cyberthreats which are involved in CTA modification each time for bypass firewalls and intrusion detection system [5, 6]. The tactical and strategic threat intelligence are considered as an effective tool and provides long-life time when compared with technical and operational threat intelligence. To evaluate the TTP process, machine learning has exhibited significant performance; hence, for evaluation of TTP process in CTI, neural network offers significant performance characteristics.

Even, burgeoning market is involved in sale of those stolen data and malicious threats specifically in the Eastern Europe and Russia. Researches on enculturation of subculture of hacker are involved in recognition of status of particular hacking community. Due to the usage of the Internet in almost all countries, hacking has been increased drastically. Throughout the world, mainstream political factor and social movements are based on dependent broadcast ideologies in the world. To overcome such hacking, several tactics have been applied for perceived injustices for secure access to people. Other countries such as Zapatistas, in Chiapas, and Mexico focused

on post-information quality [7]. Cyberattacks have been engaged in drastic range by Chinese hackers where sensitive information is obtained through resources of USA by means of network infrastructure. In April 2006, hackers of Russian and Estonian specifically during war data have been hacked [8–12].

In the Internet, user application involves several assets specifically for industrial applications. The application of attacks is involved in identification of different assets in the network [13]. Hence, it is necessary to identify the assets those are targeted by hackers. In this research, a deep learning approach integrated with metaheuristics approach is developed for the identification of APT'sTTPs and assets. The data for analysis are collected from several hacking forums for training the deep neural network. The focused domain is CTI document which is based on structured threat information expression standard (STIX). Through testing and training, APT'sTTPs are identified in the hacking forums. Results demonstrated that file and discovery of TTP have been highly performed by hackers. For evaluation, this research considers 15 APT'sTTPs. In analysis of assets, hackers focused on technological aspects particularly for hacking data.

This paper provides the metaheuristics-based approach for developed for target asset. The proposed metaheuristics focused on 15 target assets to predict the hackers target for targeted assets. This paper is organized as follows: Sect. 1 presented general description about cyberassets. In Sect. 2, existing works related to target assets are presented. Section 3 presented about materials adopted for target asset along with TTP regulatory framework. In Sect. 4, results obtained for proposed metaheuristics approach are presented. In Sect. 5. the overall conclusion obtained for proposed metaheuristics approach is stated.

2 Illustrations

The analysis of CTI focused on defense mechanism in proactive and reactive approach for analytics. The CTAs are based on the consideration of behavior, capability, and persona. With consideration of cyberdefense factor profiling involved in collection of personal data [14]. In real-time scenario, based on attributes, threats are estimated. To evaluate the performance of hacking community, CTAs are involved in utilization of several software tools and assets for campaigns hacking [15].

In hacking communities, data related to generic topic is target asset for hackers. Those collected data from social media are labeled with inclusion of several emerging tools such as crypters, vulnerabilities in database, Web, and keyloggers. Those tools are subjected to minimal vulnerabilities and exploits certain factors. Even this provides effective guidance for administration security through proactive defense mechanism. In order to identify the attack patterns, [16] is necessary to streamline the workflow memory and performing the Indicator of compromises (IoC's) analysis of generated attack pattern in each and every phases of attack chain using the machine learning algorithm. Analysis of malware is involved in provision of automated solution to evaluate interrelationship instances of malware [17]. Through the review of

existing literature review, several domains are evaluated for measuring significance of tactics involved in CTI. Hence, this research focuses on several TTPs involved in regularities of attack in the system at right time. The analysis of existing literature stated that target assets are evaluated in terms of detecting attack. However, the existing techniques are focused on classification of attacks influenced by attackers alone but fails to examine the hackers target assets,

The APT'sTTPs for CTA's involved in formulation certain regularities. The framework comprises of feature selector, ARM miner modules, and feature extractor in which feature selector is used for encoding CTI document using STIX. The selected CTI document subjected to cyberthreat is considered in this research [18]. The collected CTI document contains unique attribute ID in elements of STIX. In elements of STIX, TTP is represented where similar to CTI, TTP also has unique IDs. Each and every TTP provides description about sub-elements of TTP features. For the selected CTI document using feature extractor module, TTP's information is gathered. This extraction is performed through CTI document unique reference and database information storage. The feature extracted is applied into module of feature selector for identification of most effective APT'sTTPs. To represent effective CTA terms, several approaches are implemented by means of deep learning approach for attack identification.

