A MEASUREMENT APPROACH FOR INLINE INTRUSION DETECTION OF HEARTBLEED-LIKE ATTACKS IN IOT FRAMEWORK

[1]. Mrs. A. DIVYA
Assistant Professor, Department of CSE, Sreyas Institute of Engineering and Technology, Telangana, India,
divya.a@sreyas.ac.in

[2]. Purba Senapati
Department of CSE, Sreyas Institute of Engineering and Technology, Telangana, India,
purbas2001@gmail.com

[3]. Akhil Nellutla
Department of CSE, Sreyas Institute of Engineering and Technology, Telangana, India,
nellutlaakhil@gmail.com

[4]. Gunti Prasanna
Department of CSE, Sreyas Institute of Engineering and Technology, Telangana, India,
guntiprasanna2@gmail.com
[5]. Shaik Abdul Rahman

Department of CSE, Sreyas Institute of Engineering and Technology, Telangana, India,

shaikabdulrahman952@gmail.com

Abstract

Cyber security is one of the most crucial aspects of the Internet of Things (IoT). Among the possible threats, great interest is today paid toward the possible capturing of information caused by external attacks on both client and server sides. Whatever the IoT application, the involved nodes are exposed to cyber-attacks mainly through the vulnerability of either the sensor nodes themselves (if they have the capabilities for networking operatively) or the IoT gateways, which are the devices able to create the link between the local nodes of the IoT network, and the wide area networks. Due to the low-cost constraints typical of many IoT applications, the IoT sensor nodes and IoT gateways are often developed on low performance processing units, in many cases customized for the specific application, and thus not easy to update against new cyber threats that are continuously identified. In the framework of cyber-attacks aimed at capturing sensitive information, one of the most known was the heart bleed, which, has allowed attackers to remotely read protected memory from an estimated 24–55 percent of popular HTTPS sites. To overcome such a problem, which was due to a bug of the OpenSSL, a suitable patch was quickly released, thus allowing to avoid the problem in most of the cases. However, IoT devices may require more advanced mitigation techniques, because they are sometimes unable to be patched for several practical reasons. In this scenario, the paper proposes a novel measurement method for inline detecting intrusions due to heart bleed and heart bleed-like attacks. The proposed solution is based on an effective rule which does not require decoding the payload and that can be implemented on a low-performance

general-purpose processing unit. Therefore, it can be straightforwardly implemented and included in either IoT sensor nodes or IoT gateways. The realized system has been tested and validated on a number of experiments carried out on a real network, showing performance comparable (in some cases better) with the heavier machine learning-based methods.

I INTRODUCTION

Network security monitoring and measurements are commonly used methodologies in information security operation centres. The network traffic is captured by means of suitable measurement probes and the related logs monitored to detect any illegal activities within the network. Intrusion detection systems (IDSs) are automatic systems specifically designed for identifying threats that are able to potentially create damage to information systems as data leakages, Distributed Denial of Service (DDoS), Bad Data Injection, to cite a few, and in different contexts of application. Recent trends of cyberattacks go toward Internet of Things (IoT) and operational technology (OT) infrastructure which will involve more and more targets including critical infrastructures, traditional manufacturing facilities, even smart home networks, in the next years. Due to the prevalence of employees managing these systems via remote access, which provides a very good entry point for cybercriminals, it is expected that attackers will target industrial sensors to cause physical damage that could result in assembly lines shutting down or services being interrupted. Among the most popular cyberattacks, Heartbleed vulnerability took the Internet by surprise in April 2014 and allowed attackers to remotely read protected memory from an estimated 24%–55% of popular HTTPS sites. This kind of attack was due to a bug in OpenSSL, the most popular open-source cryptographic library that implements the SSL and TLS protocols. In particular, the implementation of TLS heartbeat extension had a bug allowing attackers to remotely access private data from both clients and servers. Although a suitable patch was quickly released for overcoming such a bug, recent scientific and technical literature prove how the problem of Heartbleed still persists in many contexts since systems that did not (or could not) upgrade to the patched version of OpenSSL are still affected by the vulnerability and open to attack. As matter of fact, any server or cloud platform should be relatively easy to patch. However, IoT devices may require more advanced mitigation techniques, because they are sometimes unable to be patched for practical reasons. Additionally, some companies often use a customized version of the vulnerable software. As an example, in the case of Heartbleed, OpenSSL is an open-source library and some companies might have modified it for their purposes. In such cases, a direct patch is not possible–the company must then reintroduce its custom code into the new version of the library. This is often the reason why web open-source software is not immediately updated by companies even if critical new bugs are found.All these considerations, together with the fact that Heartbleed-like attacks can be still dangerous, push again the research activity toward defining suitable intrusion detection strategies able to identify such kinds of attacks. Moreover, the analysis of the literature has proved how, concerning Heartbleed and Heartbleed-like attacks, IDSs able to inline identify such kinds of attacks are not so far available. Generally, to develop an IDS, most of the solutions are based on Artificial Intelligence (AI) and Machine Learning approaches, which generally incur a significant computational burden, nevertheless in many application contexts concerning IoT, where devices and network systems are characterized by low costs and consequently by low resources for data processing and storage, the applicability of such techniques is not always feasible.

