International Research Journal of Innovations in Engineering and Technology (IRJIET)
ISSN (online): 2581-3048
Volume 9, Special Issue INSPIRE'25, pp 315-322, April-2025
https://doi.org/10.47001/IRJIET/2025.INSPIRE51
International Conference on Sustainable Practices and Innovations in Research and Engineering (INSPIRE'25)

X-AI Enabled Hybrid Approach for Detection of Cyber Terrorism

[1]T.Niranjan Babu, [2]Dumpala Sravani, [3]R.Siva Sundar Reddy

[1]Assistant Professor, Dept. of C.S.E (Cyber Security), Madanapalle Institute of Technology & Science, Madanapalle, India
[2,3]UG Scholar, Dept. of C.S.E (Cyber Security), Madanapalle Institute of Technology & Science, Madanapalle, India
E-mail: [1]niranjanbabut@mits.ac.in, [2]sravanidumpala13@gmail.com, [3]sivasundarreddy27@gmail.com

***Abstract* - In an time checked by the fast advancement of innovation, cyber fear mongering postures a noteworthy danger to worldwide security and societal solidness. This paper proposes an X-AI empowered crossover approach to improve the location and avoidance of cyber fear mongering exercises. By coordination progressed counterfeit insights methods with conventional cybersecurity measures, this approach points to make a strong framework able of recognizing and relieving cyber dangers in real-time. The proposed show leverages machine learning calculations, counting profound learning and gathering strategies, to analyze tremendous datasets for designs characteristic of cyber fear monger behavior. Furthermore, the cross breed approach joins inconsistency location techniques to recognize bizarre exercises that will flag a looming cyber attack. Our framework is outlined to adjust persistently, learning from modern information and advancing danger scenes, hence guaranteeing proactive defense instruments against developing cyber dangers. We approve our approach through broad experimentation on benchmark datasets, illustrating made strides precision and diminished false-positive rates compared to existing location frameworks. The discoveries emphasize the potential of X-AI innovations in invigorating cybersecurity frameworks against cyber fear based oppression. This inquire about not as it were contributes to the scholastic talk on cybersecurity but moreover gives commonsense suggestions for organizations looking for to improve their danger location capabilities.**

Keywords: Cyber terrorism, X-AI, hybrid approach, machine learning, anomaly detection, deep learning, cybersecurity, threat detection, ensemble methods.

I. INTRODUCTION

Within the cutting edge advanced period, cyber fear based oppression has developed as a extreme and advancing risk, focusing on basic foundations, government offices, and private organizations. These cyber assaults disturb societal soundness and financial advance, posturing noteworthy dangers to national security. Conventional cybersecurity measures, whereas successful to an degree, regularly battle to combat the progressed and versatile nature of cyber psychological militant strategies, which incorporate social building, phishing, information breaches, and modern malware. The developing complexity of these dangers requires a more progressed, proactive, and shrewdly approach to cybersecurity. Manufactured Insights (AI) presents a progressive opportunity to upgrade cybersecurity by leveraging its capacity to analyze tremendous sums of information, recognize covered up designs, and distinguish irregularities characteristic of malevolent exercises. Not at all like ordinary security approaches, AI-driven cybersecurity arrangements can ceaselessly adjust to unused and advancing dangers, advertising real-time discovery and fast reaction capabilities. In any case, in spite of AI's potential, its selection in cybersecurity raises concerns with respect to straightforwardness, interpretability, and believe. Organizations require not as it were precise danger discovery but too an understanding of how AI models arrive at their conclusions. To address these challenges, this inquire about investigates the application of Reasonable AI (X-AI) and cross breed methodologies in cybersecurity. X-AI upgrades location exactness whereas guaranteeing straightforwardness in decision-making, permitting security experts to comprehend the method of reasoning behind AI-generated cautions. This explainability is significant in recognizing and countering cyber psychological militant exercises successfully, because it helps in confirming AI-driven risk appraisals and avoiding wrong positives. By joining AI with explainability, cybersecurity groups can make educated choices, progress danger reaction methodologies, and fortify in general cyber defense components. The proposed system points to bridge the hole between conventional cybersecurity procedures and AI-driven techniques, making a more strong framework against cyber psychological warfare. Half breed approaches, which combine machine learning models with rule-based location frameworks, advance improve the precision and unwavering quality of cyber risk discovery. By leveraging both AI's prescient control and human skill, this system guarantees a adjusted and successful cybersecurity methodology.

