Webology (ISSN: 1735-188X)
Volume 13, Number 2, 2016

Detection Of Cyber Vulnerability Using AI

N.K SINGH

Department of computer science ,BIT Mesra.

Abstract: In an era characterized by rapid digitalization, the security of digital systems and networks has become a paramount concern. This research delves into the innovative utilization of Artificial Intelligence (AI) for the identification and detection of cyber vulnerabilities. Focusing on the ever-evolving landscape of cybersecurity, this study examines the potential of AI algorithms, machine learning, and data analytics in identifying vulnerabilities before they can be exploited by malicious actors. By analyzing patterns, anomalies, and historical data, AI-driven approaches provide a proactive and adaptive framework for cyber vulnerability detection. Through a thorough exploration of AI methodologies, real-world case studies, and empirical analyses, this research sheds light on the efficacy, challenges, and ethical implications associated with employing AI in cyber vulnerability detection. The findings contribute to a deeper understanding of the transformative role AI can play in fortifying digital defenses and mitigating emerging cyber threats.

I. INTRODUCTION

Because of the improvement of gizmos the usage of wireless community, it's develop to become hard to find a region with out there Wi Fi inside the lives of ours. Wi Fi is readily being had around cafes, army facilities, companies, public institutions and colleges. Wi Fi is employed by a number of unspecified clients, which makes it difficult to check everybody. As well as if you're tethering such as a hotspot the use of genuine Wi Fi, identity is difficult unless you look with no hold off on the Access Point listing as well as examine the adjustments carefully [1].An entry issue is a station which will get and also sends the information. It's called transceiver. An entry issue links buyers to various clients within the local community and in addition can certainly work the aspect of interconnection with the WLAN along with a fixed cable group Because of the expansion found utilization of wise devices the way of lives of illegitimate AP has develop to become inescapable. Consumption is in addition except the stage as generally there are not anyt some rules or provisions in connection with illegitimate AP along side hotspots along with Wi Fi within places that are public. The local community could be smoothly damaged with utilizing gleaming information of various buyers who may have generate entry to to illegitimate APs. Pcs likewise can certainly be smoothly hacked [two]. In the event that a generate entry to element is undiscovered it might be a receptive doorstep to sensitive information within the local community. Businesses, government, Industries, navy offerings as well as academia desires to become conscious around the hazard of unauthorized AP's as well as market con- temporary working day detection methods. Information raiders inside companies today not any greater the time easiest obtain unfastened online end up getting entry to however likewisecan certainly look at the personal information. Investigation to find log AP as well as its risks were definitely definitely analyzed till not too long ago. A variety of methods of scientific research are presently internal enhancement dealing with a lot of areas of the difficulty for that reason one might prevent the damage, it actually is lengthy ranges important to find out what AP is an unlawful AP [3] [8]. Tests on several algorithms are needed to perceive this particular with too much precision. With this task, a dataset is produced the use of RTT (Round Trip Time) values. The dataset is carried through with the method mastering algorithms to reach the consequences as well as check for his or maybe the accuracies of her. Then they are as

in comparison to appear that's very correct. Dealing with differentfacets of the problem to be able to stop these harm, it's essential to determine what AP is an unlawful AP [3] [8]. Tests on numerous algorithms are required to recognize this particular with top accuracy.

In this project, a dataset is constructed with RTT (Round Trip Time) values. The dataset is used towards the machine learning algorithms to get the end result as well as examine for the accuracies of theirs. Then they're when compared seeing and that is a lot more precise.

II. WORKING:

The design of legitimate and ill-conceived AP is demon- strated in Figures 1 and 2. The legal access point is configured in this kind of manner that the tool the usage of its community is hooked up to it through receiving radio alerts at once from the get admission to factor. For legal Wi-Fi identity may be very plenty hard unless you appearance at once on the related to a actual AP. A valid AP is configured in this kind of manner that the tool the usage of its community is hooked up to it through accepting the radio sign of the AP. Whereas illegitimate AP is configured in this kind of manner that every other AP accepts the sign of the prevailing AP and constructs a brand new AP to which the person gadgets are related

Fig. 1. Legitimate AP

Fig. 2. Illegitimate AP

Because of the relay Access Point condition as verified in Fig two, the RTT difference together with the legitimate AP takes place. Of all the documents which struck upon AP the use of difference of these RTT values, Han's method [two] is using the straightness on the immediately type via method of ways of the use on the difference of Fashionable deviation and rtt price selling price. These're completed with the information division as well as categorized. With this check the as well as values of linear formulas for sort are not shown to be bendy via method of ways of the use of frequent constants. Various algorithms are performed for kind of rogue APs in unplanned situations.[9] [ten] As a means of functionality option for RTT values, variance, mean, the distinction, and trendy deviation of delay cases of every illegitimate and valid AP's are utilized [eleven]. Algorithm analysis related to illegitimate AP detection can be found Research goals to develop a pair of guidelines as well as utilize it to perceive the malicious wi fi networks [twelve]. With this newspaper, the check is carried out via method of way of employing onthe machine learning group of guidelines, with out there making its own detection group of guidelines. Then via method of way of verifying the end result, it's proved the method for identity of illegitimate AP through the demonstrated group of guidelines might be variously and effortlessly carried through. The device mastering algorithms worn are SVM (Support Vector Machine), KNN (K nearest neighbor's) as well as Decision Tree classifier. SYSTEM CONFIGURATION AND DATASET EXTRACTION

For detection of illegitimate AP, we have developed a "Intelligent Wireless AP Detection System" as verified within Figure3. Information is gathered as a result of the illegitimate and valid AP's as well as made as information sets. Information sets are examined via method of way of implementing machine mastering

algorithms combined with SVM (Support Vector Machine), KNN (K Nearest Neighbors), and also Decision tree classifier. The machine studying algorithms employed:

