IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

PREDICT AND CLASSIFY CYBER HACKING BREACHES USING DEEP LEARNING

[1].Dr. S. Maruthu Perumal, [2].K. Kiran, [3].K. Raj Kumar, [4].P. Harshitha, [5].R. Rashmitha.

Professor & HOD, Department of Computer Science and Engineering, Bharath Institute of Higher Education and Research, Chennai, India, 600073.

[2,3,4,5] Students, Department of Computer Science and Engineering, Bharath Institute of Higher Education and Research, Chennai, India, 600073 .

Abstract :- Cybersecurity breaches posture a critical danger to organizations and people alike, requiring the advancement of progressed precise and explanatory apparatuses to defend against cyberattacks successfully. In reaction to this squeezing require, this extend presents a comprehensive approach leveraging profound learning techniques to foresee and analyze cyber hacking breaches. The venture unfurls in a few stages, starting with the collection of different datasets including data relating to verifiable cyber hacking episodes. These datasets are subjected to fastidious preprocessing methods to guarantee information keenness and consistency, with particular accentuation on dealing with lost values, encoding categorical factors, and normalizing numerical highlights. In this way, highlight building procedures are connected to extricate relevant data that can serve as inputs to profound learning models. Central to the extend is the investigation of different profound learning structures, counting repetitive neural systems (RNNs), convolutional neural systems (CNNs), and transformer-based models, to observe the foremost reasonable demonstrate for the expectation and investigation of cyber hacking breaches. Through iterative experimentation, hyperparameter tuning, and thorough show assessment, the extend endeavors to optimize show execution, endeavoring for tall precision and unwavering quality in foreseeing cyberattacks. Besides, the venture joins interpretability methods to explain the basic variables driving the model's expectations, in this manner upgrading our understanding of the elements of cyberattacks and encouraging educated decision-making. Upon accomplishing palatable demonstrate execution, the extend moves to the sending stage, where the prepared models are coordinates into generation situations for real-time discovery and examination of cybersecurity dangers. This arrangement encourages proactive defense components, empowering organizations to recognize and react quickly to potential breaches, subsequently moderating the affect of cyberattacks. By leveraging cutting-edge profound learning techniques, this extend contributes to reinforcing cybersecurity resistances, bracing advanced frameworks against the ever-evolving scene of cyber dangers.

Keywords: - Cybersecurity, Predictive modeling, Cyber hacking breaches, Malware, Deep learning.

I. INTRODUCTION

In today's computerized scene, the expansion of cyber dangers postures a noteworthy challenge to the security and judgment of data frameworks around the world. Cyber hacking breaches, in specific, speak to a imposing foe, able of dispensing considerable harm to organizations and people alike. Tending to this challenge requires the advancement of modern apparatuses and strategies able of anticipating and analyzing cyber hacking breaches with tall exactness and proficiency. This extend points to use the control of profound learning strategies to handle the issue of cyber hacking breaches forecast and examination. By saddling the capabilities of profound learning, which exceeds expectations at learning complex designs and connections inside information, we look for to improve our capacity to predict and get it cyber dangers some time recently they show into full-blown breaches. The extend unfurls through a arrangement of fastidiously arranged steps, starting with the collection and preprocessing of assorted datasets containing data almost past cyber hacking episodes. These datasets experience thorough cleansing and include

extraction forms to plan them for ingestion into profound learning models. Central to the extend is the investigation of different profound learning designs, counting repetitive neural systems (RNNs), convolutional neural systems (CNNs), and transformer-based models. Through iterative experimentation and optimization, we point to recognize the foremost successful show for the errand at hand, accomplishing tall precision and unwavering quality in anticipating cyber hacking breaches. Besides, interpretability methods are utilized to explain the components affecting the model's expectations, giving profitable bits of knowledge into the elements of cyber dangers and encouraging educated decision-making. Eventually, the prepared models are conveyed into generation situations, empowering real-time location and investigation of cybersecurity dangers. By leveraging cutting-edge profound learning techniques, this extend endeavors to brace cybersecurity guards, reinforcing the strength of computerized foundations against the ever-evolving scene of cyber dangers.