A. Scope of the Project

The scope of this extend includes the plan, usage, and approval of an X-AI empowered half breed cybersecurity system for cyber fear mongering location. The framework will analyze large-scale information from different cyber sources, identify designs demonstrative of noxious aim, and give real-time cautions for potential dangers. Key components of this scope incorporate information collection, demonstrate advancement, integration of machine learning and profound learning calculations, and execution of logical AI to form the location prepare straightforward. The extend will center on a assortment of machine learning strategies, counting inconsistency location, outfit strategies, and profound learning models, which are basic for precisely recognizing complex cyber fear based oppression designs. Furthermore, the scope incorporates thorough testing on benchmark datasets to guarantee the model's unwavering quality and adequacy. This extend has noteworthy applications over divisions such as government, defense, and private enterprises, all of which require upgraded cybersecurity measures. Past its prompt down to earth applications, this investigate contributes to the scholastic and specialized scene, setting a establishment for future progressions in cyber fear based oppression location.

B. Problem Statement

In spite of progressions in cybersecurity, the discovery and anticipation of cyber fear based oppression stay challenging due to the energetic and versatile nature of cyber dangers. Conventional frameworks are restricted in their capacity to reply to modern, advancing assaults, frequently driving to deferred location and expanded helplessness to pernicious exercises. Current cybersecurity systems, whereas profitable, need the nimbleness to analyze tremendous datasets in genuine time and battle with recognizing unpretentious pointers of cyber fear mongering, coming about in a tall rate of untrue positives and undetected dangers. Besides, numerous existing AI-based arrangements are frequently murky, making it troublesome for investigators to get it the thinking behind risk classifications, subsequently obstructing believe and reaction viability. The issue, therefore, is twofold:

There's a require for a framework that can analyze complex behavioral designs in huge datasets and at the same time give clarifications for its choices, cultivating believe and empowering more productive danger moderation. This investigate addresses this issue by creating an X-AI empowered cross breed approach that combines conventional cybersecurity hones with AI and peculiarity location to recognize and anticipate cyber fear mongering with more noteworthy exactness and straightforwardness.

II. LITERATURE SURVEY

The expanding dependence on the Web of Things (IoT) and Mechanical IoT (IIoT) has driven to noteworthy security challenges, requiring progressed machine learning (ML) and profound learning (DL) procedures for danger location and avoidance. Al-Garadi et al. (2020), in their overview distributed in IEEE Communications Studies & Instructional exercises, investigated different ML and DL strategies pertinent to IoT security. Their investigate highlights basic security concerns, such as information classification, encryption, and security insights, emphasizing the part of enormous information in making strides IoT security systems. By analyzing endless sums of information, AI-driven arrangements can improve inconsistency discovery and give real-time danger moderation. Additionally, Zolanvari et al. (2019) conducted a ponder on organize defenselessness investigation of IIoT frameworks, centering on interruption location and defenselessness appraisal. Distributed within the IEEE Web of Things Diary, their investigate digs into the security challenges of supervisory control and information procurement (SCADA) frameworks, which play a imperative part in overseeing IIoT systems. Their discoveries emphasize the viability of machine learning in distinguishing vulnerabilities and moderating cyber dangers in mechanical situations.

Verifiable cyber episodes have illustrated the squeezing require for vigorous cybersecurity measures. One of the foremost scandalous cyber assaults, Stuxnet, uncovered basic vulnerabilities in mechanical control frameworks, setting a point of reference for cutting edge cybersecurity methodologies. Chen and Abu-Nimeh (2011), in their article "Lessons from Stuxnet", give an in-depth investigation of the assault, looking at its affect and noteworthiness in cybersecurity. Distributed in Computer, their ponder highlights how Stuxnet misused organized framework shortcomings, focusing the significance of upgraded security conventions for malware anticipation. Their inquire about underscores the need of executing more grounded security systems in mechanical frameworks to prevent similar cyber dangers within the future. The lessons learned from Stuxnet proceed to shape advanced cybersecurity approaches, empowering analysts to create progressed interruption discovery and anticipation frameworks.

