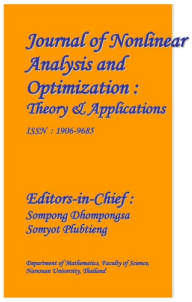
Journal of **N**onlinear **A**nalysis and **O**ptimization
Vol. 15, Issue. 1 : 2024
ISSN :**1906-9685**



CYBER SECURITY OF MOBILE APPLICATION USING ARTIFICIAL INTELLIGENCE

TADIPATRI ENGINERING COLLEGE
COMPUTER SCIENCE ENGINEERING

Munnuru Kundana, Pola Chandrika, V.Divyasree, Pommala Ganesh, Sepoori Nagaraju
MR.K. MANIKANTA, ASST.PROFF

ABSTRACT-With the development of wireless communications, many protection threats have arisen on the Internet. Intrusion detection systems (IDS) assist detect attacks on computers and discover attackers. In the beyond, IDSs used diverse device mastering techniques to enhance the adversary detection outcomes and improve the accuracy of the IDSs. This paper proposes an approach to put in force IDS using Principal Component Analysis (PCA) and Random Forest category algorithm. PCA facilitates in organizing the records units via decreasing the dimensionality of the statistics and the random jumps assist within the type. The outcomes received show that the proposed method is extra efficient in terms of accuracy as compared to different strategies including Naive Bayes and Decision Tree.

Keywords: artificial intelligence, clever sellers, cyber security, neural networks, expert systems.

INTRODUCTION

Attempting to infiltrate or make the most a laptop device. Intrusion is any interest that compromises the integrity, confidentiality and availability of any information or laptop gadget. An attacker exploits a weakness or flaw inside the machine's structure by bypassing the authentication or authorization system. With the fast boom of network services and information security at the network, community security has come to be greater essential than ever. The option to this hassle is to use Network Intrusion Detection Systems (NIDS) to hit upon attacks by monitoring diverse network activities. Therefore, it's miles important for such structures to be very correct in detecting assaults, to learn speedy and to generate as few false positives as possible. Intrusion detection systems (IDS) assist maintain your community secure through identifying malicious intrusions. Thus, IDS has emerge as an crucial part of

laptop networks. Two necessities for IDS are responsibility and efficiency. Security is at the pinnacle of all plans to save you any loss. An critical characteristic of an IDS is to offer visibility into unusual hobby after which inform network administrators of signals/warnings and/or block suspicious connections. In addition, an IDS must distinguish between attacks from within the company (from employees, clients or in any other case) and external assaults (assaults accomplished through hackers). Common styles of intrusion detection structures (IDS) are community IDS and host-based totally IDS (HIDS). In network IDS, it attempts to pick out illegitimate, illegal and anomalous behavior based totally on community site visitors.

OBJECTIVE AND PROBLEMSTATEMENT

This paper proposes a method to enforce IDS using Principal Component Analysis (PCA) and Random Forest class algorithm. PCA facilitates in organizing the data units via lowering the dimensionality of the data and the random jumps assist in the type.

LITERATURE SURVEY

1) Wireless Intrusion Detection, Net Interception and Gadget Assault Functions.

Author: Jaafar Abo Nada; Mohammed Razmi Al Moussa

This e mail report is a "living" template and already defines the factors of your article (name, text, identify, and so on.) within the fashion sheet. With the speedy deployment of Wi-Fi networks, the concept of community security has confronted many risks. Therefore, it need to provide security solutions. Traditional techniques of defensive networks from assaults are now not sufficient. For example, an intrusion detection device that works on stressed networks turns into useless on Wi-Fi networks. New wireless technology have opened up a realm for network users. Due to its ease of use and shape, this technique is gaining recognition and converting hastily. But the most important worry and fear of the consequences in the international of chocolate. This applies to the characters of this get dressed. With developing issues, it is vital to begin thinking about protection answers. This paper proposes a new wireless network intrusion and attack prevention gadget to enhance community security. Therefore, this text will talk the improvement of a Wi-Fi intrusion detection gadget referred to as "WIDPAS". It is primarily based on 3 major capabilities: tracking, analysis and protection. Monitors denial-of-carrier assaults or malicious networks, detects attacks, identifies attackers, and protects network customers.