II LITERATURE SURVEY

"***Detecting Heartbleed-Like Attacks in IoT Frameworks: A Survey***"

This comprehensive survey explores various approaches for detecting Heartbleed-like vulnerabilities in IoT frameworks. It covers techniques such as anomaly detection, signature-based detection, and machine learning-based methods. The survey evaluates the effectiveness, limitations, and challenges associated with each approach and identifies promising directions for future research in this area.

"Machine Learning-Based Intrusion Detection Systems for IoT Environments"

This study focuses on the application of machine learning techniques for intrusion detection in IoT environments. It discusses the adaptation of existing intrusion detection methods to detect Heartbleed-like attacks specifically tailored for IoT frameworks. The study evaluates the performance of these methods in terms of detection accuracy, false positive rates, and resource consumption, providing insights into their practical applicability.

"Anomaly Detection Approaches for IoT Security: A Review"

Anomaly detection is a popular technique for identifying suspicious activities indicative of potential attacks in IoT systems. This review paper surveys various anomaly detection approaches, including statistical methods, machine learning algorithms, and hybrid techniques. It discusses the applicability of these approaches in detecting Heartbleed-like attacks and highlights the importance of feature selection and data pre-processing in enhancing detection accuracy.

"Signature-Based Detection Techniques for IoT Security"

Signature-based detection techniques rely on predefined patterns or signatures of known vulnerabilities to identify malicious activities. This paper investigates the effectiveness of signature-based detection methods in the context of IoT security, with a focus on detecting Heartbleed-like attacks. It discusses the challenges of maintaining up-to-date signature databases and the trade-offs between detection accuracy and computational overhead.

"***IoT Security Frameworks and Challenges: A Systematic Literature Review"***

This systematic literature review provides an overview of existing IoT security frameworks and identifies common challenges and vulnerabilities. It discusses the importance of incorporating intrusion detection mechanisms, including those targeting Heartbleed-like vulnerabilities, into IoT security frameworks to mitigate potential risks. The review also examines the role of standardization efforts and regulatory compliance in enhancing IoT security practices.

III EXISTING SYSTEM

The internet of things (IoT) is a collection of common physical things which can communicate and synthesize data utilizing network infrastructure by connecting to the internet. IoT networks are increasingly vulnerable to security breaches as their popularity grows. Cyber security attacks are among the most popular severe dangers to IoT security. Many academics are increasingly interested in enhancing the security of IoT systems. Machine learning (ML) approaches were employed to function as intrusion detection systems (IDSs) to provide better security capabilities. This work proposed a novel distributed detection system based on machine ML approaches to detect attacks in IoT and mitigate malicious occurrences. Furthermore, NSL-KDD or KDD-CUP99 datasets are used in the great majority of current studies. These datasets are not updated with new attacks. As a consequence, the ToN-IoT dataset was used for training and testing. It was created from a large-scale, diverse IoT network. The ToN-IoT dataset reflects data from each layer of the IoT system, such as cloud, fog, and edge layer. Various ML methods were tested in each specific partition of the ToN-IoT dataset. The proposed model is the first suggested model based on the collected data from the same IoT system from all layers. The Chi2 technique was used to pick features in a network dataset. It reduced the number of features to 20.

