A Threat-Hunting of UNSW-NB15 with Machine Learning Techniques to Achieve Resilience

Diana Arulkumar, Kartheeban.K.

Abstract : In order to focus on the mission and functions of the business of the organizations, cyber resiliency have to play a critical role against the adversaries' target. The strategy recommended by NIST to reduce the suspect ability of cyber-attacks of the system with the three dimensions such as harden the target, limit the damage to the target and make the target resilient. The threats could be based on cyber and noncyber. The objective is to provide cyber resiliency on the Advanced Persistent Threat (APT), has born with the nature of sophisticated, stealthy, persistent towards target and highly adoptable to the environment. The challenge is to provide cyber resilience to the system from compromising tactics of the adversaries, uncertain in eradication of threat due to its persistent nature, recognizing its adapting ability. The cyber resiliency also links with other disciplines like safety, fault tolerance, privacy, resilience and survivability, reliability and security.

Key words: Advanced Persistent Threat (APT , Cyber-attacks, Cyber resiliency,), UNSW-NB15

I. INTRODUCTION

The Digitizing operations interprets the services to be advanced level and sophisticated work experiences. All the operations should ensure that provides confidentiality, integrity and availability of its services within the organization is secure. In order to enforce the standards of cyber security in digitizing the operation, since the cyber security has the impedance to the business continuity of the organization in a dynamic changing environment. The possibility to provide the solution is based on the severity of the threats and vulnerability by framing the policies, procedures and tools, should be responded for the cyber-attacks at that instant. If the breach has launched by the adversary in a not prepared environment, the risks results loss of the customers trust [1]. Generally cyber threats for over a time change its feature in affect the various cyber functional capabilities (like DDos, data theft, modification of code, infecting, injecting). It targets from individual to corporate and government organizations. At the individual, Sensitive the information like personal, credit card, identity card to disrupt the millions of people's life through the fraudulent activities. At the corporate level, hackers try to steal the information stored in the database of the organization and impact the users and fame of the organization. Also another one , which is the state based , sophisticated cyber threats thwarted for security, financial losses, social /political gain by an individual hackers or the group. Cyber security is to secure the cyberspace and user assets by framing the policies and guidelines, with emerging technologies and security approaches. There are many threats that has been launched by the adversaries to steal information from the organizations through their available technologies. One among method of sending the threats is Advanced Persistent Threat (APT) is used without the knowledge of the user, it will stay persistently for long time and resist the defender's system monitoring act as passive. The focus of APT is to target Individual, corporate and government organizations in the motive of political, financial gain and also out of curiosity. Due to the advancement of technologies available to use in hacking techniques, the conventional security mechanism fails due to its loophole of vulnerability nature of software or hardware. The information security which couldn't cover the border of cyber security. In order t provide security for emerging technologies is huge challenge. To gain the knowledge about the identification of APT threats with other threats in network traffic, detect the instances and to tracking the flow of such threats, to take effective measures in controlling such events and also to ensure by managing the network proactively is very important. Software's are protected by patching to update and to fix its errors. In web development, it is essential to check whether the developed code is prone to cookies poisoning, buffer overflow, cross site scripting etc. once it is hosted in the internet as website, ensure a strong cryptographic algorithm is applied to secure the transactions of the website users. The security policies are frame to audit the activity of the network and also penetration testing. The security can be breached for Fake Authentication (proof of identities) Non-Integrity(intact), Non repudiation (not refute the claim of message), Access control(privacy) (who should be able to access what), Availability (states the resource available to authorized). The security is architect between adversarial and defender team.

Manuscript published on 30 December 2019.
***** Correspondence Author (s)

Diana Arulkumar*, Computer science, Karunya Institute of Technology and science, Coimbatore, India. Email: dianacse@karunya.edu
Kartheeban.k, Computer science, Kalasalingam Academy of Research and Education , Srivilliputtur ,India. Email:k.kartheeban@klu.ac.in

Retrieval Number: A11101291S419/2019©BEIESP
DOI:10.35940/ijeat.A1110.1291S419
Journal Website: www.ijeat.org

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)
© Copyright: All rights reserved.

The role of the defender team (red-team) is to secure the asset ensure the network performance of their security policies of monitoring, testing, adapt to changes and secure to sequence one another as a security wheel for the network. Another team called adversarial team which launches attack by reconnaissance, escalating privileges and establishing the backdoors against the asset of an organization as target. The goal is to evaluate attack paths and strategies of hidden network penetration actions for complete red-teaming and determine the dynamic cyber defense.