At present, deep neural network has been employed in due to evolution of artificial neural network. It facilitates training of network with tens and millions [19–21] or even billion parameters [22]. To withstand against cyberthreats, details from hacking forums are implemented by means of training and testing large amount of data for processing. In hacking community, minimal research has been conducted to drive hacker community. According to Honeynet projects, hacker community has six targets identified, namely money, entertainment, ego, cause, entrance to a social group, and status [23]. The above-mentioned factors are the major aim of hackers to steal particular data.

Even though deep neural network is similar to neural network, it is hard to train which requires appropriate number of data for processing. The major advantage of deep neural 'network is it provides information to the human for possible prediction of attack in the network. The common process of DNN model involved in data ingesting from the different data sources which offers artifacts sequence for probabilistic ML model using pre-trained performance. Every model perform training using application of various procedure to identify artifacts through pre-existing and labelled sequence data. The output derived from this model is using probabilities model with application of set of procedure fed by other trained ML models [24].

Through the collected data from the hacking forums, data are classified for testing and training. For collected TTP data, with assigned variables, training is adopted in deep network using cognitive agent. The network cognitive agent gains prior knowledge about previous observed attack models and assets inventory [25]. The cognitive agent determination of extent to which sequence of methods adopted by ML models with indication of attack compromised for provided asset. In case, attack within the cognitive agent is observed as ongoing, it will be able to identify human

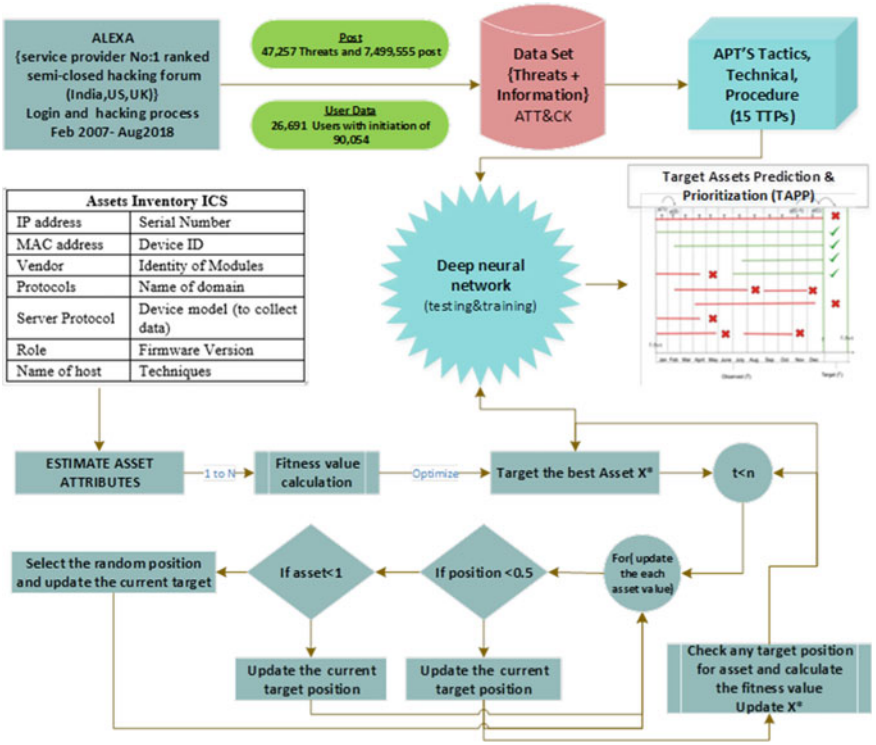

Fig. 1 Architecture of target asset prediction and prioritization (TAPP)

controller. Those are identified from the rank list involved in probable operation for prediction of objective [26].