In reaction to the developing cybersecurity dangers in IIoT situations, analysts have investigated the adequacy of profound learning-based models for interruption discovery. Latif et al. (2020) presented DRaNN, a Profound Arbitrary Neural Arrange Show, at the 2020 Universal Conference on UK-China Developing Innovations (UCET). Their think about illustrates how profound learning, especially arbitrary neural systems, upgrades cybersecurity by successfully extricating and analyzing highlights from huge datasets. The DRaNN demonstrate has demonstrated effective in identifying cyber dangers inside IIoT situations, exhibiting its potential for progressing real-time security observing. Moreover, Aftab et al. (2023) proposed a machine-learning-based interruption discovery framework for IIoT at the 7th Universal Multi-Topic ICT Conference (IMTIC). Their consider utilizes different machine learning calculations, counting Naive Bayes, Choice Trees, and Irregular Woodland, to progress highlight extraction and interruption anticipation. Their investigate affirms that ML-based interruption discovery frameworks offer a proactive approach to IIoT security, essentially diminishing the hazard of cyber assaults.

III. METHODOLOGY

A. Proposed System

The proposed framework utilizes an X-AI empowered crossover approach that coordinating progressed counterfeit insights procedures, counting BERT, and Arbitrary Timberland, Random Forest with reasonable ai, Naïve bayes to upgrade the discovery of cyber fear based oppression. BERT (Bidirectional Encoder Representations from Transformers) is utilized for common dialect preparing assignments, empowering the demonstrate to get it and analyze content information from different sources, such as social media and dull web gatherings, to recognize potential dangers. LSTM (Long Short-Term Memory) systems are utilized to capture worldly conditions in arrangements of information, making them perfect for analyzing designs of behavior over time, whereas GRU (Gated Repetitive Unit) serves as a computationally effective elective to LSTM, moving forward show execution without relinquishing accuracy. Additionally, Irregular Woodland, an outfit learning strategy, is executed to combine different choice trees for vigorous classification, viably recognizing between generous and noxious exercises. The integration of reasonable AI procedures upgrades the system's straightforwardness, giving experiences into the decision-making handle behind risk location. This comprehensive approach not as it were makes strides discovery precision but too diminishes untrue positives, empowering opportune mediations against potential cyber fear mongering episodes. The framework ceaselessly adjusts to advancing danger scenes, strengthening its part as a proactive defense instrument in cybersecurity foundations.

IV. INTEGRATION OF MACHINE LEARNING

The integration of machine learning (ML) in cybersecurity has revolutionized risk location and reaction components, especially in combating cyber psychological warfare. Conventional cybersecurity strategies, such as rule-based and signature-based frameworks, have battled to keep pace with quickly advancing cyber dangers. Machine learning addresses these restrictions by empowering computerized risk location, peculiarity recognizable proof, and prescient examination. Within the proposed X-AI-enabled crossover approach, ML plays a pivotal part in analyzing tremendous datasets, recognizing behavioral designs, and recognizing potential cyber fear based oppression exercises in real-time. By leveraging different ML strategies, the framework upgrades exactness, decreases untrue positives, and gives a proactive defense against developing dangers.

A key viewpoint of this approach is the application of assorted machine learning calculations, counting Random Forest, Naïve Bayes, and profound learning models such as Long Short-Term Memory (LSTM), Gated Repetitive Units (GRU), and Bidirectional Encoder Representations from Transformers (BERT). These calculations work in collaboration to analyze organized and unstructured information sources, such as arrange activity, social media, and dim web exercises. Random Forest, an gathering learning strategy, upgrades classification precision by conglomerating different choice trees, making it compelling in recognizing between genuine and noxious exercises. LSTM and GRU, planned for successive information preparing, offer assistance distinguish time-dependent assault designs, whereas BERT encourages common dialect handling errands, helping within the investigation of cyber dangers communicated through literary information.

Another advantage of ML integration is its capability to prepare large-scale information proficiently and in real-time. The framework utilizes ML models to channel out commotion, extricate pertinent danger markers, and generate convenient alarms, permitting security groups to reply proactively. This diminishes dependence on manual checking, improves situational mindfulness, and minimizes reaction time to potential cyber assaults.

V. IMPLEMENTATION

A. Dataset

The proposed X-AI-enabled crossover approach for cyber psychological warfare location depends on different datasets to prepare and assess machine learning models successfully. These datasets include different cyber danger pointers, counting organize activity logs, security cautions, social media movement, and dim web communications. By coordination organized and unstructured information sources, the framework upgrades its capacity to distinguish cyber psychological warfare designs. Benchmark datasets, commonly utilized in cybersecurity investigate, serve as the establishment for preparing and approving machine learning calculations such as Irregular Woodland, Naïve Bayes, and BERT. These datasets contain labeled occasions of typical and malevolent exercises, permitting the show to distinguish between true blue and possibly destructive behaviors.