Application of Cyber resilience are Digital workplace, Smart surveillance systems, Smart transportation, Smart manufacturing Digitized, SMART education ecosystem, Smart city, Digital supply chain, Transaction and payment processing, Digital government platforms, Digital healthcare infrastructure, Digital oilfields, Smart grid etc

This paper is structured as follows. In section 2, related works on various cyber resilient frameworks and key capabilities are discussed. In Section 3 the list of assets that the defenders to protect, section4 mentions about the hacker's team as an adversarial, section 5 methodology and strategy, section 6 comparison of methodologies finally conclusion in section 7

II. RELATED WORKS

A. Cyber resilient framework.

From the engineering perspective, the resilience is defined as the ability identify, classify, analyze and evolve differences, fluctuations, conflicts, interruptions and shocks [29]. The advanced cyber threats are explicitly playing a major role in engineering systems. The Cyber Resiliency Engineering Framework (CREF) [14,1925,26] and Cyber Resilience Matrix (CRM) (27) are used to improve the cyber resilience in the system. In 2009, Madni and Jackson have designed CREF framework to achieve the cyber resiliency with four goals such as plan, absorb, recover, adapt and eight objectives, and fourteen techniques. Whereas the CRM framework defines cyber resilience improvement through a resilience matrix metrics, of four goals like plan/prepare, absorb, recover, adapt suggested by

National Resilience to Hazards and Disasters 2012 and with already Alberts defined four domains such as physical, information, cognitive, social in 1996.

In February 2014, EO 1336 of NIST, recommended cybersecurity framework consists of

five components such as Identify, Protect, Detect, Respond, Recover" [NIST 2014]. The five functional components are used in the life cycle management of all outcomes in subsequent categories and subcategories. NIST Cyber security Framework (CSF) [NIST 2014, 2017] is designed for organizations and enterprise information infrastructures in critical infrastructure sectors. It indirectly involves advanced cyber threat.

SEI CERT Resilience Management Model (RMM) [28] is designed for organizations to subtly stores the advanced cyber threat through dedicated forms with 26 areas, specific practices/goals for each area.

Electricity Subsector Cybersecurity Capability Maturity Model proposed by ES-C2M2, DOE and DHS 2014 used to design obliquely house advanced cyber threat in energy sector.

Department of Homeland Security, Cyber Resilience Review (CRR, DHS) is designed for operational resilience and cybersecurity against covertly billets of advanced cyber threat. It has

10 n practice areas with goals and maturity indicator levels (MILs) for every area.

Cyber Resilience Assessment Framework (C-RAF)[KPMG 2016] designed for operational resilience and cyber defence in the financial sector to tacitly quarters with advanced cyber threat. It has 7 practice areas of governing, identifying, protecting, detecting, response & recovery, situational alertness, and 3rd party risk supervisions and maturity levels for every area.

Regional Cyber Resilience Maturity Model [The MITRE Corporation 2016] designed for regional cyber infrastructures as openly includes advanced cyber threats like funding and investment, operationalization, and technology and infrastructure. It also includes maturity levels for areas of governance, planning and prioritization.

B. Digital operation of key capabilities

Cyber security mainly concentrates on access control, whereas cyber resilience is for assets of the organizations to ensure continuous improvement [22]. It lied foundation on classification, prioritization and strategic policy of security controls in Realtime. Since it is the organizational purposes, the key assets of

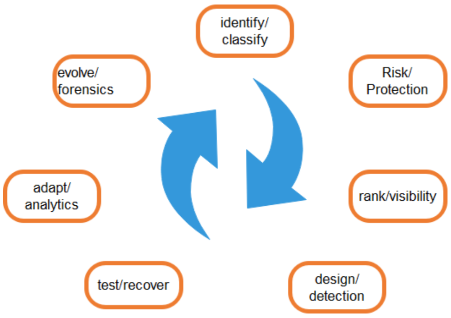

Fig 1:Cyber Resilience Objectives

electronic and behavioral are need to protect and to recover to the optimum level against the adversarial events. The Fig 1. is explained cyber resilience of various objectives and its continuous flow.

Identification. The organization/ application contains different types of assets. To identify the most valuable assets which in risk, it is necessary to perform an asset management and risk assessment. So, it is essential to know the status like communication with in network architecture, about the devices their resilient capabilities, critical business data and its resiliencies. based on the knowledge of the assets, security strategy will be framed.