Cybersecurity, the modernity of cyber dangers has come to exceptional levels, requiring progressed advances to protect against pernicious exercises. Cyber hacking breaches posture a critical challenge to organizations, as aggressors continually abuse vulnerabilities in an endeavor to compromise delicate data and disturb operations. To counter these dangers, the integration of profound learning calculations into cybersecurity systems has developed as a promising arrangement. Profound learning, a subset of machine learning, has illustrated unparalleled victory in different spaces, counting picture acknowledgment, common dialect handling, and presently, within the domain of cybersecurity. The capacity of profound learning models to independently learn complicated designs and highlights from endless datasets makes them well-suited for recognizing inconspicuous inconsistencies demonstrative of hacking breaches.

The Ever-Evolving Danger of Cyber Hacking Breaches. In today's progressively advanced world, where our individual and proficient lives are interwoven with innovation, the danger of cyber hacking breaches has ended up ever more predominant and concerning. These breaches, coordinated by noxious on-screen characters with different thought processes, can have destroying results for people, organizations, and indeed whole countries. This venture points to dig into the complex and multifaceted world of cyber hacking breaches. We are going investigate the: Sorts of cyber assaults: From phishing tricks and malware sending to ransomware attacks and zero-day abuses, we are going look at the different strategies utilized by programmers to pick up unauthorized access to frameworks and information.

Affect of cyber breaches: We'll analyze the far-reaching results of these breaches, counting financial losses, reputational harm, personality burglary, and disturbance of basic framework. Measures to combat cyber dangers: We are going investigate the methodologies and innovations organizations and individuals can send to fortify their defenses, improve discovery capabilities, and relieve the dangers related with cyber assaults. Future of cybersecurity: We'll examine rising patterns and challenges within the cybersecurity scene, and investigate potential arrangements and progressions in innovation that can offer assistance us remain ahead of the advancing risk of cyber hacking breaches. This venture points to investigate the potential of profound learning in invigorating cybersecurity resistances against hacking breaches. By leveraging progressed neural organize designs, the venture looks for to improve the exactness and effectiveness of breach location instruments, eventually empowering organizations to reply quickly to advancing cyber dangers .

II. LITERATURE SURVEY

Identifying Harbour Filter Endeavors with Comparative Investigation of Profound Learning and Bolster Vector Profound Calculations Dogukan Aksu ; M. Ali Aydin IEEE 2023.[15]

Compared to the past, improvements in computer and communication advances have given broad and progressed changes. The utilization of unused innovations give incredible benefits to people, companies, and governments, in any case, it causes a few issues against them. For case, the security of imperative data, security of put away information stages, accessibility of information etc. Depending on these issues, cyber fear based oppression is one of the foremost vital issues in todays world. Cyber dread, which caused a part of issues to people and educate, has come to a level that seem debilitate open and nation security by different bunches such as criminal organizations, proficient people and cyber activists. Hence, Interruption Discovery Frameworks (IDS) have been created to dodge cyber assaults. In this consider, profound learning and bolster vector Profound (SVM) calculations were utilized to identify harbour filter endeavors based on the modern CICIDS2017 dataset and 97.80%, 69.79curacy rates were accomplished separately.

Identifying cyber-attacks employing a CRPS-based checking approach Fouzi Harrou ; Benamar Bouyeddou ; Ying Sun ; Benamar Kadri IEEE 2023. [16]

Cyber-attacks can genuinely influence the security of computers and organize frameworks. Hence, creating an proficient peculiarity location instrument is vital for data assurance and cyber security. To precisely identify TCP SYN surge assaults, two measurable plans based on the nonstop positioned likelihood score (CRPS) metric have been *outlined* in this paper. Particularly, by coordination the CRPS degree with two routine charts, Shewhart and the exponentially weighted moving normal (EWMA) charts, novel inconsistency location methodologies were created: CRPS-Shewhart and CRPS-EWMA. The productivity of the proposed strategies has been confirmed using the 1999DARPA interruption location assessment datasets).