3 Proposed System

3.1 Target Asset Prediction and Prioritization (TAPP) Architecture

Comparative analysis of the proposed scheme with existing technique observed that Samtani et al. [2] collected data from various online hacker forum such as OpenSc, Reverse 4you, and ExploitIN. It is observed that hacker details are sufficient trends related to reliable and credible for mislead defending community. Brynielsson et al. [1] examined the collected data related to cyberdefense exercises. The main purpose of this function is participants train with defend skill for the constructed network and organization of cyberwarfare. According to [1] the data from those sources

are credible and reliable are out of scope exercises are limited which cannot be full-fledged campaign for CTA. Another researcher, M. Lee and D. Lewis., [11] examined the data related to Symantec Anti-Virus (AV) and Intrusion Prevention System (IPS) corpus for tactical CTI in terms of authentic and reliable for attack processing. The comparative analysis of results expressed that proposed analysis technique offers proactive and reactive defense strategy for recent CTA tactics (Fig. 1).

Data collection

To evaluate the TTP assets in industrial application, deep learning with metaheuristic approach is applied. For analysis, data were collected from hacking forum. According to Alexa, the service provider is involved in management of Web traffic; hence, those forums are ranked as No. 1 which is considered as subcategory hacking forum. Based on analysis, Alexa is relied on Indian Web site forum those includes various hackers in India at the rate of 16.7%, USA 21%, and UK 9.1% for various countries. However, specific hacker forum is represented as hacker forum with inclusion of semi-closed forum which is used for login forum process. The setting of forum is similar to that of other forums where threats are discussed and organized. In those formats, user post-initiates threat is referred as header. With respect to post of header, comments of other user post with several threads are included in replies. On the other hand, post of header needs to be discussed as thread and provides vast range of replies. In this paper, to evaluate the target assets, online hacker forum is utilized for assessment, hackers are not provided with intention of users based on the information forum except same interest share mechanism. During data analysis, the users are selected based on the noticeable active performance in terms of posting in the forum.

The forum data for analysis are collected from February 2007 to August 2018. The downloaded forum data consist of wide range of posting related to hacking process. Specifically, the type of information was considered in the dataset [27–30].

Post-centric data: The data of each post consist of header or replies which includes post ID, post title, post category, post content, and post author. **User-centric data**: The data registered forum is utilized for user reputation, and this includes user ID, date, user level, and user name.

The final downloaded dataset consists of information related to 26,691 users with initiation of 90,054. Also, the downloaded threads consist of 47,257 threats and 749, 9555 posts. In Table 1, the details of collected forum are presented as follows:

APT'sTTP

For analysis, 15 TTP's are identified through hacking forums and presented about description. The selected APT'sTTPs are fed into deep learning technique through process of testing and training. The prediction of operation leads to inclusion of adversary techniques, and potential measures are utilized for prediction of objective and future technique. The human controller acts as information provided to offer information about cognitive agent through utilization of deep learning. For deep learning process, selected feature sets are larger and need to identify associations

Table 1 Forum details

Forum attributes	Registered time length for days	32
	Number contributes in unique factor for a month	1736
	Monthly user retention	781.7
	Post count for individual thread	8.33
	Unique number for each individual thread	5.46
Communication behaviors	Message generated for particular user	7.7
	Word count utilized for individual message	33.35
	Number of threats for individual contributor	1.91
	User replies for data	13.97
	Density of data discussed	22.62

Table 2 TTP and its description

TTP	Description
Credential dumping (CD)	Credential is extracted from the system
File deletion (FD)	Removal of pf malicious content with elimination of attack traces
Data compression (DC)	Before the process of exfiltration, collected system information are compressed
Scheduled task (ST)	For execution of malicious content, OS task is scheduled
Valid accounts (VA)	Within the system, credentials of valid users are compromised
Windows management instrumentation (WMI)	Access to the system is obtained either locally or remotely
Windows admin shares (WAS)	Access information of hidden network is shared with admin for accessing machine victims in the network
Obfuscated files (OF)	Detection of malicious content based on unintelligible mechanism for encoding or encryption
File and directory discovery (FDD)	Extraction of system credentials either from network share or from host
PsExec	Extraction of system credentials
Registry run keys (RRK)	Addition of malicious content from the entry to the registry, it executes user logs in
Remote file copy (RFC)	Files are copied to remote machine
Input capture (IC)	User inputs are captured
PoisonIvy	Remote access tool for DLL load with inclusion of keylogger
System user discovery (SUD)	Identification of principal user of the victim machine

Table 3 Asset inventory

Assets in industrial	Control system
IP address	Serial number
MAC address	Device ID
Vendor	Identity of modules
Protocols	Name of domain
Server protocol	Device model (to collect data)
Role	Firmware version
Name of host	Techniques

among them. In the following Table 2, describes about TTP's for APT which is used for prioritize the assets in our research.