Protection. The impact of attacks is filtrated by framing new policies, processes and mechanisms to build the systems are resilient as maintaining integrity during an attack, defend against modification from unauthorized or unauthenticated entities.

Detection. The Security analyst should bank the threats which evolve through the timely discovery by measuring, collecting, verifying and analyzing the integrity of the system. Detection anticipates to notify the behavior, log and forwarding techniques to protect from harmful user or the network.

Recovery. Restoring the operation of corrupted/compromised platforms, apps and services to approximately to normal. An agent is allowed to run and correct/replace compromised components.

Visibility. The visibility mechanisms support from protection to forensics phase. Visibility tool are graphically representing system integrity with cyber resiliency functions to the security and compliance stances to administrators, users, tools, applications or third parties.

Analytics. The incident data examines to supplement situational alertness. The analytics tools reduce the time from detection to recovery to provide proactive defense in the network.

Forensics. The support team should ingest relevant recovery document of protective, dispensation, scrutinizing and bestowing system evidence

A digital transformation is about how much the technical investments, tools, policies and processes are involved to protect the investments. The capabilities of the agent cannot completely remove cyber risk, but could create alertness to the risks and build proactive defenses to reduce the impact of threats.

C. Resilience performance metrics

It deals with the real-world representation of data through the mathematical and physical concepts. To model the system, acquisition of the information towards the critical functions (CF) of the system, time for identifying patterns(T),estimating the threshold (TH), requirement of memory and adaptation nature(M), and for network model presentation of interconnection network is needed.

$$\text{Resilience} = CF * TH * T * M \qquad (1)$$

According to the Merriam Webster, 2013 defines resilience is the capability to recuperate from or simply regulate to disaster or transformation [15]. The term resilience is defined by NAS (national academy of sciences) the ability to formulate and plot for engross, recuperate from and more successfully acclimate to adversative trials [10]. From the equation 1, The critical functionality is to comprehend and design to fight against interrupt, thresholds should be tolerance of stress and stability to absorber against the shocks and recovery time also estimated. Recovery time (scale) is used to find the system resilience after the interrupt, even the threshold is not increased. lastly the memory is to the level of auto organization of the system and adaptative nature of safe-to-fail to manage and learn the system resilience.

Critical functionality is defined as the source of sensitive information like system which is integrated resilience. To manage uncertain and unknown threats the conventional risk-based approaches are criticized in critical infrastructure [11]. The 4R's of resilience helps to measures are robustness, redundancy, resourcefulness and rapidity [12].

Operational resilience is the capability of an entity which can tolerant to encounter the task even with disturbances and reappear to its earlier position caused by adversaries. Entities such as networks, critical infrastructure, nations etc,. Operational resilience is the intrinsic capability of an enterprise at various levels in administrations and business cubes to rebel unsuspected pressure. The threats and prospects come from internal and external sources, to continue on assuring the effective accomplishment of purposes and targets earlier, during, and subsequently come across of the pressure [17].

The future opportunity for resilience Engineering in the interdependent critical infrastructures like water, transport and energy. There four main principles in defining the resilience as anticipate, absorb, adapt, recover. To provide resilience in engineering to focus on the performance of system's infrastructure by enhancing the key features: Robustness, Redundancy, resourcefulness, rapid recovery. spatial- temporal patterns.

The resilience has 5 processes such as plan the resilience feature of a critical functions which services for physical and technical engineered system, absorb the system functioning threshold based on the sensitivity to changes in input variables, recover is to calculate the time and scale until recovery is happened, adapt memory/adaptive management redesigning of engineering systems designs based on past and future stressors learned from past events.

III. Defenders Assets

Adversaries are the launchers of the attacks for various purposes. The perpetuators are hacktivist, cyber criminals, APT attackers, terrorist and malicious insiders.

A. Targets:

Assets may be tangible and intangible. Some of the groups targets the sensitive information of personal identity and/or financial information, and but the openly available corporate information tends to commit identity theft and financial fraud. the some group have competitive role against other industry and/or state-sponsored intellectual services and targets proprietary and non-public information, also intellectual property and trade secrets, with the purpose to competed products and services to devise a strategy in order to steal information from([Hacking exposed 7] p. 314)information systems; command, control, and communication systems; and industrial or process control systems (ICS or PCS).