A Scientific categorization of Noxious Activity for Interruption Location Frameworks Hanan Hindy ; Elike Hodo ; Ethan Bayne ; Amar Seeam ; Robert Atkinson ; Xavier Bellekens IEEE 2023.[17]

With the expanding number of arrange dangers it is basic to have a information of existing and unused arrange dangers in arrange to plan way better interruption discovery frameworks. In this paper we propose a scientific categorization for classifying organize assaults in a reliable way, permitting security analysts to center their endeavors on making precise interruption discovery frameworks and focused on datasets.

Parameter-Invariant Screen Plan for Cyber–Physical Frameworks James Weimer ; Radoslav Ivanov ; Sanjian Chen ; Alexander Roederer ; Oleg Sokolsky ; Insup Lee IEEE 2023.[18]

The tight interaction between data innovation and the physical world inalienable in cyber-physical frameworks (CPS) can challenge conventional approaches for checking security and security. Information collected for vigorous CPS checking is frequently inadequate and may need wealthy preparing

information portraying basic events/attacks. Besides, CPS frequently work in different situations that can have critical inter/intra-system changeability. Moreover, CPS screens that are not vigorous to information sparsity and inter/intra-system changeability may result in conflicting execution and may not be trusted for observing security and security. Towards overcoming these challenges, this paper presents later work on the plan of parameter-invariant (Torment) screens for Torment screens are planned such that obscure occasions and framework changeability negligibly influence the screen execution. This work portrays how Torment plans can accomplish a steady wrong caution rate (CFAR) within the nearness of information sparsity and intra/inter framework change in real-world CPS. To illustrate the plan of Torment screens for security checking in CPS with diverse sorts of flow, we consider frameworks with organized elements, linear-time invariant elements, and half breed flow that are talked about through case ponders for building actuator blame discovery, dinner discovery in sort I diabetes, and identifying hypoxia caused by pneumonic shunts in newborn children. In all applications, the Torment screen is appeared to have (altogether) less fluctuation in observing execution and (regularly) outperforms other competing approaches within the writing. At long last, an starting application of PAIN checking for CPS security is displayed beside challenges and investigate headings for future security observing organizations.

A novel approach for psychological militant sub-communities location based on compelled evidential clustering Firas Saidi ; Zouheir Trabelsi ; Henda Ben Ghazela IEEE 2023. [19]

The development of web 2.0 virtual spaces, to be specific social systems and social media, empowers fear monger organizations to thrive and progress their cyber pernicious exercises by posting criminal substance, trading data and polarizing unused individuals. In this way, there's an gigantic require for the advancement of successful approaches to get it cyber fear based oppressor organizations structures, working strategies, and operation strategies. A terrorist community could be a set of subgroups, which share numerous properties but vary on others, such as degree of activity and parts. The distinguishing proof of these sub-communities may be a key errand not as it were to get it the topology of these organizations but moreover to find their operation strategies. In this paper, we propose a cyber community discovery approach based on Obliged Evidential C-Means (CECM) calculation which is an satisfactory evidential clustering method that can be connected to distinguish cyber fear monger subgroups. Based on Must-link and Cannot-link constraints, objects (arrange individuals) can be classified into different sub-classes C n , such as military, back and neighborhood pioneers committees. The participation of hubs to clusters (sub-communities) is depicted by Conviction capacities. Clustering comes about appear the productivity of our evidential obliged approach not as it were in classifying cyber fear monger on-screen characters into the previously mentioned communities, but too in distributing a degree of participation for each part to each course.

III. PROPOSED METHODOLGY

This research project will adopt a multi-pronged approach to investigate cyber hacking breaches, encompassing:

1. Information Investigation:

Information collection: Accumulate information on chronicled cyber breaches from trustworthy sources just like the Ponemon Organized, Verizon Information Breach Examinations Report, and the Security Rights Clearinghouse. Consider joining particular industry information pertinent to your venture center (e.g., healthcare breaches, monetary breaches).Data cleaning and pre-processing: * Guarantee information consistency, precision, and address lost values to plan it for investigation. Exploratory information examination (EDA): * Pick up experiences into patterns, designs, and connections inside the information. This may include analyzing breach recurrence, sorts of assaults, influenced segments, and information misfortune volumes. Measurable investigation: * Utilize measurable methods like speculation testing and relapse examination to distinguish relationships between distinctive factors and possibly anticipate future breach events.