Another feature selection tool employed in the windows dataset was the correlation matrix, which was used to extract the most relevant features from the whole dataset. To balance the classes, the SMOTE method was used. This paper tests numerous ML approaches in both binary and multi-class classification problems. According to the findings, the XGBoost approach is superior to other ML algorithms for each node in the suggested model.

Disadvantages

- The system doesn't found DATA LEAKAGE DUE TO Lack of HEARTBLEED ATTACKS
- The system doesn't implement Rule-based Methodology for supporting ML Algorithms.

IV PROBLEM STATEMENT

As the deployment of Internet of Things (IoT) devices continues to grow within smart city infrastructures, the inherent vulnerabilities of these devices become increasingly apparent. Among the emerging threats, the risk of Heartbleed-like attacks poses a significant challenge to the security and integrity of sensitive data transmitted across the IoT framework. Heartbleed, a well-known security vulnerability in the OpenSSL cryptographic software library, has underscored the potential for attackers to remotely exploit weaknesses and compromise the confidentiality of information.

The primary problem addressed by this project is the absence of an effective and resource-efficient measurement approach for the inline detection of Heartbleed-like attacks within smart city IoT frameworks. The challenge is to develop a rule-based intrusion detection system capable of identifying patterns indicative of such attacks in real-time, without compromising the limited processing capabilities of IoT sensor nodes and gateways. The solution should be adaptive to the unique characteristics of smart city IoT deployments, ensuring continuous monitoring, timely alerting, and efficient mitigation techniques. The project seeks to bridge the gap in cybersecurity for smart city IoT frameworks by proposing a comprehensive and practical solution that safeguards against the growing threat of Heartbleed-like attacks, thereby ensuring the secure operation of critical infrastructure in the smart city ecosystem.

V PROPOSED SYSTEM

In this framework, starting from the preliminary results provided in and on the basis of the past experience in the fields of measurements systems for network performance analysis, in this paper, the authors propose a novel measurement method designed for inline detecting on low performance systems, and able to identify heart bleed-like attacks on the basis of very straightforward and easy to implement rules. It falls in the class of network-based IDS and it is implemented by using very low-cost hardware and open-source software for data acquisition and analysis. To evaluate the performance of the proposed system, a suitable experimental setup has been realized for operating in real operating scenarios.

The experimental characterization made on several kinds of real attacks and several kinds of real standard data traffic shows very good performance in terms of the ability to correct detecting the heart bleed-like attacks and in discriminating them from the standard traffic, thus keeping the number of false alarms low.

Advantages

1.Rule-Based Intrusion Detection System: Implement a rule-based system that can identify patterns and behaviours indicative of Heartbleed-like attacks within the network traffic. These rules should be specifically tailored for the characteristics of IoT devices and the potential threats they face.

2.Payload Inspection and Decoding: Develop a mechanism for inspecting and decoding network payloads to analyse the content for signs of a Heartbleed-like attack. Consider the unique challenges posed by IoT devices, optimizing the process for minimal impact on resource-constrained processing units.

3.Low-Performance Processing Optimization: Optimize the intrusion detection system to operate seamlessly on low-performance general-purpose processing units commonly found in IoT devices. Utilize lightweight algorithms and efficient data structures to minimize resource consumption.

4. full Packet Capture (PCAP) allows obtaining detailed information about packets belonging to the network, such as packet headers, packet size, protocol, flags. Moreover, it is also possible to read the packet payload containing private information or sensitive data.

5. Net Flow, unlike the aforementioned method, provides a measurement of some parameters about each flow. Examples of measurements are the number of bytes exchanged during a flow, the number of packets in both directions, and derived parameters (e.g. average, standard deviation, variance).