The experts suggest Machine learning supports in malware analysis of the PE files which executes in windows. The software developer, reverse engineers would benefit to automate the process and also to tracking flow control. The idea of analysis contains objective of analysis, PE features and possible algorithm used to predict the malware.

There may be several objective of malware analyses such as similarities between different malwares, prediction, categorical detection etc., PE files have several features like byte sequences, APIs, opcodes, CPU registers, etc.,

D. Risk assessment

[2] Due to the sudden rapture of advanced potential threats with unpredictability, uncertainty nature, the existing risk assessment methods are in adequate to the identify the threats in cyber ecosystem. Cyber risk can be identified and reduce the risk, cyber resilience is necessary to completely trashed till the residual level for the known threats, but for unknown and emerging zero-day exploits, mitigation is impossible.

Risk=threat*vulnerability*consequences. (2)

a) Threats

Threats which are created by human or by an event is known as malevolent actor. It may be cyber, kinetics and hybrid cyber-kinetic. The generic threat matrix techniques are difficult to designate and degree the threats. The threat matrix classifies threats and allots a threat level from 1 (most capable) to 8 (least capable). Influencing factors to classify the threat are time, technical personnel, cyber knowledge. To prevent APT attack is virtually impossible and APT's passive character and persistent for long time. [4]. Data driven security is proactive cyber defense mechanism to protect from cyber threats. The security analyst usually collects logs from critical systems to analyze the network threats. In the data driven security scenario, deep packet inspection technique (DPI) [3] is used to analyze all data traffic at every layer of the network stack instead of analyzing logs alone. [5]

b) vulnerability

[3] An existing approach mostly used to characterize vulnerabilities on the basis of known vulnerabilities or common Vulnerability Scoring System (CVSS) framework of software and the hardware.[5] Modern infrastructure management tools used in enterprise for patching and hardening, in order to strengthen the system and to reduce the chance of adversaries entering through the vulnerabilities. Yet APT actors continually prove the capability with modern tools, skills, customized generic malware, zero-day exploits to compromise systems.

c) Consequences

Most frameworks for measuring cyber risk include some credentials and quantification of penalties [3]. The consequences are often labeled in dollar amounts or scores to be used for evaluation of risk scenarios. To measure the consequences of the risk, the Software Engineering Institute proposed Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE Allegro) framework to calculate the risk analysis of a cyber system based on the assets.

d) Likelihood

In order to measure the cyber-attack, like hood could be estimated with apriori known characteristics of system/network.

IV. ADVERSARIAL/HACKER'S TEAM.

The hacker groups may be anonymous and non-state terror organizations may seek to do damage without concern of long term information extraction. Stuxnet, Flame and Gauss attacks are all examples of these as are Wikileaks-style information dumps.

A. *Cyber-attack lifecycle modelling*

1) Cyber kill model

In cyber security, [5] computer network attack (CNA) or computer network espionage (CNE), The Kill Chain is used to describe [20] seven steps of attack, as follows:

1. Reconnaissance – [8] To identify the target, the information is crawled from Internet websites which are publicly available.
2. Weaponization – a coupling technique of combining a malicious payload such as trojan along with an application data file like adobe reader, Microsoft office documents act as an automatic weaponize to exploit the victim.
3. Delivery – [7] the weapon is transmitted to the victim to target the environment. [8,9][The Lockheed Martin Computer Incident Response Team (LM-CIRT)] APT actors use attachments, links, and USB as the three delivery vectors of weaponize are through the communication of.
4. Exploitation – At the click of the victim downloads the payload, it triggered the intruders malicious code that cause exploitation to the targets (application/Operating system) through their vulnerabilities.
5. Installation -The Installation of malware (trojan) on the victims' computer, helps the adversary maintains the persistence to break the chain.
6. Command and Control (C2) – once after malware is installed, the adversary uses command and control channel through their backdoors to access the assets of the victim. The system is compromised by the adversaries.
7. Actions on Objectives – The objective is achieved by creating a gateway in the victim's host or network. Thus, the adversaries could exfiltrate the data, by violating the integrity and availability.