Asset Inventory

Data related to industrial control system have been evaluated for schematic illustration of the assets. Hacking forums are involved in prediction of assets for prioritizing the assets. Through the optimization approach, assets are scheduled which helps in reducing the attack in the network [31]. This research considers 14 assets for evaluating the priority of the network. The assets considered are listed in Table 3

Metaheuristics of ABCTAPP

This paper utilized industrial data for target asset focused by the hackers; for analysis, data were collected from Alexa. The collected dataset from Alexa was processed as follows using ABC meta-heuristics algorithm. Initially, ABC optimization algorithm involved in construction of elements for randomly identify the position within the boundary range of asset values. The dataset elements with attribute 1 are selected from processing else it will be eliminated. The selection of elements is stated in Eq. (3).

$$x_m = l_i + \text{rand}(0, 1) * (u_i - l_i) \tag{1}$$

In the above equation, food source is stated as x_m, which means assets. The parameters u_i and l_i provide the upper- and lower-level solution space. rand(0,1) represents random number value of range [0,1]. The targeted assets by the attacker are identified through consideration of target solution which is represented in Eq. (4):

$$v_{mi} = x_{mi} + \phi_{mi}(x_{mi} - x_{ki}) \tag{2}$$

The parameter I represents randomly selected index, randomly selected attributes are denoted as x_{ki}, and parameter φ_{mi} denotes randomly selected integer value of [−1, 1]. The parameter v_{mi} provides estimated asset value using fitness evaluation in Eq. (5) as follows:

$$fit_i = \begin{cases} \frac{1}{f_i+1} & f_i > 0 \\ 1 + |f_i| & f_i <= 0 \end{cases} \tag{3}$$

In the above Eq. (5), the asset objective equation is estimated using f_i which provides optimal value for targeted asset by the hacker. Through estimation of individual asset, values targeted by hackers are estimated using probability of asset selection using Eq. (6):

$$p_i = \frac{\text{fit}_i}{\sum_{n=1}^{N} \text{fit}_i} \tag{4}$$

The value N denotes total assets targeted by the hackers. fit_i provides the optimal value for identification of asset targeted by the hackers. The ABC algorithm for identification of target asset prediction and prioritization (TAPP) in hacking forum is presented below:

Algorithm 1: ABC for Target Asset Prediction and Prioritization (ABCTAPP)

```
Initialize the asset attributes estimation Xi (i = 1, 2, ..., n)
Calculate the fitness of each asset target
X*=the best asset target
while (t < maximum number of iterations)
 for each asset target
   Update a, A, C, l, and p
   if1 (p<0.5)
    if2 (|A| < 1)
      Update the position of the current asset target
    else if2 (|A|=>1)
     Select a random asset target (Xrand)
      Update the position of the current asset target
    end if2
   else if1 (p> 0.5)
     Update the position of the current asset target
   end if1
 end for
   Check if any asset target goes beyond the asset target    space and adjust it
   Calculate the fitness of each asset target
   Update X* if there is a better solution
t=t+1
end while
return X*
```

Deep Learning—Deep Neural Network (DNN)

For Fig. 2, let us consider number of samples or assets as: $D = \{(X_i, Y_i)\}N$ where $N = 1$. The collected data from the Web sites are represented as X_i for the time period $[\Gamma - T + 1, \Gamma]$ with length of T. The prediction of assets for hackers is denoted as $Y_i \in Y = \{0, 1\}$; the targeted assets for window are shown as of length τ.