VI IMPLEMENTATION

1. **Traffic Capture Module**:

- Responsible for capturing incoming and outgoing network traffic.
- Might utilize network interfaces or specific sensors to collect traffic data.

2. **Traffic Analysis Module**:

- Analyzes the captured network traffic.
- Identifies patterns or anomalies that could indicate potential attacks.

3. **Anomaly Detection Module**:

- Detects anomalies in the network traffic.
- Utilizes various algorithms or heuristics to identify deviations from normal behavior.

VII ALGORITHMS

Naive Bayes:

In the context of the project, Naive Bayes serves as a pivotal classification algorithm for distinguishing network traffic patterns. Its application involves categorizing the patterns as either normal or indicative of a Heartbleed-like attack based on specific features. By leveraging the inherent simplicity and effectiveness of Naive Bayes, the algorithm can effectively learn from labeled datasets, enabling the identification of subtle deviations in network traffic indicative of potential threats in real-time IoT frameworks.

Support Vector Machine (SVM):

Support Vector Machine (SVM), a robust classification algorithm, is employed in the project to detect anomalies within network traffic associated with potential Heartbleed-like attacks. Known for its proficiency in handling complex datasets and binary/multi-class classification tasks, SVM establishes decision boundaries to distinguish between normal and potentially malicious traffic patterns. Its versatility in capturing intricate relationships within the data makes SVM a valuable asset in real-time intrusion detection for IoT frameworks.

Logistic Regression:

Logistic Regression plays a pivotal role in modeling the relationship between network traffic features and the likelihood of Heartbleed-like attacks. This binary classification algorithm is well-suited for predicting the probability of intrusion events based on observed patterns in network traffic. By utilizing logistic regression, the project aims to gain insights into the probability of potential security breaches, contributing to the system's ability to make informed decisions in identifying and mitigating threats in IoT frameworks.

Decision Tree:

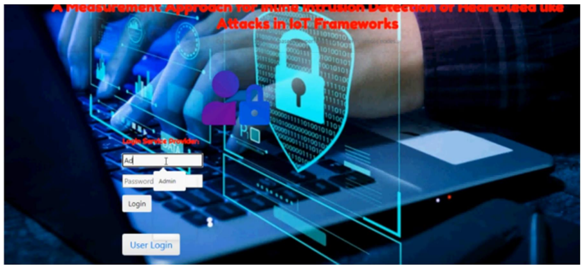
The project incorporates Decision Trees, known for their interpretability and clear decision-making structures, to model the decision process for identifying Heartbleed-like attacks. Decision Trees analyze specific features in network traffic to establish criteria for classifying patterns as normal or potentially malicious. This algorithm's ability to visually represent decision-making processes makes it an invaluable tool for creating intuitive and transparent intrusion detection models in the IoT framework.

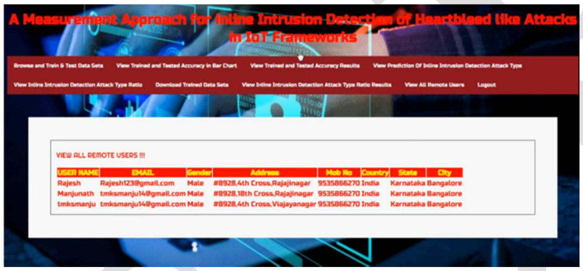
Random Forest

In enhancing the overall accuracy of intrusion detection, the project employs Random Forest, an ensemble learning method. By aggregating predictions from multiple Decision Trees, Random Forest provides a more robust classification of network traffic. This ensemble approach mitigates overfitting and variance, making it particularly effective for capturing nuanced patterns indicative of potential threats in real-time IoT frameworks. The versatility and accuracy of Random Forest contribute significantly to the reliability of the intrusion detection system.