B. *Attack strategy*

The authors of [19],[21] suggests that Feature manipulation cost ($Fman_{cost}$) and Adversarial Skill/budget (S_{adv}) Cyber-attacks are the tools for financial gain, which ranges between hundreds of billions and several trillions of dollars .To launch the shot of cyber-attack the adversarial capabilities (skills, dedicated team, fixing the target, tools selection, stealing mechanism and technical skills and sophisticated infrastructure , etc.,) are essentially high profiled. The adversarial can do either inserting additional resources or manipulate the data or both in in the training data. The goal is to achieve identify the potential of adversary and their attack budget S_{adv} and to set the feature resilient.

C. *Risk management strategy*

To identify the assets which are prone to vulnerable and to protect them from all the known threats for many isolated systems. but it is not from unknown threats to protect the system. The risk management strategy can also define an order of precedence for responding to identified risks, analogous to the safety order of precedence, such as "harden, sensor, isolate, obfuscate." Defenders budget (bud_{def})- *to* develop algorithms and a methodology to leverage budget for an optimal defense strategy.

$$Fman_{cost}+S_{adv}=F_{resilient}\{\text{if } Fman_{cost}>S_{adv}\} \quad (3)$$

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)
© Copyright: All rights reserved.

V. METHODOLOGY

The data extracted behavior are through static and dynamic.[21] The approach is static, without executing malicious patterns are identified within the malicious executable body, it contains function call name, file structure information, import tables, strings, control flows, etc; In dynamic approach , execute the analyzed file to zoomed out its inter process communication of OS include system call names, combined with arguments, return values, and context environment variables.

A. *Feature extraction*

(4)$\theta^* = \arg max_\theta\, G(\theta) + \gamma R(\theta)$

[29],[30],[19] In abstract G and R denote a generalization ability and resilience to an attack; θ selected feature subset from the total set of features, and γ tradeoff coefficient formalizing the relative weights related to generalization and resilience.

B. *Classifier*

In cyber security, classifier is used to measure true positive rate (TPR) and false positive rate (FPR) values; TPR is defines as the correctly identified percentage of all malicious data entries are malicious and FPR is calculated as percentage of wrongly classified of benign data entries as malicious .[19],[22],[28] as a defender, shots to aim TPR_{max} and FPR_{min}.

C. *Receiver Operating Characteristics (ROC)*

The Receiver Operating Characteristics (ROC) curve plots the trade-off between a classifier's TPR and FPR. The area under curve (AUC), a complete plot has a single number, if it is high value, then it indicates performance is better. Thus, AUC is act as an optimizer factor and for analyze the performance of different models.

VI. EXPERIMENTS

In the last decade, the researchers used benchmark datasets like KDD98, KDDCUP99 and NSLKDD. Due to the lack of dataset, UNSW-NB15 data set was created and published as a latest bench mark dataset for research purposes.- The data set comprises nine families of attacks, includes Fuzzers, Analysis, Backdoors, DoS, Exploits, Generic, Reconnaissance, Shellcode and Worms. with 49 features were developed using twelve algorithms and agus, Bro-IDS tools along with the class label. The size of dataset has merged the training set is 175,341 records and the testing set is 82,332 records of various types of attack and normal of hybrid real time network traffic and also has low footprint behavior.

The data set contains the features are grouped into six types such as the Flow, Basic, Content, Time, Additional Generated and Labelled. The Additional Generated Features are further categorized into two subgroups called General Purpose Features and Connection Features

The features of the UNSW-NB 15 data set are divided into six groups as follows [34]:

1) Flow features: The identifier attributes between hosts, (client- to- serve or server-to-client.)

2) Basic features: the attributes that represent protocols connections.

3) Content features: It wrap the attributes of TCP/IP, some http services.

4) Time features: The attributes of time, (for ex: arrival time between packets, start/end packet time and round-trip time of TCP protocol).

5) Additional generated features: It further divided into two forms: (1) General purpose features (from number 36 - 40) which each feature has its own purpose, in order to protect the service of protocols. (2) Connection features (from number 41- 47) are built from the flow of 100 record connections based on the sequential order of the last time feature.