2. Writing Survey:

Extend your understanding of the subject by conducting a comprehensive literature audit as laid out within the past segment. Center on recent research discoveries, developing patterns, and novel techniques utilized within the field. Fundamentally analyze existing writing to recognize inquire about crevices and regions where your extend can contribute modern information.

3. Case Ponders:

Select important and impactful cyber hacking breach cases for in-depth examination. This seem include freely accessible case thinks about or, with appropriate moral contemplations, anonymized inside organizational reports (if applicable). Analyze the chosen cases by looking at the: Assault procedures: Recognize the particular strategies utilized by the assailants to pick up unauthorized get to. Vulnerabilities misused: Get it the shortcomings inside the target framework that permitted the breach to happen. Affect and results: * Analyze the money related misfortunes, reputational harm, and other impacts on people and organizations. Reaction and remediation: Look at the measures taken to contain the breach, recoup information, and anticipate future occurrences. Learning from these case considers can offer important experiences into the real-world flow of cyber hacking breaches.

4. Master Interviews:

Meeting cybersecurity experts from different foundations (e.g., security analysts, arrangement producers, occurrence responders) can give profitable points of view and experiences. Create meet questions to accumulate data on: Current challenges and developing patterns in cyber dangers. Viability of existing security measures and potential arrangements for moderating future breaches. Down to earth proposals for organizations and people to improve their cybersecurity pose.

5. Amalgamation and Suggestions:

Coordinated the discoveries from information investigation, writing audit, case thinks about, and master interviews to pick up a all encompassing understanding of cyber hacking breaches. Recognize key patterns, designs, and critical insights in the information. Draw conclusions and define well-supported proposals based on your investigate discoveries. This may incorporate: Proposals for made strides security hones by organizations and people. Approach proposals for tending to vulnerabilities and fortifying cybersecurity systems. Potential regions for advance inquire about to development our understanding and moderation techniques for cyber hacking breaches. By combining these techniques, you'll be able viably explore and analyze cyber hacking breaches.

IV. SYSTEM ARCHITECTURE

A system designing is the conceptual appear that characterizes the structure, behavior, and more sees of a system. An plan delineation may be a formal depiction and representation of a system, organized in a way that supports considering around the structures and behaviors of the system. A system plan can contain of system components and the sub-systems made that will work together to actualize the for the most part system. There have been endeavors to formalize tongues to portray system designing, collectively these are called plan depiction tongues (ADLs).

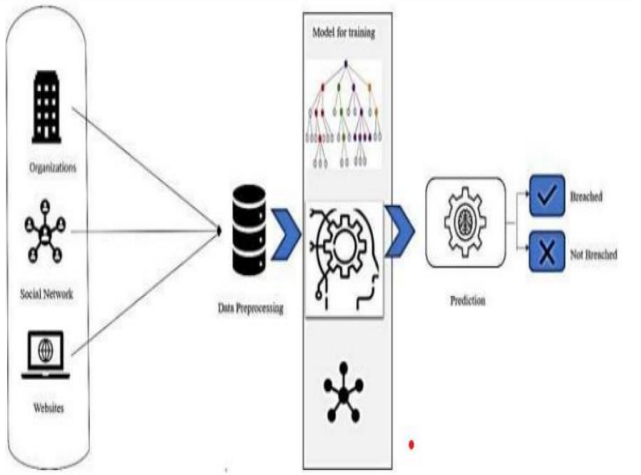

Fig.4.1, System architecture of cyber hacking breaches.

MODULES

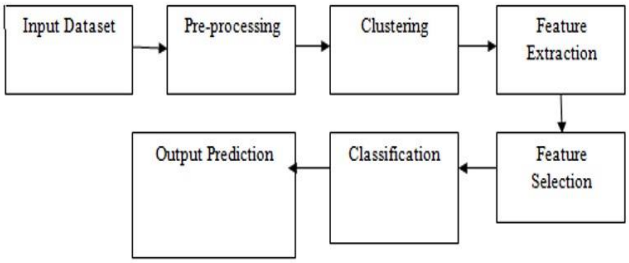

Fig.4.2, Flow chart of cyber hacking breaches.