VIII RESULTS

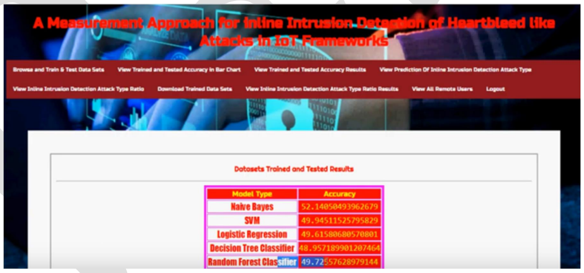
A Measurement Approach for inline Intrusion Detection of Heartbleed like Attacks in IoT Frameworks


A Measurement Approach for inline Intrusion Detection of Heartbleed like Attacks in IoT Frameworks
Login Service Provider:
Ad
Password
Admin
Login
User Login


A Measurement Approach for inline Intrusion Detection of Heartbleed like Attacks in IoT Frameworks
Browse and Train & Test Data Sets
View Trained and Tested Accuracy in Bar Chart
View Trained and Tested Accuracy Results
View Prediction Of Inline Intrusion Detection Attack Type
View Inline Intrusion Detection Attack Type Ratio
Download Trained Data Sets
View Inline Intrusion Detection Attack Type Ratio Results
View All Remote Users
Logout

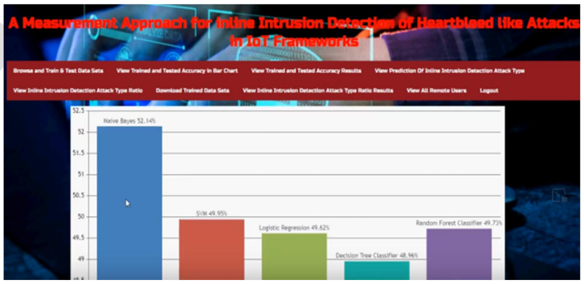
VIEW ALL REMOTE USERS !!!

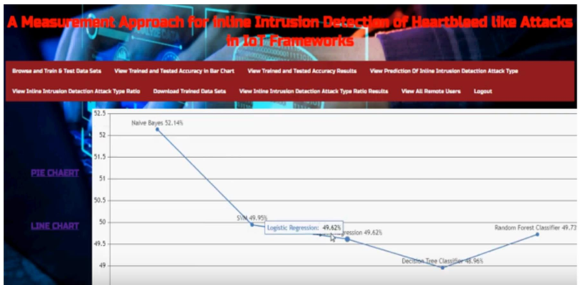
USER NAME	EMAIL	Gender	Address	Mob No	Country	State	City
Rajesh	Rajesh123@gmail.com	Male	#8928,4th Cross,Rajajinagar	9535866270	India	Karnataka	Bangalore
Manjunath	tmksmanju14@gmail.com	Male	#8928,18th Cross,Rajajinagar	9535866270	India	Karnataka	Bangalore
tmksmanju	tmksmanju14@gmail.com	Male	#8928,4th Cross,Viajayanagar	9535866270	India	Karnataka	Bangalore

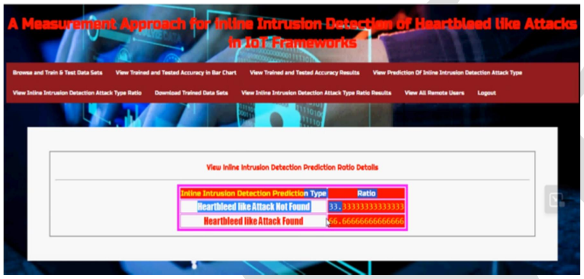

A Measurement Approach for inline Intrusion Detection of Heartbleed like Attacks in IoT Frameworks
Browse and Train & Test Data Sets
View Trained and Tested Accuracy in Bar Chart
View Trained and Tested Accuracy Results
View Prediction Of Inline Intrusion Detection Attack Type
View Inline Intrusion Detection Attack Type Ratio
Download Trained Data Sets
View Inline Intrusion Detection Attack Type Ratio Results
View All Remote Users
Logout

Datasets Trained and Tested Results

Model Type	Accuracy
Naive Bayes	52.14050493962679
SVM	49.94511525795829
Logistic Regression	49.61580680570801
Decision Tree Classifier	48.957189901207464
Random Forest Classifier	49.72557628979144