6) Labelled Features: this group represents the label of each record

VII. RESULTS AND DISCUSSION

The experiment is conducted using UNSW-NB15 dataset consists of attack categories such as Normal, Reconnaissance, Backdoor, DoS, Exploits, Analysis, Fuzzers, Worms, Shellcode, Generic [34]. Normal contains 2,218,761 and considered as Natural transaction data. Fuzzers has 24,246and it means that attempting to cause a program or network suspended by feeding it the randomly generated data [24]. Analysis of 2,677 contains different attacks like port scan, spam and html files penetrations. Backdoors of 2,329 follows a technique in which a system.security mechanism is bypassed stealthily to access a computer or its data. DoS of 16,353 tries as malicious attempt to make a server or a network resource unavailable to users, usually by temporarily interrupting or suspending the services of a host connected to the Internet. Exploits of 44,525 a technique of the attacker knows of a security problem within an operating system or a piece of software and leverages that knowledge by exploiting the vulnerability. Generic of 215,481 uses technique that works against all block ciphers (with a given block and key size), without consideration about the structure of the block-cipher. Reconnaissance of 13,987 Contains all Strikes that can simulate attacks that gather information. Shellcode of 1,511 A small piece of code used as the payload in the exploitation of software vulnerability. Worms of 174 a technique used by the attacker replicates itself in order to spread to other computers [35]. Often, it uses a computer network to spread itself, relying on security failures on the target computer to access it

The dataset is processed with various algorithms to check the performance metrics Firstly attribute selected classifier and CFS feature is selected and REP Tree algorithm using 10-fold the cross-validation results are calculated for various metrics.

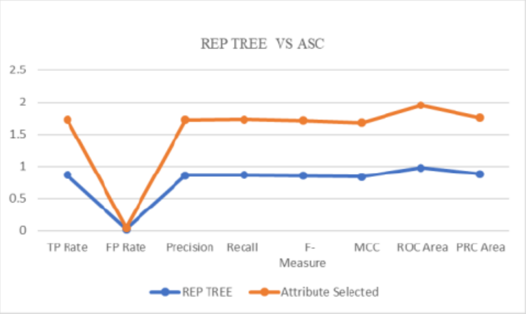

Fig 2. Performance metrics of REP TREE algorithm vs Attribute selected Classifier with TP and FP

The REP tree can learn as a fast decision tree to sort the using entropy to build a decision/regression tree calculates the impurity measure and reduced-error pruning whereas Attribute Selected Classifier (ASC) selects only training set to do cross-validation for evaluation with J48 in association of ZeroR, OneR, IBk. It is used for Cost-sensitive evaluation and classification to learn the subsets with entropy and information gain calculation to develop new classifier.

In Weka, Attribute evaluators are OneR, infoGain, Gain Ratio, Symmetrical Uncertainty and also Chi Squared, SVM, Relief F, Principal Components, Latent Semantic Analysis.

TABLE I: COMPARISION OF TWO CLASSIFIER

	REP TREE	Attribute Selected
TP Rate	0.861	0.865
FP Rate	0.022	0.022
Precision	0.858	0.862
Recall	0.861	0.865
F-Measure	0.855	0.858
MCC	0.838	0.842
ROC Area	0.977	0.976
PRC Area	0.88	0.876

In the Table I, the values of True positive (TP), False positive (FP), precision, recall, Receiver operating characteristics curve (ROC) are calculated. From the fig 3 it is observed that TP is increased by checking the attribute selected model, where the result is evaluated to produce a greater number of true positive to be resilient when compare with REP tree algorithm.

Table II explains the summary of the total instances in the dataset are correctly classified and incorrectly classified. The ASC classifier can be better performing than REP Tree which is from the performance graph, ASC dominated the REP tree slightly in all of its performance.

TABLE II: SUMMARY OF CLASSIFIER RESPONSES

	REP	ASC
Correctly Classified Instances	221905	222904
Incorrectly Classified Instances	35768	34769
Total Number of Instances	257673	257673
Mean absolute error	0.0348	0.034
Root mean squared error	0.1365	0.1355
Relative absolute error (%)	22.57	22.0183
Root relative squared error(%)	49.13	48.7922
Kappa statistic	0.819	0.8239

Thus, the result is evaluated on various metrics, in order to analyze the instances of the dataset and to know the essential information about the cyber security operation usually used to classify the Unsw-nb15 dataset. The dataset is categorized with classifier and the error, statistics, and f-measure are calculated.

VIII. CONCLUSION

The cyber security is about the improve the IT infrastructure security. However, today's security measures are not enough to ensure the security in all means. So cyber resilience is discussed as essential in each operation of cyber environment. To achieve the resilience in each operation, the security analyst to be aware in knowledge and understanding of the methods and strategies employed by the hackers. Using UNSW NB15 dataset, detection of the TP can be improved by using ASC classifier. Future works may be implemented in deep learning algorithm to produce more TP.