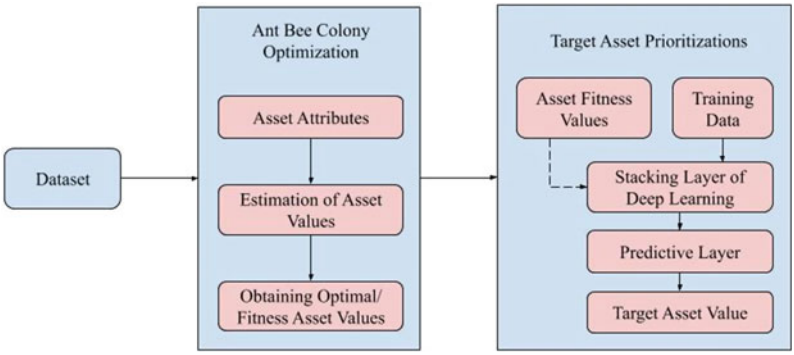

Fig. 2 ABCTAPP

$X_i[\Gamma - T + 1, \Gamma]$ For user data, X_i and $[\Gamma + 1, \Gamma + \tau]$ involves three heterogeneous primitive sub-components based on granularity of observed data as X_{ia}, dynamic user information X_{id}, and static user profiles X_{is}, namely, and it is given in Eq. (5) as follows (Fig. 3) [31]:

$$X_i = (X_{ia}, X_{id}, X_{is}) \in X \tag{5}$$

For evaluation of log components applied in target window is shown as time _x0010_span T right in which dynamic information is denoted in Eq. (6):

$$X_{id} = X(\Gamma - T + 1)_{id}, X(\Gamma - T + 2)_{id}, \ldots, X(\Gamma - 1)_{id}, X(\Gamma)_{id} \tag{6}$$

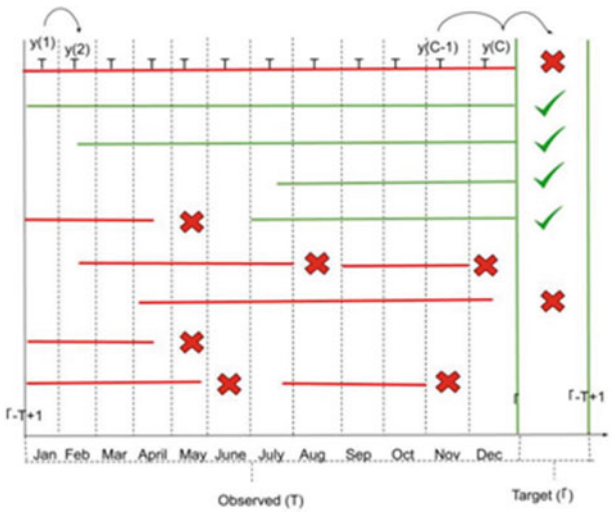

Fig. 3 Schematic overview of assets

The deep learning approach utilizes mapping rule for attribute for estimation of feature space attributes, which is represented as $R(\cdot)$: $X \rightarrow Y$ and subsequently $R(\cdot)$ involved in estimation of future sample. The probability of sample i in attrition can be denoted as $p(y_i = 1|X)$.

4 Experimental Analysis and Results

The metrics considered for comparison are data sources, CTI type, data features, defense strategy, and outcome. The data sources metric is represented as data source collected for analysis. This data source metric is involved in authentication and credibility of analysis process. For future comparisons, ground truth is provided for data sources baseline. As stated earlier, this research utilizes ATT and CK dataset for processing [16]. The extracted ATP'sTTP list from ATT&CK is performed in each phases of intrusion Cyber Kill chain which connects CTA's and utilize appropriate software for processing. In Fig. 4, TTP in the industrial application is presented which is targeted by attackers. Through analysis of proactive and reactive defense strategy, it is observed that IC and SUD exhibit higher utilization in TTP asset by hackers at the rate of 93%. The DC offers TTP % values of 92%, failed directory deletion (FDD) provides TTP utilization rate of 90%, VA provides TTP value of 83%, WAS, WMI provides 73% and 70%, respectively. The parameter CD exhibits TTP of 78% and FD provides TTP of 85% (Tables 4 and 5).

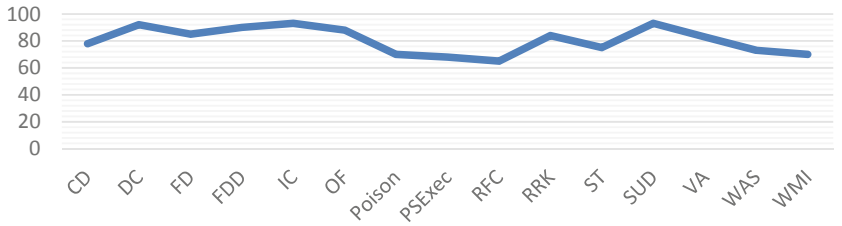

Fig. 4 APT'sTTP utilization in each phases of intrusion chain

Table 4 Data sources with hacker's forum

Data sources	Hacking forum, dataset, benchmark dataset
CTI type	Operational, tactical, technical, and strategic
Defense strategy	Proactive, reactive
Data features	Source code, attachments, tutorials, and emails
Outcome	Topic labels, language of implementation