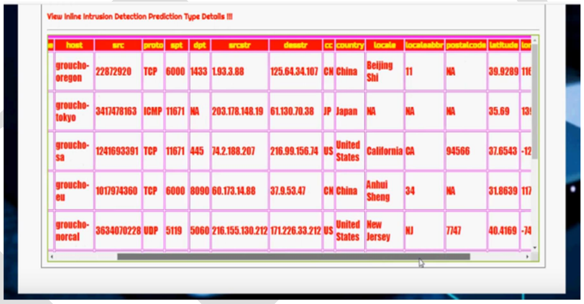

A Measurement Approach for inline Intrusion Detection of Heartbleed like Attacks in IoT Frameworks
Browse and Train & Test Data Sets
View Trained and Tested Accuracy in Bar Chart
View Trained and Tested Accuracy Results
View Prediction Of Inline Intrusion Detection Attack Type
View Inline Intrusion Detection Attack Type Ratio
Download Trained Data Sets
View Inline Intrusion Detection Attack Type Ratio Results
View All Remote Users
Logout
52.5
52
51.5
51
50.5
50
49.5
49
Naive Bayes 52.14%
SVM 49.95%
Logistic Regression 49.62%
Decision Tree Classifier 48.96%
Random Forest Classifier 49.73%


A Measurement Approach for Inline Intrusion Detection of Heartbleed like Attacks in IoT Frameworks
Browse and Train & Test Data Sets
View Trained and Tested Accuracy in Bar Chart
View Trained and Tested Accuracy Results
View Prediction Of Inline Intrusion Detection Attack Type
View Inline Intrusion Detection Attack Type Ratio
Download Trained Data Sets
View Inline Intrusion Detection Attack Type Ratio Results
View All Remote Users
Logout
PIE CHAERT
LINE CHART
52.5
52
51.5
51
50.5
50
49.5
49
Naive Bayes 52.14%
SVM 49.95%
Logistic Regression: 49.62%
Logistic Regression 49.62%
Decision Tree Classifier 48.96%
Random Forest Classifier 49.73


A Measurement Approach for Inline Intrusion Detection of Heartbleed like Attacks in IoT Frameworks
Browse and Train & Test Data Sets
View Trained and Tested Accuracy in Bar Chart
View Trained and Tested Accuracy Results
View Prediction Of Inline Intrusion Detection Attack Type
View Inline Intrusion Detection Attack Type Ratio
Download Trained Data Sets
View Inline Intrusion Detection Attack Type Ratio Results
View All Remote Users
Logout

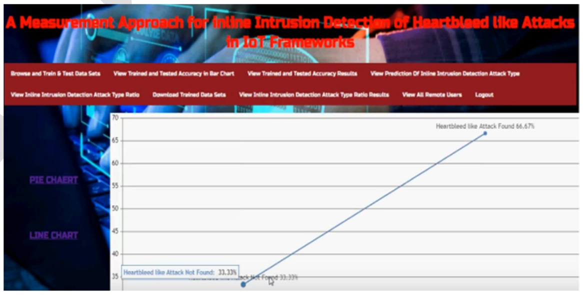
View Inline Intrusion Detection Prediction Ratio Details

Inline Intrusion Detection Prediction Type	Ratio
Heartbleed like Attack Not Found	33.3333333333333
Heartbleed like Attack Found	66.6666666666666



View Inline Intrusion Detection Prediction Type Details !!!

e	host	src	proto	spt	dpt	srcstr	desstr	cc	country	locale	localeabbr	postalcode	latitude	lo
	groucho-oregon	22872920	TCP	6000	1433	1.93.3.88	125.64.34.107	CN	China	Beijing Shi	11	NA	39.9289	116
	groucho-tokyo	3417478163	ICMP	11671	NA	203.178.148.19	61.130.70.38	JP	Japan	NA	NA	NA	35.69	139
	groucho-sa	1241693391	TCP	11671	445	74.2.188.207	216.99.156.74	US	United States	California	CA	94566	37.6543	-12
	groucho-eu	1017974360	TCP	6000	8090	60.173.14.88	37.9.53.47	CN	China	Anhui Sheng	34	NA	31.8639	117
	groucho-norcal	3634070228	UDP	5119	5060	216.155.130.212	171.226.33.212	US	United States	New Jersey	NJ	7747	40.4169	-74