REFERENCES

1. Deng, X., Shi, H., & Mirkovic, J. (2017). Understanding malware's network behaviors using fantasm. In The {LASER} Workshop: Learning from authoritative Security Experiment Results ({LASER} 2017) (pp. 1-11).
2. Kolias, G. Kambourakis, A. Stavrou, and S. Gritzalis, "Intrusion Detection in 802.11 Networks: Empirical Evaluation of Threats and aPublic Dataset," IEEE Communications Surveys Tutorials, vol. 18, no. 1, pp. 184–208, 2016
3. Ganin, A. A., Quach, P., Panwar, M., Collier, Z. A., Keisler, J. M., Marchese, D., & Linkov, I. (2017). Multicriteria decision framework for cybersecurity risk assessment and management. Risk Analysis.
4. Chen, Jiageng, Chunhua Su, Kuo-Hui Yeh, and Moti Yung. "Special issue on advanced persistent threat." (2018): 243-246.
5. Hutchins, Eric M., Michael J. Cloppert, and Rohan M. Amin. "Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains." Leading Issues in Information Warfare & Security Research1, no. 1 (2011): 80.
6. Levy-Bencheton, C., and E. Darra. "Cyber security and resilience of intelligent public transport: good practices and recommendations." (2015).
7. Giura, Paul, and Wei Wang. "A context-based detection framework for advanced persistent threats. strategies 69-74. IEEE, 2012.
8. Krekel, Bryan. Capability of the People's Republic of China to conduct cyber warfare and computer network exploitation. NORTHROP GRUMMAN CORP MCLEAN VA, 2009.
9. . Damballa, "The Command Structure of the Aurora Botnet," http://www. damballa.com/research/aurora/, March 2010.
10. Connelly, Elizabeth B., Craig R. Allen, Kirk Hatfield, José M. Palma-Oliveira, David D. Woods, and Igor Linkov. "Features of resilience." Environment systems and decisions 37, no. 1 (2017): 46-50.
11. Ganin, Alexander A., Emanuele Massaro, Alexander Gutfraind, Nicolas Steen, Jeffrey M. Keisler, Alexander Kott, Rami Mangoubi, and Igor Linkov. "Operational resilience: concepts, design and analysis." Scientific reports 6 (2016): 19540.