Table 5 Applying the ABCTAPP with DNN to calculate target asset value

	CD	DC	FD	FDD	IC	OF	Poison	PSExec	RFC	RRK	ST	SUD	VA	WAS	WMI
IP address	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00
MAC address	0.98	0.99	0.90	0.90	0.99	0.90	0.78	0.90	0.90	0.90	0.90	0.98	0.90	0.78	0.90
Vendor	0.78	0.97	0.98	0.77	0.95	0.70	0.50	0.70	0.75	0.70	0.70	0.98	0.70	0.70	0.70
Protocols	0.84	0.98	0.99	0.90	0.98	0.90	0.65	0.60	0.64	0.90	0.75	0.99	0.90	0.90	0.90
Server protocol	0.77	0.98	0.86	0.93	0.98	0.99	0.10	0.15	0.13	0.75	0.45	0.98	0.65	0.54	0.87
Role	0.71	0.87	0.83	0.98	0.95	0.90	0.88	0.90	0.83	0.95	0.89	0.99	0.89	0.90	0.85
Name of host	0.65	0.83	0.80	0.81	0.87	0.84	0.65	0.89	0.61	0.78	0.68	0.98	0.97	0.72	0.65
Serial number	0.56	0.95	0.96	0.98	0.97	0.88	0.69	0.73	0.69	0.96	0.42	0.99	0.65	0.60	0.62
Device ID	0.70	0.99	0.98	0.98	0.97	0.99	0.89	0.87	0.77	0.98	0.98	0.97	0.96	0.62	0.54
Identity of modules	0.42	0.80	0.68	0.79	0.77	0.70	0.74	0.80	0.78	0.63	0.77	0.65	0.75	0.30	0.40
Name of domain	0.35	0.95	0.94	0.99	0.98	0.96	0.99	0.98	0.98	0.97	0.97	0.98	0.95	0.98	0.58
Device model (to collect biometric data)	0.70	0.30	0.56	0.87	0.58	0.78	0.45	0.55	0.69	0.60	0.65	0.72	0.70	0.65	0.54
Firmware Version	0.28	0.88	0.76	0.85	0.88	0.87	0.79	0.74	0.73	0.79	0.75	0.90	0.87	0.74	0.54
Techniques	0.15	0.97	0.72	0.87	0.62	0.95	0.75	0.79	0.84	0.85	0.64	0.78	0.73	0.84	0.76