2) Classification Of Attack Kinds For Intrusion Detection Structures The Usage Of Device Mastering Algorithms.

Author: Keenam Park; Song of Youth; Yoon-Kyung Chong

In this paper, we present the results of our experiments to assess the detection of different sorts of assaults (e.g., IDS, malware, and spyware). We examine the recognition performance by way of applying the random forest set of rules on unique datasets created through the Kyoto 2006+ dataset that is the present day community packet statistics accumulated to build intrusion detection structures. We finish with discussions and guidelines for destiny research.

3) The Choice of Timber in Selecting a Random Wooded Area

Author: St. Bernard, l. Hatte and St. Adam

In this paper, we gift an ensemble of random woodland (RF) research. In the "traditional" RF induction manner, a small number of random choice trees are created in groups. This kind of algorithm has two important hazards: (i) the number of trees ought to be determined a priori (ii) The interpretation and analysis of assets which are misplaced during the decision of the type bushes, because of the precept of randomization. This type of method, wherein timber are distinguished independently, does now not guarantee that each one timber will cooperate effectively within the identical group. This statement raises two questions: Are there selection trees that display the RF overall performance of a reciprocal collection? If so, is it possible to make a greater accurate map by using casting off timber making terrible selections? Answering these questions is taken into consideration a query of department of the lesson. We show that choicest units of decision bushes can also be received the use of a sub-most advantageous classifier choice approach. This proves that the "classical" RF induction manner, which randomly assembles random bushes into agencies, is not the exceptional technique for building correct RF classifiers. We are also inquisitive about RF design, adding timber to conventional "classical" RF induction algorithms.

4) Intrusion Detection Using Random Soar Classifier With Movement And Characteristic Pruning.

Author: A. Desphon, D. Lalita Bhaskari

Intrusion detection systems (IDS) have come to be an vital factor of laptop and community security. The NSL-KDD intrusion detection dataset, an improved version of the KDDCUP'99 dataset, is used because the test dataset in this paper. Due to the inherent characteristics of intrusion detection, there may be nevertheless a huge imbalance among classes within the NSL-KDD dataset, which makes it

difficult for system mastering within the field of intrusion detection. To deal with the unevenness of the order, on this paper, a minority oversampling (smote) approach is carried out to the schooling information set. A data acquisition-based totally selection approach is presented to generate decreased line units of NSL-KDD datasets. Random forests are used as a classifier inside the proposed intrusion detection system. Empirical results display that random woodland type and records retrieval-primarily based selection the use of SMOTE provide better overall performance in IDS improvement.

5) Impact of PCA-Scale GRU Improvement on Intrusion Detection.

Authors: Le T.-T.-H., Kang H. And Kim H.

An intrusion detection machine (IDS) is a tool or software program that monitors a network or system for malicious interest. Traditional IDSs can't stumble on large cyber assaults together with low-frequency DoS attacks and unknown assaults. To overcome those boundaries, gadget getting to know has attracted increasing hobby in current years. In this paper, we proposed a new approach to enhance the accuracy of recurrent unit (GRU) intrusion detection by making use of the proposed scaling PCA with alternatives, together with well-known PCA and PCA-minmax, within the GRU layer. Both strategies implicitly observe prioritization to professional item maps, influencing the route of most variance by high-quality covariance. This approach may be carried out to GRU models with additional fee accounting. We gift experimental results on actual-global analyzers, KDD report 99 and NSL-KDD, demonstrating that the skilled PCA-scaled GRU model achieves huge performance enhancements.

EXISTING SYSTEM:

• Iftikhar Ahmed and p. Al studied numerous system getting to know algorithms for intrusion detection systems. They were comparing a few excessive device learning methods. The authors concluded that the acute system gaining knowledge of approach outperformed different algorithms.