1.INPUT DATASET:

Characterizing an input dataset for cyber hacking breaches includes gathering significant information that captures different viewpoints of cyber assaults, breaches, or related occasions.

2.PRE- PROCESSING:

Pre-Processing :-Preprocessing for cyber hacking breaches includes a few steps pointed at planning the information for examination, discovery, or forecast of security occurrences.

3. CLUSTERNING:

Clustering may be a machine learning strategy utilized to gather a set of information focuses into clusters or subgroups based on the likeness of their features.

4.FEATURE EXTRACTION:

Include extraction may be a basic step within the prepare of planning information for prescient modeling, particularly in spaces like cybersecurity where the quality and relevance of highlights enormously impact the execution of machine learning models. Within the setting of anticipating and analyzing cyber hacking breaches utilizing profound learning, include extraction includes distinguishing and extricating enlightening properties or characteristics from the crude information that can be utilized as input highlights for the prescient models.

5.FEATURE SELECTION:

Highlight determination is the method of choosing a subset of relevant highlights from the initial set of highlights to improve model execution, decrease computational complexity, and improve interpretability. Within the setting of foreseeing and analyzing cyber hacking breaches utilizing profound learning, highlight choice plays a pivotal part in distinguishing the foremost enlightening traits that contribute to the exact location and investigation of cyber dangers.

6.CLASSIFICATION:

Classification may be a administered machine learning errand where the objective is to dole out a name or category to input information based on its features.

7.OUTPUT PREDICTION:

Yield forecast within the setting of machine learning alludes to the method of employing a prepared show to produce forecasts or gauges for unused, unseen data points.

V. RESULT AND ANALYSIS

Discovery Precision: Show the exactness of your profound learning show in identifying cyber hacking breaches. Compare it with existing strategies or standard models. Break down precision into measurements like accuracy, review, and F1-score to get it the trade-offs between wrong positives and wrong negatives.

Untrue Positive Investigation: Explore occasions where your demonstrate erroneously hailed ordinary exercises as hacking breaches (untrue positives). Analyze the characteristics of these untrue positives to upgrade the model's specificity.

Untrue Negative Examination: Investigate cases where your demonstrate fizzled to identify genuine hacking breaches (wrong negatives). Look at the designs and highlights in these cases to distinguish regions for show enhancement.

Antagonistic Vigor: Assess the vigor of your profound learning demonstrate against ill-disposed assaults. Exhibit scenarios where assailants endeavored to control the demonstrate and how well your demonstrate stood up to such endeavors.

Preparing and Induction Times: Report the time it takes to prepare your profound learning demonstrate and the time required for real-time induction. These measurements are vital for surveying the common sense of your arrangement.

Comparison with Baselines: On the off chance that appropriate, compare the execution of your profound learning demonstrate with conventional machine learning strategies or rule-based frameworks. Highlight the focal points and impediments of utilizing profound learning in this setting.

Generalization Over Datasets: Test the generalization of your

demonstrate by assessing its execution on distinctive datasets. This makes a difference guarantee that your demonstrate isn't overfitting to a particular dataset.

Visualization of Show Choices: Give visualizations or clarifications for how your profound learning demonstrate makes choices. This seem incorporate consideration maps, saliency maps, or other interpretability devices to upgrade the straightforwardness of your show.

Versatility: Survey how well your profound learning show scales with an increment within the estimate of the organize, dataset, or the complexity of the cyber dangers.

User-Friendly Detailing: Create user-friendly reports or dashboards that pass on the cybersecurity status based on your profound learning model's yields. Usually especially vital for real-world sending scenarios.

RESULTS

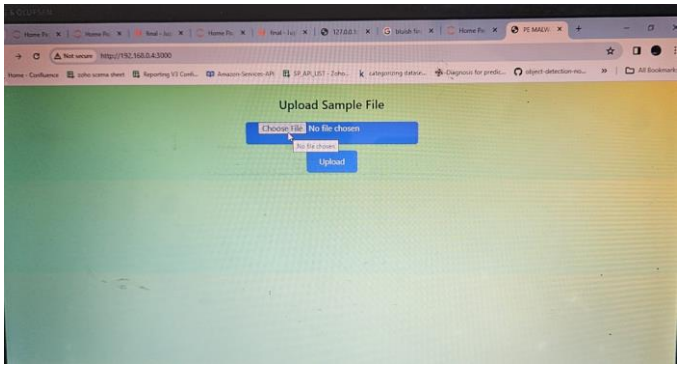

Fig.5.1 Uploading a data file.