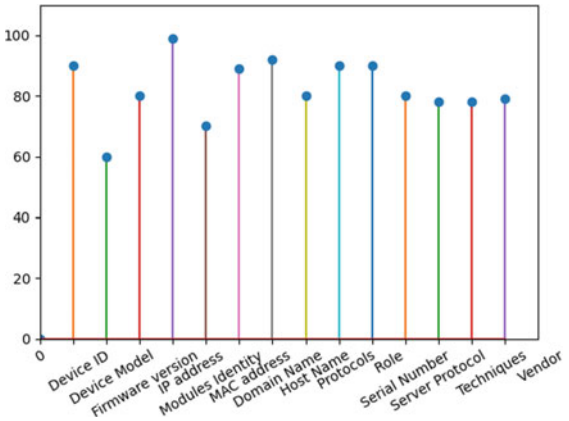

Fig. 5 Target asset prediction and prioritization

Table 4 portraits that the data can be collected from various sources such as cyber defense exercises [1], online hacker forum such as OpenSc, Reverse 4you and ExploitIN [2], Symantec Anti-Virus (AV) and Intrusion Prevention System (IPS) corpus [16]. The comparative analysis with existing technique is observed that Brynielsson et al., [1] said the function is to train participants with defend skill for the constructed network and organization of cyber warfare. Samtani et al., [2] that hacker details are sufficient trends related to reliable and credible for mislead defending community. Another researcher, M. Lee and D. Lewis., [16] examined for tactical CTI in terms of authentic and reliable for attack processing. The proposed analysis technique of combined model of deep neural networks and ABCTAPP. Table 5 offers proactive and reactive defense strategy for recent CTA tactics. Through analysis of proactive and reactive defense strategy, it is observed that IC and SUD exhibit higher utilization in TTP by hackers at the rate of 93%. The DC offers TTP % values of 92%, failed directory deletion (FDD) provides TTP utilization rate of 90%, VA provides TTP value of 83%, WAS, WMI provides 73% and 70%, respectively. The parameter CD exhibits TTP of 78%, and FD provides TTP of 85% .The asset prioritization is presented in Fig. 5; with asset prioritization, the collected dataset consists of 667 users with exhibition of similar pattern in casual hacker forum. From analysis, it is observed that behavioral pattern decreases with knowledge provision. The examination of assets stated that IP address, protocol, and role number are identified assets by the attackers. In secondary stage, serial number and name of host are targeted. From the graphical representation of calculated value of ABC TAPP wit9n front are targeted highly by the attackers (Fig. 6).

5 Conclusion

The TTPs represent the behavior of a CTA when interacting with the victims' resources such as operating system and network. This research adopted deep learning

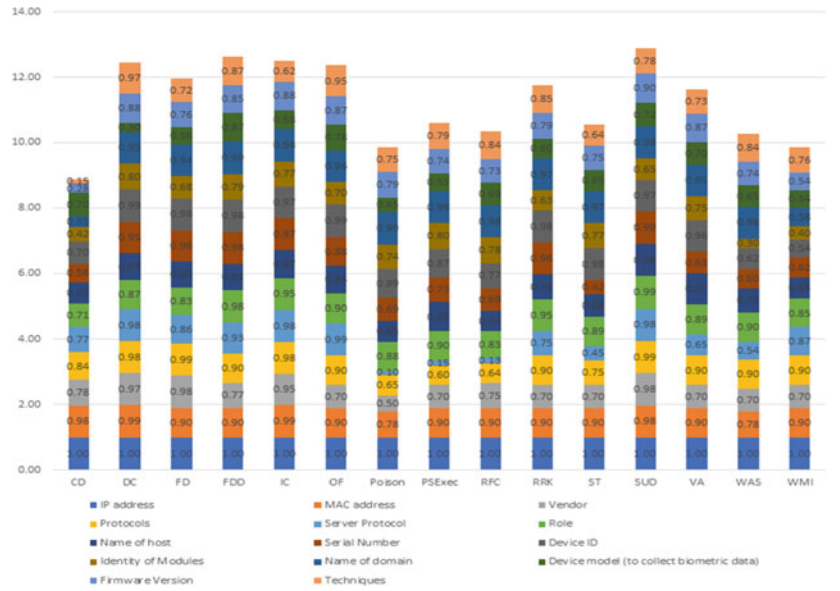

Fig. 6 ABCTAPP with DNN to calculate target asset value

method for identification of number of TTP used in hacking forum. Through the application of deep neural network, target asset and multiple target asset have been evaluated. The collected cyberassets are process adopted, people and technology, and infrastructure (PPTI). The assets are prioritized with the help of DNN by training 15 TTP and inventory asset processed with ABC algorithm. Simulation analysis stated that IC and SCO are highly utilized assets for hacking forum. Further, hackers use protocol, host address, and IP address as targeted assets in the network. In the future, this research can be implemented in other wireless communication system such as WSN and IoT for attack identification.

References

1. Brynielsson, J., Franke, U., Tariq, M.A., Varga, S.: Using cyber defense exercises to obtain additional data for attacker profiling. In: IEEE Conference on Intelligence and Security Informatics (ISI) (2016)
2. Samtani, S., Chinn, R., Chen, H., Nunamaker, J.F.: Exploring emerging hacker assets and key hackers for proactive cyber threat intelligence. J. Manage. Inf. Syst. **34**(4) (2017)
3. Agrafiotis, I., Nurse, J.R., Buckley, O., Legg, P., Creese, S., Goldsmith, M.: Identifying attack patterns for insider threat detection. Comput. Fraud Secur. **7** (2015)
4. Miles, C., Lakhotia, A., LeDoux, C., Newsom, A., Notani, V.: Virusbattle: state-of-the-art malware analysis for better cyber threat intelligence. In: 7th International Symposium on Resilient Control Systems (ISRCS) (2014)