• B. Riaz and p. Al., worked here on enhancing the high-quality of information for feeding intrusion detection structures. To develop the dataset, even though, we used a rule-primarily based characteristic choice technique. The KDD dataset become used and they showed dynamic growth on the stop of IDS.

Disadvantages of Existing System:

• Systems going for walks on the Internet are vulnerable to numerous malicious activities. The main problem located on this area is the penetration of leakage structures.

• Current effects imply that some improvements can be made in phrases of accuracy and detection price in addition to false alarm rate.

Other techniques can update the preceding method, including Naive Bayes. Additionally, the take a look at indicates that the statistics set can be advanced the usage of precise strategies. Increase the nice of inputs within the proposed gadget.

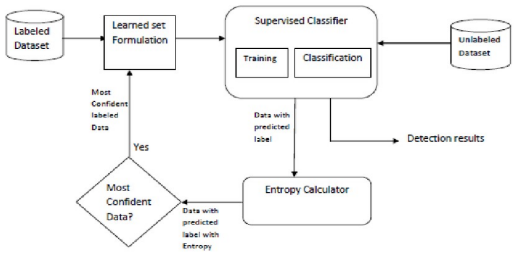
PROPOSED SYSTEM:

Intrusion detection structures work to make the machine extra prone to attackers. This machine can stumble on incoming calls. The proposed machine attempts to triumph over preceding troubles with existing work. The proposed system includes methods: most important aspect analysis and the random woodland method. Principal element evaluation is used to decrease the dimensionality of a facts set; with this technique, the exceptional of the dataset is advanced due to the fact the dataset has the right features. A random wooded area set of rules is then used to come across intruders, which offers each higher detection charges and fake alarm rates than SVM.

Advantages of Proposed System:

• The error price located in our proposed technique is very low, as much as 0.21%.
• In addition, the accuracy of the algorithm is better than the previous one.
• Also, the execution time is much less in comparison to other algorithms.

SYSTEM ARCHITECTURE:



SYSTEM REQUIREMENTS:

Hardware Requirements:

- System : Pentium IV 2.4 GHz.
- Hard Disk : 40 GB.
- Floppy Drive : 1.44 Mb.
- Monitor : 15 VGA Colour.
- Mouse : Logitech.
- Ram : 512 Mb.

Software Requirements:

- Operating system: Windows 7.
- Coding Language : Python
- Database : MYSQL

MODULES:

- Data Collection
- Dataset
- Data Preparation
- Model Selection
- Analyze and Prediction
- Accuracy on test set
- Saving the Trained Model

Data Collection:

Collecting facts is the first actual step in truly developing a system studying model. This is important: the better the version, the better the facts we get, the higher our model will do. There are many techniques of statistics collection consisting of textual content scraping, guide intervention, and so on. The dataset used in this intrusion detection system dataset is taken from KDD.

Data Set:

The dataset includes 125974 unique statistics. The dataset has 42 columns, which are described under.

Data Preparation:

We will trade the statistics. Removed lacking data and getting rid of some columns. First, allows make a listing of column names that we need to save or save. Then we delete all the columns besides the ones we need to keep. Finally, we drop or get rid of rows and not using a values from the dataset. Divide the fund and kill the estimate.

Model Selection:

Principal element analysis is a method particularly used to reduce the dimensionality of a statistics set. Principal element evaluation is a very powerful and correct method of reducing the dimensionality of facts to produce the desired results.

Analyze and Prediction:

In the actual facts set, we decided on only 9 capabilities;

1.Duration	length (number of seconds) of the connection
2.Protocol_type	type of the protocol, e.g. tcp, udp, etc.
3.Src_bytes	number of data bytes from source to destination
4.Dst_bytes	number of data bytes from destination to source
5.Is_hot_login	1 if the login belongs to the "hot" list; 0 otherwise
6.Is_guest_login	1 if the login is a "guest"login; 0 otherwise
7.Diff_srv_rate	% of connections to different services
8.Srv_diff_host_rate	% of connections to different hosts
9.Flag	normal or error status of the connection
10. Labels	Normal or attacker

Accuracy on Test Set:

We achieved 93.1% accuracy in testing.