12. Linkov, Igor, Todd Bridges, Felix Creutzig, Jennifer Decker, Cate Fox-Lent, Wolfgang Kröger, James H. Lambert et al. "Changing the resilience paradigm." Nature Climate Change 4, no. 6 (2014): 407.
13. . Vespignani, Alessandro. "Complex networks: The fragility of interdependency." Nature 464, no. 7291 (2010): 984.
14. Linkov, Igor, Daniel A. Eisenberg, Matthew E. Bates, Derek Chang, Matteo Convertino, Julia H. Allen, Stephen E. Flynn, and Thomas P. Seager. "Measurable resilience for actionable policy." (2013): 10108-10110.
15. Linkov, Igor, Daniel A. Eisenberg, Kenton Plourde, Thomas P. Seager, Julia Allen, and Alex Kott. "Resilience metrics for cyber systems." Environment Systems and Decisions 33, no. 4 (2013): 471-476.
16. Park J, Seager TP, Rao PS, Convertino M, Linkov I (2012) Integrating risk and resilience approaches to catastrophe management in engineering systems. Risk Anal 33(3):356–367
17. Birkie, Seyoum Eshetu, Paolo Trucco, and Matti Kaulio. "State-of-the-Art Review on Operational Resilience: Concept, Scope and Gaps." In IFIP International Conference on Advances in Production Management Systems, pp. 273-280. Springer, Berlin, Heidelberg, 2012.
18. . Linkov, Igor, and Alexander Kott. "Fundamental concepts of cyber resilience: Introduction and overview." In Cyber resilience of systems and networks, pp. 1-25. Springer, Cham, 2019
19. T. Sakuraba, S. Domyo, B.-H. Chou, and K. Saku, “Exploring security counter measures along the attack sequence,” in Information Security andAssurance,2008. ISA 2008. International Conference on. IEEE, 2008,pp. 427–432
20. Conklin, William Arthur, Dan Shoemaker, and AnnKohnke. "Cyber resilience: Rethinking cybersecurity strategy to build a cyber resilient architecture." In ICMLG2017 5th International Conference on Management Leadership and Governance, p. 105. 2017.
21. Moustafa, Nour, and Jill Slay. "The evaluation of Network Anomaly Detection Systems: Statistical analysis of the UNSW-NB15 data set and the comparison with the KDD99 data set." Information Security Journal: A Global Perspective 25, no. 1-3 (2016): 18-31.
22. Moustafa, Nour, and Jill Slay. "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), pp. 1-6. IEEE, 2015.
23. Elovici, Yuval, Asaf Shabtai, Robert Moskovitch, Gil Tahan, and Chanan Glezer. "Applying machine learning techniques for detection of malicious code in network traffic." In Annual Conference on Artificial Intelligence, pp. 44-50. Springer, Berlin, Heidelberg, 2007.
24. Rovito, Sarah Maria. "An integrated framework for the vulnerability assessment of complex supply chain systems." PhD diss., Massachusetts Institute of Technology, 2016.
25. Bodeau, Deborah, and Richard Graubart. "Cyber resiliency engineering framework." MTR110237, MITRE Corporation (2011).
26. Linkov, Igor, Daniel A. Eisenberg, Kenton Plourde, Thomas P. Seager, Julia Allen, and Alex Kott. "Resilience metrics for cyber systems." Environment Systems and Decisions 33, no. 4 (2013): 471-476.
27. Caralli, Richard A., Julia H. Allen, and David W. White. CERT resilience management model: A maturity model for managing operational resilience. Addison-Wesley Professional, 2010.
28. Hollnagel, Erik, David D. Woods, and Nancy Leveson. Resilience engineering: Concepts and precepts. Ashgate Publishing, Ltd., 2006.
29. Kaur, Ratinder, and Maninder Singh. "Automatic evaluation and signature generation technique for thwarting zero-day attacks." In Internationa Conference on Security in Computer Networks and Distributed Systems, pp. 298-309. Springer, Berlin, Heidelberg, 2014.
30. Ng, George Y., Feiyin Zhang, and Fernando Tancioco. "Inferential analysis using feedback for extracting and combining cyber risk information." U.S. Patent 9,521,160, issued December 13, 2016.
31. Deng, Ruilong, Gaoxi Xiao, and Rongxing Lu. "Defending against false data injection attacks on power system state estimation." IEEE Transactions on Industrial Informatics 13, no. 1 (2015): 198-207.
32. . Moustafa, Nour, and Jill Slay. "The significant features of the UNSW-NB15 and the KDD99 data sets for network intrusion detection systems." In 2015 4th international workshop on building analysis datasets and gathering experience returns for security (BADGERS), pp. 25-31. IEEE, 2015.

[33]. Rajendra Patil, Harsha Dudeja, Chirag Modi. "Designing an Efficient Security Framework for Detecting Intrusions in Virtual Network of Cloud Computing", Computers & Security, 2019.

[34]. Nour Moustafa, Jill Slay. "UNSW-NB15: a comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set)", 2015 Military Communications and Information Systems Conference (MilCIS), 2015

AUTHORS PROFILE

Diana Arulkumar, worked as an assistant professor in karunya institute of technology and science,coimbatore. she is currently doing the research on “**Cyber Resilience Against The Advanced Persistent Threats**”. Her research areas are cyber security ,IoT, Biometrics.

Dr. K. KARTHEEBAN working as Associate professor, Department of computer Science and Engineering, Kalasalingam Academy of Research and Education, Krishnankoil, and Tamilnadu, India. Also he was worked as a Deputy Director Academic. He received his M.E degree in computer science and Engineering from College of Engineering, Anna University, and Chennai in 2007 and Completed PhD in the title of **“Development of Efficient Algorithms for Secure Communication in Distributed Computing Environment”** in the Department of Computer Science and Engineering at Kalasalingam Academy of Research and Education, Anandnagar, and TAMILNADU, INDIA in 2014. He worked as a faculty from Adhiyamaan College of Engineering, Hosur, India between 1996-1998. Currently 1 scholar completed his PhD and 6 students are doing their PhD under him with the topics such as Internet of Things, Medical Image Processing, Video Analytics, Cyber Forensics , Sentimental Analysis and Scheduling in Cloud computing. He has published many papers in SCI journals and Scopus indexed conferences. Also he has submitted proposals to DeIT, SERB and DRDO. His areas of interests include IoT, Medical image processing, cryptography and bioinformatics and grid and cloud computing.