A Measurement Approach for Inline Intrusion Detection of Heartbleed like Attacks in IoT Frameworks
Browse and Train & Test Data Sets
View Trained and Tested Accuracy in Bar Chart
View Trained and Tested Accuracy Results
View Prediction Of Inline Intrusion Detection Attack Type
View Inline Intrusion Detection Attack Type Ratio
Download Trained Data Sets
View Inline Intrusion Detection Attack Type Ratio Results
View All Remote Users
Logout
PIE CHAERT
LINE CHART
70
65
60
55
50
45
40
35
Heartbleed like Attack Found 66.67%
Heartbleed like Attack Not Found: 33.33%
Heartbleed like Attack Not Found 33.33%

IX CONCLUSION

The development of an inline intrusion detection system for detecting Heartbleed-like attacks in IoT frameworks presents a significant step towards securing IoT networks. Through this project, a comprehensive system has been crafted, capable of inspecting incoming traffic, identifying anomalies, and specifically recognizing patterns resembling Heartbleed vulnerabilities.

REFERENCES

- D. A. Kumar and S. Venugopalan, "Intrusion detection systems: A review", *Int. J. Adv. Res. Comput. Sci.*, vol. 8, no. 8, pp. 1-15, 2017.
- K. Yu, K. Nguyen and Y. Park, "Flexible and robust real-time intrusion detection systems to network dynamics", *IEEE Access*, vol. 10, pp. 98959-98969, 2022.\
- Y. Li and Q. Liu, "A comprehensive review study of cyber-attacks and cyber security; emerging trends and recent developments", *Energy Rep.*, vol. 7, pp. 8176-8186, Nov. 2021
- H. Sarjan, A. Ameli and M. Ghafouri, "Cyber-security of industrial Internet of Things in electric power systems", *IEEE Access*, vol. 10, pp. 92390-92409, 2022.
- A. Chidukwani, S. Zander and P. Koutsakis, "A survey on the cyber security of small-to-medium businesses: Challenges research focus and recommendations", *IEEE Access*, vol. 10, pp. 85701-85719, 2022.
- A. Huseinovic, S. Mrdovic, K. Bicakci and S. Uludag, "A survey of denial-of-service attacks and solutions in the smart grid", *IEEE Access*, vol. 8, pp. 177447-177470, 2020.
- G. Bernieri, M. Conti and F. Pascucci, "A novel architecture for cyber-physical security in industrial control networks", *Proc. IEEE 4th Int. Forum Res. Technol. Soc. Ind. (RTSI)*, pp. 1-6, Sep. 2018.
- Z. Durumeric et al., "The matter of heartbleed", *Proc. Conf. Internet Meas. Conf.*, pp. 475-488, Nov. 2014.
- M. Carvalho, J. DeMott, R. Ford and D. A. Wheeler, "Heartbleed 101", *IEEE Secur. Privacy*, vol. 12, no. 4, pp. 63-67, Jul. 2014.
- T. A. Nidecki, The Heartbleed Bug—Old Bugs Die Hard, Oct. 2022, [online] Available: https://www.acunetix.com/blog/web-security-zone/heartbleed-bug/.
- D. E. Geer and P. Kamp, "Inviting more heartbleed", *IEEE Secur. Privacy*, vol. 12, no. 4, pp. 46-50, Jul. 2014.
- Z. Hu, P. Chen, M. Zhu and P. Liu, "A co-design adaptive defense scheme with bounded security damages against heartbleed-like attacks", *IEEE Trans. Inf. Forensics Security*, vol. 16, pp. 4691-4704, 2021

- J. Sigholm and E. Larsson, "Cyber vulnerability implantation revisited", *Proc. IEEE Mil. Commun. Conf. (MILCOM)*, pp. 464-469, Nov. 2021.