Saving the Trained Model:

Once you're confident enough to take your template designed and examined into production, the first step is to convert it to .H5 or .H5. It uses the PKL library as a firewall. Make certain the firewall is mounted for your surroundings. Then fetch a copy of the module and import the copy into a .PKL report.

GOALS

The principal targets of UML design are:

1. Provide users with an equipped-to-use, obvious visual design language to be able to create and percentage significant fashions.
2. Provide extra coaching and special guidance to enhance key ideas.
3. be independent from particular programming languages and improvement techniques.
4. Provide a proper basis for expertise language formation.
5. To sell the improvement of market orientated products.

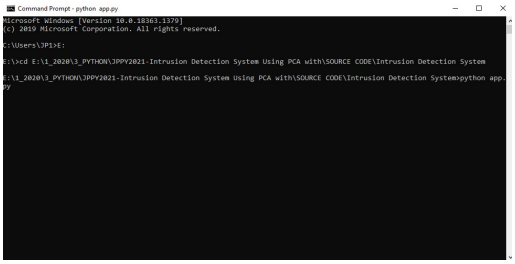
6. Supports excessive-degree improvement standards which include collaboration, composition, modeling, and components.

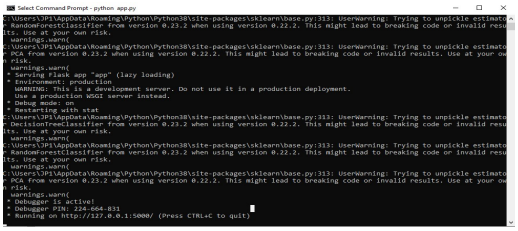
7. Complete with the quality talents.

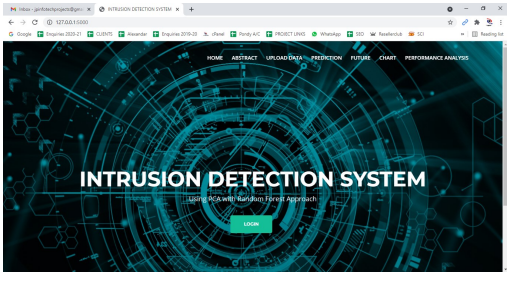
RESULT AND DISCUSSION

This is completed to reduce the dimensionality of the statistics set; with this method, the nice of the dataset is advanced because the dataset has the proper capabilities. A random wooded area algorithm is then used to stumble on intruders, which presents both higher detection prices and false alarm charges than SVM.

SCREENSHOTS







CONCLUSION

In modern-day situation of developing threats and increasing cyber-attacks, a clever protection gadget is vital. Artificial intelligence technologies are more bendy and dependable than ultra-modern cyber security answers. It protects against increasingly more advanced and complex cyber threats and improves machine safety. Although artificial intelligence systems have a dizzying impact on cyber security, the associated structures are not yet geared up for a full transformation. Although we've got many benefits when the use of artificial intelligence generation for cyber safety, it is not the most effective safety solution. Systems can fail while a human adversary attacks them for the express purpose of bypassing smart security forces. This does now not imply that we should no longer use synthetic intelligence era, however be aware of its barriers. Artificial intelligence technology requires human interaction and education. This incorporated approach has many tested effects because it works closely with danger researchers.

FUTURE ENHANCEMENT

We can use AI in extraordinary methods for cyber protection. In the future, we may additionally have extra wise systems in these ways. It may also use attackers or AI attackers for attacks. It is apparent that the advances in expertise, manipulating, and visualizing statistics, specifically inside the discipline of device getting to know, will drastically enhance

the cyber security skills of the structures that use it.