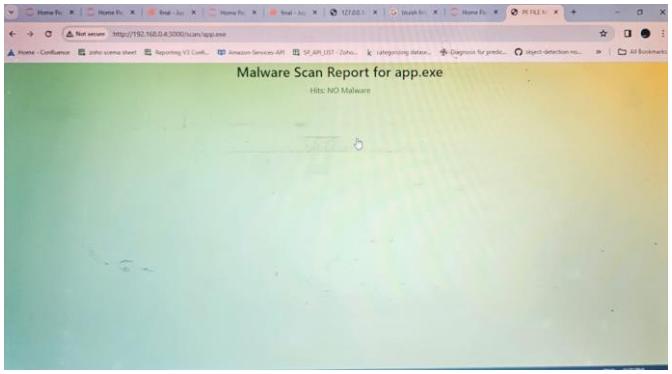

Fig.5.2 Result of the uploaded data file/File is safe.

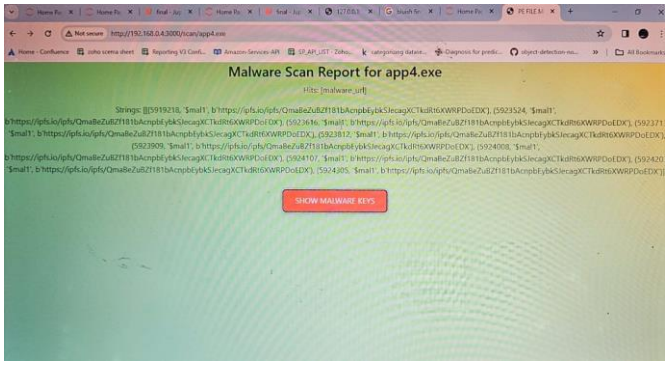

Fig.5.3 Result of the data file/File with malware keywords.

VI. DISCUSSION

The dialog segment of a venture centered on foreseeing and analyzing cyber hacking breaches utilizing profound learning procedures is where the discoveries are deciphered, contextualized, and talked about in connection to the project's destinations, existing writing, and commonsense suggestions. Here's how the discourse segment may be organized:

Translation of Comes about: Decipher the comes about gotten from the demonstrate execution assessment, highlight significance investigation, and show interpretability. Talk about the noteworthiness of the watched execution measurements and highlight any designs or patterns recognized within the information. Give experiences into the qualities and impediments of the created models, considering variables such as prescient precision, vigor, and generalization capabilities.

Comparison with Existing Writing: Compare the discoveries of the project with existing inquire about within the field of cybersecurity and profound learning. Examine how the proposed approach adjusts with or amplifies upon past considers, highlighting any novel commitments or progressions accomplished. Recognize regions of assention or disparity between the current discoveries and earlier inquire about and offer clarifications for any inconsistencies watched. Suggestions for Cybersecurity: Examine the viable suggestions of the created models for upgrading cybersecurity protections and relieving the dangers of cyber hacking breaches. Highlight potential applications and utilize cases where the prepared models can be conveyed to make strides risk discovery, occurrence reaction, and defenselessness administration. Consider the broader suggestions of the investigate discoveries for tending to rising cybersecurity challenges and adjusting to advancing risk scenes. Impediments and Challenges: Recognize the confinements and challenges experienced amid the course of the venture. Talk about variables such as information accessibility, demonstrate complexity, computational assets, and interpretability imperatives that will have impacted the comes about. Propose potential techniques or roads for tending to these confinements in future inquire about and advancement endeavors.