1) SVM (support vector machine): Determined by a certain group of specifics, we develop a non probabilistic binary linear category design which decides what classifications of newest files have to become harmed printed and also accustomed to symbolize limits within the distance whereby specifics is mapped. The SVM algorithm un- covers the boundary with the most crucial width.
2) KNN (k nearest neighbor's algorithm): As a sort of chart item is given towards the optimum not uncommon area product learning, the get into consists of the knearest education details within the characteristic area, of course, if useful for category applications, the item is assigned to the maximum not uncommon place product the majority of the k nearest friends and neighbors and also categorised via method of way of greater part vote.
3) Decision tree classifier: Decision tree creates kind or maybe regression designs withinside the form of a tree building. It breaks bad an information established into smaller sized as well as smaller sized subsets even while during the the exact same period a connected choice tree is incrementally developed. The final result is a tree with choice nodes as well as leaf nodes. A choice node has or perhaps additional limbs. Leaf node belongs to acategory or even choice.

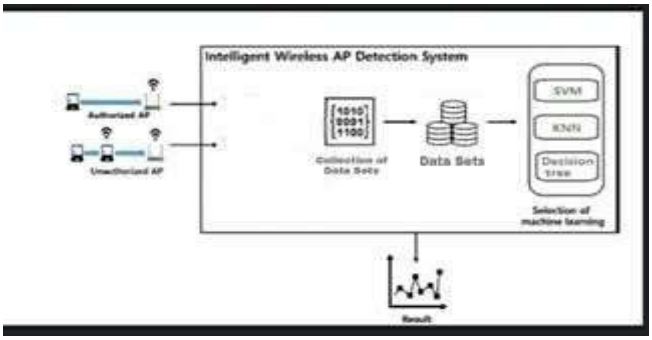

Fig. 3. Intelligent Wireless AP Detection System

Traits of informational index are demonstrated in Figure 4. The deliberate worth of RTT test (RTT to real AP), RTT DNS (RTT to DNS), RTT DNS - RTT probe,variance and standard deviation are utilized as trademark esteems to sort the information.

Mean probe	Mean DNS	Variance probe	Variance DNS	standard deviation probe	standard deviation DNS	Mean probe -Mean DNS
11	4	98	38	9.899465	6.164414	-7
11	4	0	96	0	9.797959	-7
				. . . .		
1	1	1	5	1	2.236068	0

Fig. 4. Attributes of data set

II. RESULT ANALYSIS

The calculations to be as analyzed had been settled on from the characterization - related calculations the vast majority of the AI calculations. The calculations are SVM (Support Vector Machine), KNN (K closest neighbors) and Decision tree classifier. The exploratory impacts for each class set of rules are demonstrated

in the underneath figure. After evaluating the experimental results, it could be concluded that Decision Tree classifier indicates maximum accuracy. They have much less mistakess charge and are less complicated in comparison to KNN and SVM. The understanding in Decision tree is represented in the shape of IF- THEN rules. It is less complicated for human beings to understand.

In this paper, decision tree classifier is used to discover the legitimate and illegitimate AP's for the given dataset

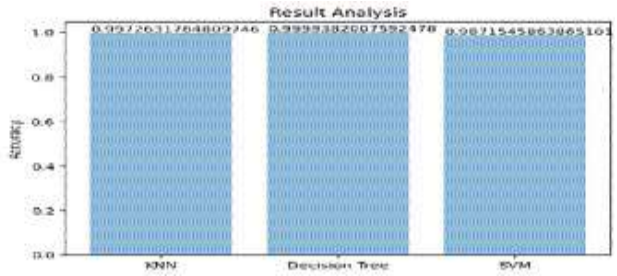

Fig. 5. Bar plot of Accuracy Scores of different algorithms used

III. CONCLUSION

In this paper, we confirmed how the legitimate and ille- gitimate APs may be categorised through machine learning algorithms. We can protect the structures if we discover the assaults from illegitimate AP's. The techniques on this paper may be carried out for the safety of information, which incorporates lifelong. As a destiny research, we will layout the safety scheme of a person's lifelong which is accumulated from clever gadgets and analyzed the usage of intelligent algorithms.

IV. FUTURE SCOPE

Our project detection of illegitimate access point using machine learning for data safety method is aimed at classifying the legitimate and illegitimate access points in a network. For this we've got used three machine learning algorithms and checked the overall performance contrast among those three algorithms. For enhancement of the project there may be a scope to apply Artificial neural networks that could boom the overall performance of the version similarly mode. It can provide the better effects whilst there may be a massive dataset.

VI. REFERENCES

[1]S. Jana and S.K. Kasera. "On fast and accurate detection of unauthorized wireless access points using clock skews," IEEE Transactions on Mobile Computing, Vol. 9, No. 3, pp. 449-462, 2010.

[2]H.Han, et al. "A timing-based scheme for rogue AP detection," IEEE Transactions on parallel and distributed Systems, Vol. 22,No.11, pp. 1912-1925, 2011.

[3]F. Awad, M. Al-Refai, and A. Al-Qerem. "Rogue access point localiza- tion using particle swarm optimization," in 8th International Conference on Information and Communication Systems (ICICS), Irbid, Jordan.May 2017. doi: 10.1109/IACS.2017.7921985

[4]S. Liu, Y. Liu, and Z. Jin. "Attack behavioural analysis and se- cure access for wireless Access Point (AP) in open system authen- tication," in 13th International Wireless Communications and Mobile Computing Conference (IWCMC), Valencia, Spain,June 2017. doi: 10.1109/IWCMC.2017.7986377