REFERENCES

1. JafarAbo Nada; Mohammad Rasmi Al-Mosa, 2018 International Arab Conference on Information Technology (ACIT), A Proposed Wireless Intrusion Detection Prevention and Attack System

2. Kinam Park; Youngrok Song; Yun-Gyung Cheong, 2018 IEEE Fourth International Conference on Big Data Computing Service and Applications (BigData Service), Classification of Attack Types for Intrusion Detection Systems Using a Machine Learning Algorithm

3. S. Bernard, L. Heutte and S. Adam "On the Selection of Decision Trees in Random Forests" Proceedings of International Joint Conference on Neural Networks, Atlanta, Georgia, USA, June 14-19, 2009, 978-1-4244-3553-1/09/$25.00 ©2009 IEEE

4. A. Tesfahun, D. Lalitha Bhaskari, "Intrusion Detection using Random Forests Classifier with SMOTE and Feature Reduction" 2013 International Conference on Cloud & Ubiquitous Computing & Emerging Technologies, 978-0-4799-2235-2/13 $26.00 © 2013 IEEE

5. Le, T.-T.-H., Kang, H., & Kim, H. (2019). The Impact of PCA-Scale Improving GRU Performance for Intrusion Detection. 2019 International Conference on Platform Technology and Service (PlatCon). Doi:10.1109/platcon.2019.8668960

6. Anish Halimaa A, Dr K.Sundarakantham: Proceedings of the Third International Conference on Trends in Electronics and Informatics (ICOEI 2019) 978-1-5386-9439-8/19/$31.00 ©2019 IEEE "MACHINE LEARNING BASED INTRUSION DETECTION SYSTEM."

7. Mengmeng Ge, Xiping Fu, Naeem Syed, Zubair Baig, Gideon Teo, Antonio Robles-Kelly (2019). Deep Learning-Based Intrusion Detect ion for IoT Networks, 2019 IEEE 24th Pacific Rim International Symposium on Dependable Computing (PRDC), pp. 256-265, Japan.

8. R. Patgiri, U. Varshney, T. Akutota, and R. Kunde, "An Investigation on Intrusion Detection System Using Machine Learning" 978-1-5386-9276-9/18/$31.00 c2018IEEE.

9. Rohit Kumar Singh Gautam, Er. Amit Doegar; 2018 8th International Conference on Cloud Computing, Data Science & Engineering (Confluence) "An Ensemble Approach for

Intrusion Detect ion System Using Machine Learning Algorithms."

10. Kazi Abu Taher, Billal Mohammed Yasin Jisan, Md. MahbuburRahma, 2019 International Conference on Robot ics, Electrical and Signal Processing Techniques (ICREST)"Network Intrusion Detect ion using Supervised Machine Learning Technique with Feature Selection."

11. L. Haripriya, M.A. Jabbar, 2018 Second International Conference on Electronics, Communication and Aerospace Technology (ICECA)" Role of Machine Learning in Intrusion Detection System: Review"

12. Nimmy Krishnan, A. Salim, 2018 International CET Conference on Control, Communication, and Computing (IC4) " Machine Learning-Based Intrusion Detect ion for Virtualized Infrastructures"

13. Mohammed Ishaque, LadislavHudec, 2019 2nd International Conference on Computer Applications & Information Security (ICCAIS) "Feature extract ion using Deep Learning for Intrusion Detection System."

14. Aditya Phadke, Mohit Kulkarni, Pranav Bhawalkar, Rashmi Bhattad, 2019 3rd International Conference on Computing Methodologies and Communication (ICCMC)"A Review of Machine Learning Methodologies for Network Intrusion Detection."

15. Iftikhar Ahmad , Mohammad Basheri, Muhammad Javed Iqbal, Aneel Rahim, IEEE Access (Volume: 6) Page(s): 33789 – 33795 "Performance Comparison of
Support Vector Machine, Random Forest, and Extreme Learning Machine for Intrusion Detection."

16. B. Riyaz, S. Ganapathy, 2018 International Conference on Recent Trends in Advanced Computing (ICRTAC)" An Intelligent Fuzzy Rule-based Feature Select ion for Effective Intrusion Detection."