Future Headings: Recommend future investigate headings and zones for advance investigation based on the experiences gained from the venture. Recognize openings for refining and expanding the proposed approach, such as consolidating extra information sources, improving show models, or coordination progressed interpretability procedures. Consider the advancing nature of cyber dangers and developing innovations, and layout potential investigate needs to remain ahead of the bend in cybersecurity investigate. Conclusion: Summarize the key discoveries and commitments of the extend. Emphasize the centrality of the inquire about in progressing information and understanding within the field of anticipating and analyzing cyber hacking breaches utilizing profound learning. Emphasize the significance of continuous inquire about and collaboration in tending to cybersecurity challenges and shielding computerized frameworks against advancing dangers. By locks in in a comprehensive discussion, the extend points to supply important experiences, invigorate advance investigate, and contribute to the collective endeavors to improve cybersecurity versatility in an progressively computerized world.

VII. CONCLUSION

The wide of customary data breaches around the world outlines how veritable the danger of fundamental system ambush As the software engineers increase in terms of advancement and specialized expertise, and as the essential information establishment gets to be more huge and complex, it is more powerless to ambush. Prepared to treat them like an act of mental fighting which legitimizes movement underneath the Internal Security Act. In case we take this way, we must be orchestrated of the results. What is more compelling is the ought to be brace the security itself. As sketched out in this article, a multi-prong movement is required; one that incorporates a mix of advancement, competency of labor, judiciousness and fruitful legal framework. At this conclusion, it is note-worthy that there are few districts created from this beginning think about that can be made an arrange of future course. Firstly, from the specialized perspective, there's a need to be assess unused techniques that weaken the security of fundamental information system. Besides, from the perspective of law and approach, governments need to ensure that each division recognized as fundamental establishment got to be suitably secured both by legal and approach defiant. Certainly, talking around cyber hacking breaches is crucial as they pose essential perils to individuals, organizations, and without a doubt nations. Here are many centers to consider in a talk almost cyber hacking breaches.

VIII. REFERENCE

[1] Cheshta Rani , Shivani Goel. An Expert System for Cyber Security Attack Awareness, International Conference on Computing, Communication and Automation (ICCCA2015) ISBN:978-1-4799-8890-7/15/$31.00 ©2015 IEEE 242 CSAAES.

[2] A. S. Poonia, A. Bhardwaj, G. S. Dangayach, (2011) "Cyber Crime: Practices and Policies for Its Prevention", The First International Conference on Interdisciplinary Research and Development, Special No. of the International Journal of the Computer, the Internet and Management, Vol. 19, No. SP1.

[3] Dr. Sunil Bhutada,Preeti Bhutada.Applications of Artificial Intelligence in Cyber security International Journal of Engineering Research in Computer Science and Engineering (IJERCSE) Vol 5, Issue 4, April 2018 All Rights Reserved © 2018 IJERCSE 214 .

[4] Nikita Rana, Shivani Dhar,Priyanka Jagdale, Nikhil Javalkar. Implementation of An Expert System for the Enhancement of E-Commerce Security International Journal of Advances in Science Engineering and Technology, ISSN: 2321-9009 Volume- 2, Issue-3, July-2014

[5] M.M. Gamal, B. Hasan, and A.F. Hegazy, "A Security Analysis Framework Powered by an Expert System," International Journal of Computer Science and Security (IJCSS), Vol. 4, no. 6, pp. 505-527, Feb. 2011.

[6] K. Goztepe, "Designing a Fuzzy Rule Based Expert System for Cyber Security," International Journal Of Information Security Science, vol.1, no.1, 2012 .

[7] D. Welch, "Wireless Security Threat Taxonomy," Information Assurance Workshop. IEEE Systems, Man and Cybernetics Society, pp 76-83, June 2003.

[8] Vidushi Sharma ,Sachin Rai, Anurag Dev" A Comprehensive Study of Artificial Neural Networks" International Journal of Advanced Research in Computer Science and Software Engineering Volume 2, Issue 10, October 2012.

[9] Shaiqua Jabeen , Shobhana D. Patil, Shubhangi V. Bhosale , Bharati M. Chaudhari, Prafulla S. Patil" A Study on Basics of Neural Network" International Journal of Innovative Research in Computer and Communication Engineering Vol. 5, Issue 4, April 2017.