5. Franklin, D., Ransomware, P.: Available https://exchange.xforce.ibmcloud.com/collection/PetyaRansomware024ee880d86e353ef307155cfe936c5a. Accessed 28 Jan 2018
6. Han, J., Pei, J., Yin, Y.: Mining frequent patterns without candidate generation. ACM Sigmod Rec. (2000)
7. Simonite, T.: Chinese Hacking Team Caught Taking Over Decoy Water Plant (2013)
8. Daly, M.K.: The advanced persistent threat (or informationized force operations). In: 23rd Large Installation System Administration Conference (LISA) (2009)
9. Risk Based Security: A breakdown and analysis of the December 2014 Sony hack. Risk Based Secur. (2014)
10. O'Gorman, G., McDonald, G.: The Elderwood Project (2012)
11. Lee, M., Lewis, D.: Clustering disparate attacks: mapping the activities of the advanced persistent threat. In: Virus Bulletin Conference (2011)
12. Jiang, G., Caselden, D., Winters, R.: The EPS awakens. FireEye Threat Res. (2015)
13. Symantec Security Response: Hydraq—An Attack of Mythical Proportions. Symantec (2010)
14. Winters, R.: The EPS awakens—part 2. FireEye Threat Intell. (2015)
15. Selvaraj, K.: Hydraq (Aurora) Attackers Back? Symantec (2010)
16. Mandiant: APT1—Exposing One of China's Cyber Espionage Units (2013)
17. Hoglund, G.: Inside an APT Covert Communications Channel. Fast Horizon (2011)
18. Alperovitch, D.: Cyber Deterrence in Action? A Story of One Long HURRICANE PANDA Campaign. Crowdstrike (2015)
19. Kumar, B.S., Rukmani, K.: Implementation of web usage mining using apriori and fp growth algorithms. Int. J. Adv. Netw. Appl. **1**(6) (2010)
20. Győrödi, C., Győrödi, R., Holban, S.: A comparative study of association rules mining algorithms. In: Hungarian Joint Symposium on Applied Computational Intelligence (2004)
21. Bonchi, F., Goethals, B.: Fp-bonsai: the art of growing and pruning small fp-trees. In: Pacific-Asia Conference on Knowledge Discovery and Data Mining (2004)
22. Agrawal, R., Srikant, R.: Fast algorithms for mining association rules. In: 20th Proceedings of International Conference of Very Large Data bases (VLDB), pp. 487–4991(1994)
23. Krebs, B.: Anthem breach may have started in April 2014. Krebs Secur. (2015)
24. Yates, M., Scott, M., Levene, B., Miller-Osborn, J., Keigher, T.: Operation Ke3chang Resurfaces with New TidePool Malware. PaloAlto (2016)
25. Monnappa: 2nd Meetup—Reversing and Decrypting the Communications of APT malware. CYSINFO (2016)
26. Ducklin, P.: The Sandworm Malware—What You Need to Know. Sophos (2014)
27. Coogan, P.: Targeted Attacks Make WinHelp Files Not So Helpful. Symantec (2012)
28. Chang, Z., Lu, K., Luo, A., Pernet, C., Yaneza, J.: Operation Iron Tiger: Exploring Chinese CyberEspionage Attacks on United States Defense Contractors (2015)
29. Chen, X., Scott, M., Caselden, D.: New zero-day exploit targeting internet explorer versions 9 through 11 identified in targeted attacks. FireEye (2014)
30. Schworer, A., Liburdi, J.: Storm chasing: hunting hurricane panda. Crowdstrike (2015)
31. Kharouni, L., Hacquebord, F., Huq, N., Gogolinski, J., Mercês, F., Remorin, A., Otis, D.: Operation Pawn Storm Using Decoys to Evade Detection (2014)
32. Crowdstrike Global Intelligence Team: Use of Fancy BearAndroid Malware in Tracking of Ukrainian Field Artillery Unit (2016)
33. Raiu, C., Soumenkov, I., Baumgartner, K., Kamluk, V., G. R. A. A. Team: The MiniDuke Mystery: PDF 0-day Government Spy Assembler 0x29A Micro Backdoor (2013)