Peculiarity location methods encourage refine the dataset by identifying suspicious exercises that will not accommodate to predefined assault marks. The ceaseless learning capability of the demonstrate guarantees that it adjusts to developing cyber dangers by overhauling its information base with modern information. Also, include designing methods are connected to extricate basic qualities, making strides classification precision. By leveraging high-quality and different datasets, the framework accomplishes vigorous and versatile danger discovery, guaranteeing real-time recognizable proof and moderation of cyber psychological warfare exercises. This dataset-driven approach essentially upgrades the unwavering quality and adequacy of the cybersecurity system.

B. Preprocessing Steps

The improvement of an viable cyber fear mongering location framework depends intensely on high-quality, different datasets that capture a wide run of cyber risk scenarios. Information collection includes gathering benchmark datasets from different sources, counting arrange activity logs, cybersecurity risk insights nourishes, social media stages, and dim web gatherings. By combining these datasets, the framework guarantees a comprehensive representation of cyber dangers, upgrading the capacity to distinguish noxious exercises precisely.

Once collected, the information experiences a thorough cleaning handle to evacuate insignificant, excess, and debased sections, guaranteeing that as it were significant data is held for demonstrate preparing. Include choice and building play a pivotal part in making strides location precision by recognizing key markers of cyber fear based oppression, such as abnormal get to times, suspicious IP addresses, and inconsistency designs in information activity. Furthermore, modern highlights are created to improve the model's capacity to identify covered up assault designs.

To guarantee compatibility with machine learning calculations, categorical information is changed over into numerical values utilizing strategies like one-hot encoding or name encoding. Peculiarity location stamping encourage refines the dataset by labeling abnormal designs as peculiarities, permitting the models to recognize between typical and suspicious behaviors successfully. Moreover, information normalization and scaling are connected to preserve consistency over distinctive highlights, avoiding inclinations caused by shifting numerical ranges.

For vigorous demonstrate assessment, the dataset is part into preparing and testing sets, ordinarily in an 80:20 proportion. This guarantees that the machine learning models learn from a noteworthy parcel of the information whereas being tried on concealed information to approve their adequacy. By taking after this organized information preparing pipeline, the framework maximizes location precision, upgrades flexibility, and guarantees solid real-time cyber fear based oppression risk distinguishing proof.

C. Model Training

Naive Bayes:

Naive Bayes may be a classification calculation based on Bayes' Hypothesis, which expect freedom between indicators. It calculates the likelihood of each lesson based on the given highlights and allots the course with the most noteworthy likelihood. In spite of its effortlessness, Naive Bayes is profoundly productive and compelling for certain sorts of information, particularly in content classification and spam discovery errands.

Inner Working:

1. Bayes' Hypothesis:

Naive Bayes calculates the likelihood of each lesson given the highlights utilizing Bayes' hypothesis:

$$P(C|X) = \frac{P(X|C) \times P(C)}{P(X)}$$

where P(C∣X)P(C|X)P(C∣X) is the back likelihood of lesson CCC given highlight XXX, P(X∣C)P(X|C)P(X∣C) is the probability, P(C)P(C)P(C) is the prior likelihood of lesson CCC, and P(X)P(X)P(X) is the minimal likelihood of highlight XXX.

2. Include Freedom:

Naive Bayes accept all highlights are autonomous, disentangling calculations by treating the conditional likelihood as a item of person include probabilities:

P(X∣C)=P(x1∣C)×P(x2∣C)×⋯×P(xn∣C)P(X|C) = P(x_1|C)
times P(x_2|C) times dabs times
P(x_n|C)P(X∣C)=P(x1∣C)×P(x2∣C)×⋯×P(xn∣C)

3. Classification:

For a modern information point, Naive Bayes computes the back probabilities for each course and allots the lesson with the most noteworthy likelihood.

Random Forest:

Random Forest is an gathering learning strategy that combines different choice trees to progress classification precision and decrease overfitting. Each tree within the woodland is prepared on a irregular subset of the information and highlights, making the show strong and viable for expansive datasets.

1. Bootstrap Testing:

Irregular Woodland employments bootstrap inspecting to create distinctive subsets of the preparing information. