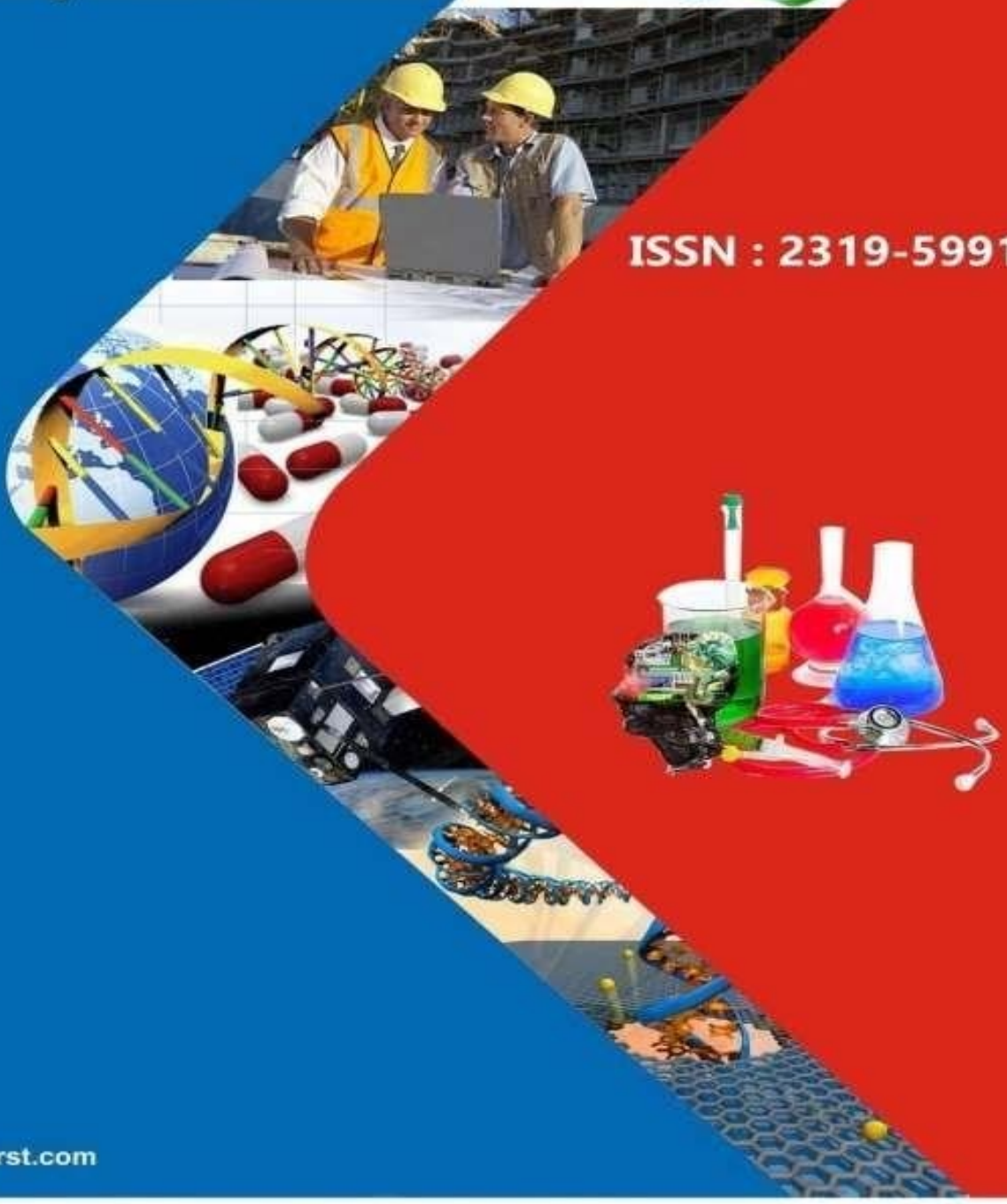
International Journal of Engineering Research and Science & Technology

IJERST

ISSN : 2319-5991



www.ijerst.com

Email: editor@ijerst.com or editor.ijerst@gmail.com

International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com

https://doi.org/10.62643/ijerst.2025.v21.i2.pp387-397

Vol. 21, Issue 2, 2025

AN ENHANCED MEASUREMENT APPROACH FOR INLINE DETECTION OF HEARTBLEED-STYLE ATTACKS IN IOT ENVIRONMENTS

[1] *Shaik Sohail Aman, MCA Student, Department of MCA*

[2] *B Purushotham, M.Tech, Assistant Professor, Department of MCA*

[12]*Dr KV Subba Reddy Institute of Technology, Dupadu, Kurnool*

ABSTRACT

One of the most important components of the Internet of Things (IoT) is cyber security. These days, a lot of attention is focused on the potential for external attacks to capture information from both the client and the server. The vulnerability of either the sensor nodes themselves (if they have the ability to network operationally) or the IoT gateways—devices that can establish a connection between the local nodes of the IoT network and the wide area networks—makes the involved nodes vulnerable to cyberattacks, regardless of the IoT application. The IoT sensor nodes and IoT gateways are frequently built on low performance processing units, often customised for the particular application, due to the low cost constraints common to many IoT applications. As a result, they are difficult to update against newly discovered cyberthreats. One of the most well-known cyberattacks focused on obtaining private data was the heart bleed, which gave hackers the ability to remotely access protected memory from between 24 and 55 percent of well-known HTTPS websites. A appropriate patch was promptly issued to address the issue, which was caused by an OpenSSL flaw. This allowed for the problem to be avoided in the majority of circumstances. However, since IoT devices can't always be patched for a variety of practical reasons, they could need more sophisticated mitigation strategies. The research suggests a unique measuring technique for inline detection of intrusions caused by heart bleed and heart bleed-like events in this situation. The suggested method is based on an efficient rule that can be used with a low-performance general-purpose processor and does not need decoding the payload. It is hence easily implementable and may be included into IoT gateways or sensor nodes. Several tests conducted on an actual network have verified and confirmed the implemented system, demonstrating performance that is on par with—and often even better than—that of the more complex machine learning-based techniques.

I. INTRODUCTION

OVERVIEW OF INTRODUCTION

Information security operation centres often use techniques for network security monitoring and measurements. Appropriate measurement probes are used to record network traffic, and the associated logs are tracked to identify any illicit activity occurring on the network [1], [2].

Intrusion Detection Systems (IDSs) are automated systems created especially to detect attacks that might harm information systems, such as data leaks, Distributed Denial of Service (DDOS), and Bad Data Injection, to name a few, in various application settings [3]–[7]. The Internet of Things (IOT) and operational technology (OT) infrastructure are the targets of recent trends in cyberattacks, which will increasingly target conventional industrial facilities, vital infrastructures, and even smart home networks in the coming years. It is anticipated that attackers will target industrial sensors to cause physical damage that could cause assembly lines to shut down or services to be interrupted because employees frequently

International Journal of Engineering Research and Science & Technology
ISSN 2319-5991 www.ijerst.com
https://doi.org/10.62643/ijerst.2025.v21.i2.pp387-397
Vol. 21, Issue 2, 2025

manage these systems remotely, which gives cybercriminals an excellent entry point [8].

The heart bleed vulnerability, one of the most well-known cyberattacks, caught the Internet off guard in April 2014 and gave hackers the ability to remotely access protected memory from between 24 and 55 percent of well-known HTTPS websites [9], [10]. The most widely used open-source cryptographic library that supports the SSL and TLS protocols, Open SSL, has a weakness that allowed for this kind of attack. Specifically, there was a flaw in the TLS Heartbeat Extension implementation that gave hackers direct access to sensitive information from servers and clients. Recent scientific and technical literature demonstrates how the issue of heartbleed still exists in many situations, despite the rapid release of a suitable patch to fix the vulnerability. This is because systems that failed to upgrade to the patched version of OpenSSL are still vulnerable to attacks. In actuality, patching any server or cloud platform ought to be rather simple. However, since they can't always be patched for practical reasons, Internet of Things (IOT) devices could need more sophisticated mitigation approaches. Furthermore, a customised version of the susceptible software is often used by some businesses. For instance, Open SSL is an open-source library, and some businesses may have altered it to suit their needs in the Heart Bleed scenario. A straight patch is not feasible in these situations; instead, the business must reinsert its unique code into the updated library version. This is often the cause of businesses delaying updates to their open-source software, even when serious new issues are discovered [11].

All of these factors, together with the fact that assaults that resemble heartbleeds may still be harmful, encourage more study into developing appropriate intrusion detection techniques that can recognise these types of attacks [12]–[18]. Furthermore, the literature review has shown that there are currently no intrusion detection systems (IDSs) that can detect heart bleed and heart bleed-like assaults inline. In most IOT application contexts, where devices and network systems are characterised by low costs and, consequently, low resources for data processing and storage, the applicability of such techniques is not always feasible. Generally, the majority of solutions for developing an IDS are based on Artificial Intelligence and Machine Learning approaches, which typically incur a significant computational burden [19]–[21].

The authors of this paper propose a novel measurement method for inline detection on low performance systems that can detect heartbleed-like attacks based on very simple and easy-to-implement rules. This is based on the preliminary results provided in [22] and on the prior experience in the fields of measurements systems for network performance analysis [23]–[31]. It is categorised as a network-based intrusion detection system and is developed utilising open-source software for data collection and processing and very inexpensive hardware. An appropriate experimental setup that can function in actual operational conditions has been created in order to assess the performance of the suggested system. The experimental characterisation conducted on a variety of real attacks and real standard data traffic types demonstrates excellent performance in terms of accurately identifying heartbleed-like attacks and differentiating them from standard traffic, thereby reducing the number of false alarms.

The remainder of the document is structured as follows: Section IV presents an example of the measurement method's implementation on a common low-performance system along with the experimental results

International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com

https://doi.org/10.62643/ijerst.2025.v21.i2.pp387-397

Vol. 21, Issue 2, 2025

obtained on a wide measurement campaign, allowing comparison of the suggested solutions with ML-based techniques; Section V discusses the potential extensions of the proposed methodology to wider networks; and, finally, Section VI draws conclusions. Section II offers a detailed analysis of heart bleed and heart bleed-like attacks. Section III describes the preliminary experimental analysis conducted for designing and tuning the proposed measurement method.

Project Purpose

This project aims to develop and evaluate a real-time, lightweight, measurement-based intrusion detection method specifically designed to detect Heartbleed and Heartbleed-like assaults in Internet of Things frameworks. Without the need for payload decoding or a significant amount of processing power, this method seeks to provide an inline, low-overhead security mechanism that may be installed straight into IoT devices and gateways with little resources. The research tackles the urgent need for workable, patch-independent security solutions in susceptible IoT contexts by using a rule-based detection technique that is compatible with low-performance general-purpose processing units. Experiments on actual networks show how successful the suggested solution is and how competitive it is when compared to more conventional machine learning-based techniques.

II. LITERATURE SURVEY

D. A. Kumar and S. Venugopalan, "Intrusion Detection Systems: a Review," International Journal of Advanced Research in Computer Science, vol. 8, no. 8, 2017.

The significance of secure networks has grown significantly, and intrusion detection has emerged as a crucial element of information security due to the Internet's exponential expansion and expanded bandwidth availability. Although James Anderson J. P. first proposed the idea of intrusion detection in 1980, it has become more significant in recent years due to recent assaults on IT infrastructure. This study's primary goals are to review the literature on different approaches to intrusion detection, especially anomaly detection, analyse their conceptual underpinnings, classify intrusion detection systems (IDS), and create an easily comprehensible morphological framework for IDS. This paper presents a thorough overview of IDS from its inception, including its evolution, architectures, and constituent parts.

Y. Li and Q. Liu, "A comprehensive review study of cyber–attacks and cyber security; Emerging trends and recent developments," Energy Reports, vol. 7, pp. 8176–8186, 2021.

The majority of nations' economic, commercial, cultural, social, and governmental contacts and activities now take place online, including people, non-governmental organisations, and governmental agencies. Many government agencies and commercial businesses worldwide are now dealing with the threat of wireless communication technology and the issue of cyberattacks. The modern society is heavily reliant on electronic technology, making it difficult to safeguard this data against cyberattacks. The goal of cyberattacks is to cause financial damage to businesses. In other situations, cyberattacks may be carried out for political or military objectives. PC infections, knowledge breaches, data distribution services (DDS), and other attack vectors are a few examples of these harms. In order to mitigate the harm that cyberattacks might do, different organisations use different strategies. Cyber security keeps up with the most recent IT data in real time. Researchers from all around the globe have so far put out a number of strategies to stop cyberattacks or lessen the harm they inflict.

International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com

https://doi.org/10.62643/ijerst.2025.v21.i2.pp387-397

Vol. 21, Issue 2, 2025

While some of the approaches are at the research stage, others are in the operational stage. In addition to examining the difficulties, shortcomings, and advantages of the suggested approaches, the study's objective is to examine and thoroughly analyse the standard advancements made in the area of cyber security. A variety of novel descendent assault types are thoroughly examined. The history of early-generation cyber-security techniques are explored together with standard security frameworks. Furthermore, new advances and trends in cyber security are discussed, along with security risks and difficulties. The thorough review study offered to IT and cyber security experts is anticipated to be beneficial.

A. Chidukwani, S. Zander, and P. Koutsakis, "A Survey on the Cyber Security of Small-to-Medium Businesses: Challenges, Research Focus and Recommendations

SMBs make up a significant portion of the economy of many nations, but research indicates that they are not putting cyber security into practice enough, making them vulnerable to cyberattacks. Furthermore, although making up a significant fraction of enterprises, SMBs are seldom the subject of cyber security study. This study examines current research on SMB cyber security, emphasising how it aligns with the widely used NIST Cyber Security Framework (CSF). We also highlight the main obstacles SMBs have when putting strong cyber security into practice, drawing on the literature, and close with important suggestions. We discover that the majority of SMB cyber security research is qualitative in nature and primarily focusses on the NIST CSF's Identify and Protect functions, with very little attention paid to the other functions that are already in place. SMBs should be able to recognise, react to, and recover from cyberattacks; if there is a dearth of research in these areas, they may not have much direction on how to proceed. Future studies on SMB cyber security should be more balanced, and researchers should use proven, effective quantitative research techniques to evaluate and improve their findings. At the same time, governments and academic institutions should provide incentives for researchers to broaden their areas of study.

A. Huseinovi´c, S. Mrdovi´c, K. Bicakci, and S. Uludag, "A survey of denial-of-service attacks and solutions in the smart grid

The Smart Grid has been receiving increased attention as a result of the growing breadth, size, and severity of actual and prospective assaults. The accessibility and availability of electricity as well as associated information and communications infrastructures are key concerns of Smart Grid cybersecurity initiatives. We overuse the term Denial-of-Service (DoS) to describe these Smart Grid assaults. In order to encourage more focused and coordinated study into this field—the absence of which might have serious repercussions—we provide the DoS attack taxonomy in this work in a comprehensive and logical manner, along with a review of possible remedy approaches. To the best of our knowledge, there isn't a thorough survey research of DoS assaults and Smart Grid solutions in the literature. Index terms include cybersecurity, smart grid security, and denial-of-service assaults.

Z. Durumeric, F. Li, J. Kasten, J. Amann, J. Beekman, M. Payer, N. Weaver, D. Adrian, V. Paxson, M. Bailey et al., "The matter of heartbleed," in Proceedings of the 2014 conference on internet measurement conference, 2014, pp. 475–488.

From identifying broad flaws in random number generators to monitoring the changing effects of Heartbleed, rapid Internet-wide scanning has created new opportunities for security research. But even basic questions like "What models of

International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com

https://doi.org/10.62643/ijerst.2025.v21.i2.pp387-397

Vol. 21, Issue 2, 2025

embedded devices prefer CBC cyphers?" still require a lot of work: creating an application scanner, manually identifying and tagging devices, negotiating with network administrators, and handling abuse complaints are all necessary. In this work, we provide Censys, a publicly available search engine and data processing facility supported by information gathered from continuous scans of the whole Internet. Censys, which provides full-text searches on protocol banners and querying a variety of derived fields (e.g., 443.https.cipher), was created to assist researchers in finding answers to security-related queries. It may provide statistical data on general use patterns and trends in addition to identifying particular susceptible devices and networks. Censys significantly reduces the work required to comprehend the hosts that make up the Internet by returning these findings in less than a second. We describe the design of the search engine and assess its performance empirically. We also examine the uses of Censys and demonstrate how current research' queries may be easily answered.

III. SYSTEM ANALYSIS AND DESIGN

EXISTING SYSTEM

—The internet of things (IoT) is a group of common physical objects that can connect to the internet and use network infrastructure to communicate and synthesise data. As IoT networks gain popularity, they become more susceptible to security breaches. One of the most common and serious threats to IoT security is cyberattacks. Improving the security of IoT devices is attracting the attention of more and more researchers. To improve security capabilities, machine learning (ML) techniques were used to operate as intrusion detection systems (IDSs). This study suggested a unique machine learning-based distributed detection system to identify IoT threats and stop harmful events.

Additionally, the vast bulk of recent research uses the NSL-KDD or KDD-CUP99 datasets. New attacks have not been added to these databases. Consequently, training and testing were conducted using the ToN-IoT dataset. It was developed from a vast, heterogeneous Internet of Things network. The ToN-IoT dataset includes information from the cloud, fog, and edge layers, among other IoT system layers. Every distinct ToN-IoT dataset division was used to evaluate different machine learning techniques. The recommended model is the first one based on data gathered from all levels of the same IoT system. Features in a network dataset were selected using the Chi2 approach. It lowered the feature count to 20.

The correlation matrix, which was used to extract the most relevant characteristics from the whole dataset, was another feature selection approach utilised in the Windows dataset. The SMOTE technique was used to balance the classes. Several machine learning techniques are tested in this work for both binary and multi-class classification issues. The results show that for every node in the proposed model, the XGBoost method outperforms alternative ML techniques.

Disadvantages

- Because there aren't any heart-attacked attacks, the system doesn't detect data leaks.
- Rule-based methodology for supporting machine learning algorithms is not implemented by the system.

PROPOSED SYSTEM

The authors of this paper propose a novel measurement method for inline detection on low performance systems that can detect heartbleed-like attacks based on very simple and easy-to-implement rules. This is based on the

International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com

https://doi.org/10.62643/ijerst.2025.v21.i2.pp387-397

Vol. 21, Issue 2, 2025

preliminary results provided in [22] and on the prior experience in the fields of measurements systems for network performance analysis [23]–[31].

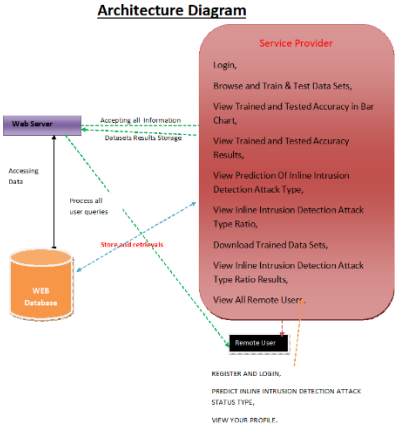
It is categorised as a network-based intrusion detection system and is developed utilising open-source software for data collection and processing and very inexpensive hardware. An appropriate experimental setup that can function in actual operational conditions has been created in order to assess the performance of the suggested system. The experimental characterisation conducted on a variety of real attacks and real standard data traffic types demonstrates excellent performance in terms of accurately identifying heartbleed-like attacks and differentiating them from standard traffic, thereby reducing the number of false alarms.

Advantages

• Full Packet Capture (PCAP) makes it possible to get comprehensive details about network packets, including protocol, flags, size, and headers. Furthermore, the packet payload holding sensitive or private information may potentially be read.

• In contrast to the previously described approach, netflow offers a measurement of certain parameters pertaining to every flow. The number of packets sent and received in both ways, the amount of bytes transferred during a flow, and the resulting parameters (such as average, standard deviation, and variance) are examples of measurements.

SYSTEM ARCHITECTURE



IV. IMPLEMENTATION

Modules

Service Provider

The Service Provider must use a working user name and password to log in to this module. He can do many tasks after successfully logging in, including browsing and training and testing data sets. View Results of Trained and Tested Accuracy, View Trained and Tested Accuracy in Bar Chart, See the Inline Intrusion Detection Attack Type Prediction, View the Inline Intrusion Detection Attack Type Ratio, Get Trained Data Sets here. See the results of the Inline Intrusion Detection Attack Type Ratio. See Every Remote User.

View and Authorize Users

The administrator may see a list of all registered users in this module. Here, the administrator may see the user's information, like name, email, and address, and they can also grant the user permissions.

Remote User

A total of n users are present in this module. Before beginning any actions, the user needs register. Following registration, the user's information will be entered into the database. Following a successful registration, he must use his password and authorised user name to log in. Following a successful login, the user may do tasks including registering and logging in,

International Journal of Engineering Research and Science & Technology
ISSN 2319-5991 www.ijerst.com
https://doi.org/10.62643/ijerst.2025.v21.i2.pp387-397
Vol. 21, Issue 2, 2025

predicting the kind of intrusion detection attack, and seeing their profile.

ALGORITHIMS

RANDOM FOREST

Random forests, also known as random decision forests, are ensemble learning techniques that build a large number of decision trees during training for tasks like regression and classification. The class chosen by the majority of trees is the random forest's output for classification problems. The mean or average forecast of each individual tree is given back for regression tasks. The tendency of decision trees to overfit to their training set is compensated for by random decision forests. Although random forests are less accurate than gradient enhanced trees, they often perform better than choice trees. However, their performance may be impacted by data peculiarities.

Tin Kam Ho[1] developed the first algorithm for random decision forests in 1995 by using the random subspace technique, which in Ho's definition is a means of putting Eugene Kleinberg's "stochastic discrimination" approach to classification into practice.

Leo Breiman and Adele Cutler created an algorithm extension and filed for a trademark in 2006 for "Random Forests" (owned by Minitab, Inc. as of 2019). The extension builds a set of decision trees with controlled variance by combining Breiman's "bagging" concept with random feature selection, which was initially proposed by Ho[1] and then separately by Amit and Geman[13].

Businesses often employ random forests as "blackbox" models since they need minimal setup and provide accurate forecasts across a variety of inputs.

SVM

The goal of a discriminant machine learning approach in classification problems is to identify a discriminant function that can accurately predict labels for newly acquired instances based on an independent and identically distributed (iid) training dataset. A discriminant classification function takes a data point x and assigns it to one of the several classes that are part of the classification job, in contrast to generative machine learning techniques that call for calculations of conditional probability distributions. Discriminant techniques are less effective than generative approaches, which are mostly used when prediction entails the identification of outliers. However, they need less training data and processing resources, particularly when dealing with a multidimensional feature space and when just posterior probabilities are required. Finding the equation for a multidimensional surface that optimally divides the various classes in the feature space is the geometric equivalent of learning a classifier.

SVM is a discriminant approach that, unlike genetic algorithms (GAs) or perceptrons, which are both often used for classification in machine learning, always returns the same optimum hyperplane value since it solves the convex optimisation issue analytically. The initialisation and termination criteria have a significant impact on the solutions for perceptrons. While the perceptron and GA classifier models are distinct every time training is started, training yields uniquely specified SVM model parameters for a given training set for a certain kernel that converts the data from the input space to the feature space. The only goal of GAs and perceptrons is to reduce training error, which will result in several hyperplanes satisfying this criterion.

NAÏVE BAYES

The naive bayes approach is a supervised learning technique that is predicated on the straightforward premise that a class's existence

International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com

https://doi.org/10.62643/ijerst.2025.v21.i2.pp387-397

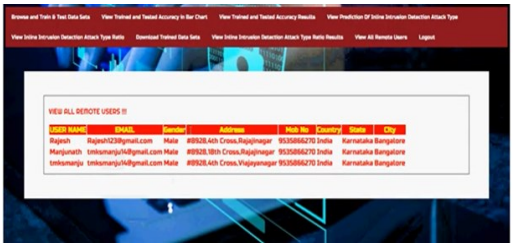
Vol. 21, Issue 2, 2025

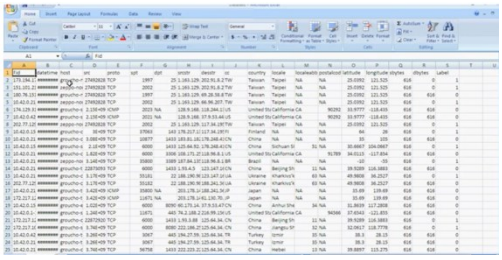
(or lack) of a specific feature has no bearing on the presence (or lack) of any other feature.

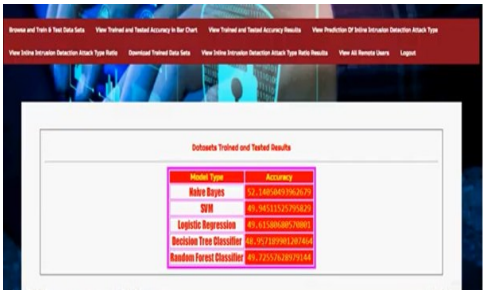
However, it seems sturdy and effective in spite of this. It performs similarly to other methods of guided learning. Numerous explanations have been put forward in the literature. We emphasise a representation bias-based explanation in this lesson. Along with logistic regression, linear discriminant analysis, and linear SVM (support vector machine), the naive bayes classifier is a linear classifier. The technique used to estimate the classifier's parameters (the learning bias) makes a difference.

Although the Naive Bayes classifier is commonly used in research, practitioners who want to get findings that are useful do not utilise it as often. On the one hand, the researchers discovered that it is very simple to build and apply, that estimating its parameters is simple, that learning occurs quickly even on extremely big datasets, and that, when compared to other methods, its accuracy is rather excellent. The end users, however, do not comprehend the value of such a strategy and do not get a model that is simple to read and implement.

As a consequence, we display the learning process's outcomes in a fresh way. Both the deployment and comprehension of the classifier are simplified. We discuss several theoretical facets of the naive bayes classifier in the first section of this lesson. Next, we use Tanagra to apply the method on a dataset. We contrast the outcomes (the model's parameters) with those from other linear techniques including logistic regression, linear discriminant analysis, and linear support vector machines. We see that the outcomes are quite consistent.







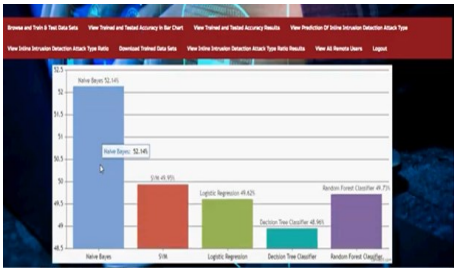
V. SCREEN SHOTS

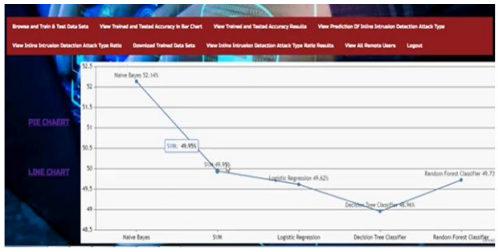
International Journal of Engineering Research and Science & Technology

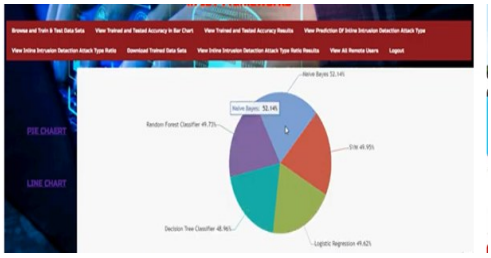
ISSN 2319-5991 www.ijerst.com

https://doi.org/10.62643/ijerst.2025.v21.i2.pp387-397

Vol. 21, Issue 2, 2025







VI. CONCLUSION

In the framework of IOT applications, cyber attacks represent a significant threat to developers of systems and applications. Indeed, the typical application constraints of low-cost, low-powerful architecture, and, at the same time, the required networking operativity make such systems intrinsically vulnerable to cyber criminals. Moreover, the use of low-powerful platforms for developing IOT sensor nodes or IOT gate ways, often makes it impossible to update the systems with suitable patches for correcting the frequently identified vulnerabilities.

Therefore, among data leakage attacks, Heart bleed and Heart bleed-like still represent significant threats to IOT applications. In this context, the paper has presented a novel and rule-based measurement method that can be developed on low cost platforms for inline detecting the presence of such kinds of cyber attacks. The low complexity of the proposed solution makes it directly implementable on IOT gateways and allows well-discriminating malicious traffic from the benign one (that could involve an IOT sensor node belonging to the IOT gateway segment).

International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com

https://doi.org/10.62643/ijerst.2025.v21.i2.pp387-397

Vol. 21, Issue 2, 2025

In particular, the implementation of the proposed method on a very popular platform (i.e. Rasp berry TM Pi 4), has proved that, compared with solutions based on popular ML-based techniques, the proposed solution keeps similar performance (in several cases also better) in terms of the typical figures of merit adopted in the context of IDSs, but, due to the lowest complexity, it requires very lower execution times and memory requirements. These features become particularly attractive, looking at the long-term goal of the research activity of developing an IDS able to detect several kinds of attacks.

Indeed, future developments will extend the proposed method to further kinds of cyber attacks typically affecting IOT applications, like DDOS and Bad Data Injection.

REFERENCES

[1] D. A. Kumar and S. Venugopalan, "Intrusion Detection Systems: a Review," International Journal of Advanced Research in Computer Science, vol. 8, no. 8, 2017.

[2] K. Yu, K. Nguyen, and Y. Park, "Flexible and Robust Real–Time Intrusion Detection Systems to Network Dynamics," IEEE Access, vol. 10, pp. 98 959–98 969, 2022.

[3] Y. Li and Q. Liu, "A comprehensive review study of cyber–attacks and cyber security; Emerging trends and recent developments," Energy Reports, vol. 7, pp. 8176–8186, 2021.

[4] H. Sarjan, A. Ameli, and M. Ghafouri, "Cyber–Security of Industrial Internet of Things in Electric Power Systems," IEEE Access, vol. 10, pp. 92 390–92 409, 2022.

[5] 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. 85 701–85 719, 2022.

[6] A. Huseinovi´c, S. Mrdovi´c, K. Bicakci, and S. Uludag, "A survey of denial-of-service attacks and solutions in the smart grid," IEEE Access, vol. 8, pp. 177 447–177 470, 2020.

[7] G. Bernieri, M. Conti, and F. Pascucci, "A Novel Architecture for Cyber-Physical Security in Industrial Control Networks," 2018 IEEE 4th International Forum on Research and Technology for Society and Industry (RTSI), pp. 1–6, 2018.

[8] N. Weinberg, "7 hot cybersecurity trends (and 2 going cold)," accessed on 2022-10-24. [Online]. Available: https://www.csoonline.com/article/ 3262972/7-hot-cybersecurity-trends-and-2-going-cold.html

[9] Z. Durumeric, F. Li, J. Kasten, J. Amann, J. Beekman, M. Payer, N. Weaver, D. Adrian, V. Paxson, M. Bailey et al., "The matter of heartbleed," in Proceedings of the 2014 conference on internet measurement conference, 2014, pp. 475–488.

[10] M. T. M. Carvalho, J. D. DeMott, R. A. Ford, and D. A. Wheeler, "Heartbleed 101," IEEE Security & Privacy, vol. 12, pp. 63–67, 2014.

[11] T. A. Nidecki, "The Heartbleed Bug – Old Bugs Die Hard," accessed on 2022-10-24. [Online]. Available: https://www.acunetix.com/blog/ web-security-zone/heartbleed-bug/

[12] D. E. Geer and P.-H. Kamp, "Inviting More Heartbleed," IEEE Security & Privacy, vol. 12, no. 04, pp. 46–50, 2014.

[13] Z. Hu, P. Chen, M. Zhu, and P. Liu, "A co–design adaptive defense scheme with bounded security damages against Heartbleed–like attacks," IEEE Transactions on Information Forensics and Security, vol. 16, pp. 4691–4704, 2021.

[14] Y. Wang, H. Wang, X. Hei, W. Ji, and L. Zhu, "Petri net modeling and vulnerability analysis of the Heartbleed," in 2021 International Conference on Networking and

International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com

https://doi.org/10.62643/ijerst.2025.v21.i2.pp387-397

Vol. 21, Issue 2, 2025

Network Applications (NaNA). IEEE, 2021, pp. 155–160.

[15] J. Sigholm and E. Larsson, "Cyber Vulnerability Implantation Revisited," in MILCOM 2021-2021 IEEE Military Communications Conference (MILCOM). IEEE, 2021, pp. 464–469.

[16] M. Kherbache, K. Amroun, and D. Espes, "A new wrapper feature selection model for anomaly-based intrusion detection systems," International Journal of Security and Networks, vol. 17, no. 2, pp. 107–123, 2022.

[17] R. Panigrahi, S. Borah, M. Pramanik, A. K. Bhoi, P. Barsocchi, S. R. Nayak, and W. Alnumay, "Intrusion detection in cyber–physical environment using hybrid Na¨ıve Bayes—-Decision table and multi-objective evolutionary feature selection," Computer Communications, vol. 188, pp.
133–144, 2022.

[18] M. Madou, "Now is the time to strengthen cyber defences," Network Security, vol. 2022, no. 8, 2022.

[19] S. H. Fern, A. Amir, and S. N. Azemi, "Multi–class Imbalanced Classification Problems in Network Attack Detections," in Proceedings of the 6th International Conference on Electrical, Control and Computer Engineering. Springer, 2022, pp. 1057–1069.

[20] M. S. Milosevic and V. M. Ciric, "Extreme minority class detection in imbalanced data for network intrusion," Computers & Security, p. 102940, 2022.

[21] D. Krishnan, "Detection of Denial-of-Service Attacks Using Stacked LSTM Networks," in Proceedings of Data Analytics and Management. Springer, 2022, pp. 229–239.

[22] A. Amodei, D. Capriglione, L. Ferrigno, G. Miele, G. Tomasso, and G. Cerro, "A rule–based approach for detecting heartbleed cyber attacks," in 2022 IEEE International Symposium on Measurements & Networking (M&N). IEEE, 2022, pp. 1–6.

[23] L. Angrisani, D. Capriglione, L. Ferrigno, and G. Miele, "A methodological approach for estimating protocol analyzer instrumental measurement uncertainty in packet jitter evaluation," IEEE Transactions on Instrumentation and Measurement, vol. 61, no. 5, pp. 1405–1416, 2012.

[24] ——, "An internet protocol packet delay variation estimator for reliable quality assessment of video-streaming services," IEEE Transactions on Instrumentation and Measurement, vol. 62, no. 5, pp. 914–923, 2013.

[25] ——, "A methodological approach for estimating protocol analyzer instrumental measurement uncertainty in packet jitter evaluation," IEEE Transactions on Instrumentation and Measurement, vol. 61, no. 5, pp. 1405–1416, 2012.