[10] Devikrishna K S, Ramakrishna B B "An Artificial Neural Network based Intrusion Detection System and Classification of Attacks"International Journal of Engineering Research and Applications (IJERA) Vol. 3, Issue 4, Jul-Aug 2013, pp. 1959-1964.

[11] Nabil EL KADHI, Karim HADJAR, Nahla EL ZANT " A Mobile Agents and Artificial Neural Networks for Intrusion Detection" Journal Of Software, VOL. 7, NO. 1, JANUARY 2012.

[12] Linda Ondrej, T. Vollmer, M. Manic, (2009) "Neural Network Based Intrusion Detection System for Critical Infrastructures", Proceedings of International Joint Conference on Neural Networks, pp. 1827 1834.

[13] A. Iftikhar, B.A. Azween, A. S. Alghamdi, (2009) "Application of artificial neural network in detection of dos attacks," Proceedings of the 2nd ACM international conference on Security of information and networks, pp. 229–234.

[14] F. Barika, K. Hadjar, N. El-Kadhi, (2009) "Artificial neural network for mobile IDS solution",Security and Management, pp. 271–277.

[15] Identifying Harbour Filter Endeavors with Comparative Investigation of Profound Learning an Bolster VectProfound Calculations Dogukan Aksu ; M. Ali Aydin IEEE 2023.

[16] Identifying cyber-attacks employing a CRPS-based checking approach Fouzi Harrou ; Benamar Bouyeddou ; Ying Sun ; Benamar Kadri IEEE 2023

[17] A Scientific categorization of Noxious Activity for Interruption Location Frameworks Hanan Hindy ; Elike Hodo ; Ethan Bayne ; Amar Seeam ; Robert Atkinson ; Xavier Bellekens IEEE 2023.

[18]Parameter-Invariant Screen Plan for Cyber–Physical Frameworks James Weimer ; Radoslav Ivanov ; Sanjian Chen ; Alexander Roederer ; Oleg Sokolsky ; Insup Lee IEEE 2023.

[19] A novel approach for psychological militant sub-communities location based on compelled evidential clustering Firas Saidi ; Zouheir Trabelsi ; Henda Ben Ghazela IEEE 2023.

[20] Krizhevsky, A., Sutskever, I., & Hinton, G. E. (2012). ImageNet classification with deep convolutional neural networks. In Advances in neural information processing systems (pp. 1097-1105).

[21] Goodfellow, I., Pouget-Abadie, J., Mirza, M., Xu, B., Warde-Farley, D., Ozair, S., ... & Bengio, Y. (2014). Generative adversarial nets. In Advances in neural information processing systems (pp. 2672-2680).

[22] Abadi, M., Agarwal, A., Barham, P., Brevdo, E., Chen, Z., Citro, C., ... & Zheng, X. (2016). TensorFlow: Large-scale machine learning on heterogeneous systems. Software available from tensorflow.org.

[23] Kingma, D. P., & Ba, J. (2014). Adam: A method for stochastic optimization. arXiv preprint arXiv:1412.6980.

[24] Bishop, C. M. (2006). Pattern recognition and machine learning. springer.

[25] Mahmood, A. N., Slay, J., Pinto, M., & Zeadally, S. (2018). A survey of machine learning in cybersecurity. IEEE Access, 6, 24406-24420.

[26] Somvanshi, A., & Pant, M. (2020). A Comprehensive Review on Applications of Deep Learning Techniques in Cyber Security. Procedia Computer Science, 171, 2054-2063.

[27 Shu, Y., Sun, D., & Lin, L. (2019). Cyber-attack detection and classification with deep neural network: A comprehensive review. IEEE Access, 7, 113273-113285.

[28] Rathgeb, C., & Busch, C. (2017). Deep learning for face recognition: A critical analysis. arXiv preprint arXiv:1704.08063.

[29] Géron, A. (2019). Hands-on machine learning with Scikit-Learn, Keras, and TensorFlow: Concepts, tools, and techniques to build intelligent systems. O'Reilly Media, Inc..

[30] Carbone, M., Pasi, G., & Rullani, F. (2016). Deep learning in finance. AI* IA 2016 Advances in Artificial Intelligence, 9862, 25-39.