——, “An internet protocol packet delay variation estimator for reliable
[illegible]

- S. H. Fern, A. Amir, and S. N. Azemi, “Multi-class imbalanced classification problems in network attack detections,” in Proc. 6th Int. Conf. Electr., Control Comput. Eng. Cham, Switzerland: Springer, 2022, pp. 1057–1069.

- M. S. Milosevic and V. M. Ciric, “Extreme minority class detection in imbalanced data for network intrusion,” Comput. Secur., vol. 123, Dec. 2022, Art. no. 102940.

- D. Krishnan, “Detection of denial-of-service attacks using stacked LSTM networks,” in Proc. Data Analytics Manage. Singapore: Springer, 2022, pp. 229–239.

- A. Amodei, D. Capriglione, L. Ferrigno, G. Miele, G. Tomasso, and G. Cerro, “A rule-based approach for detecting heartbleed cyber attacks,” in Proc. IEEE Int. Symp. Meas. Netw. (MN), Jul. 2022, pp. 1–6.

- L. Angrisani, D. Capriglione, L. Ferrigno, and G. Miele, “A methodological approach for estimating protocol analyzer instrumental measurement uncertainty in packet jitter evaluation,” IEEE Trans. Instrum. Meas., vol. 61, no. 5, pp. 1405–1416, May 2012. 5502610 IEEE TRANSACTIONS ON INSTRUMENTATION AND MEASUREMENT, VOL. 72, 2023

- L. Angrisani, D. Capriglione, L. Ferrigno, and G. Miele, “An internet protocol packet delay variation estimator for reliable quality assessment of video-streaming services,” IEEE Trans. Instrum. Meas., vol. 62, no. 5, pp. 914–923, May 2013.

- L. Angrisani, D. Capriglione, L. Ferrigno, and G. Miele, “Internet protocol packet delay variation measurements in communication networks: How to evaluate measurement uncertainty?” Measurement, vol. 46, no. 7, pp. 2099–2109, Aug. 2013.

- L. Angrisani, E. Atteo, D. Capriglione, L. Ferrigno, and G. Miele, “An efficient experimental approach for the uncertainty estimation of QoS parameters in communication networks,” in Proc. IEEE Instrum. Meas. Technol. Conf., May 2010, pp. 1186–1191.

- D. Capriglione, G. Cerro, L. Ferrigno, and G. Miele, "How to quantify trust in your network emulator?" in Proc. Int. Conf. Wired/Wireless Internet Commun. Cham, Switzerland: Springer, 2018, pp. 171–182.

- D. Capriglione, G. Cerro, L. Ferrigno, and G. Miele, "The effect of hardware/software features on the performance of an open–source network emulator," in Proc. Int. Conf. Wired/Wireless Internet Commun. Cham, Switzerland: Springer, 2019, pp. 233–245.

- L. Angrisani, D. Capriglione, G. Cerro, L. Ferrigno, and G. Miele, "Experimental analysis of software network emulators in packet delay emulation," in Proc. IEEE Int. Workshop Meas. Netw. (MN), Sep. 2017, pp. 1–6.

- L. Angrisani, D. Capriglione, L. Ferrigno, and G. Miele, "Measurement of the IP packet delay variation for a reliable estimation of the mean opinion score in VoIP services," in Proc. IEEE Int. Instrum. Meas. Technol. Conf., May 2016, pp. 1–6.

- A. H. Lashkari, G. D. Gil, M. S. I. Mamun, and A. A. Ghorbani, "Characterization of tor traffic using time based features," in Proc. 3rd Int. Conf. Inf. Syst. Secur. Privacy, 2017, pp. 253–262.

- G. Draper-Gil, A. H. Lashkari, M. S. I. Mamun, and A. A. Ghorbani, "Characterization of encrypted and VPN traffic using time-related features," in Proc. 2nd Int. Conf. Inf. Syst. Secur. Privacy, 2016, pp. 407–414.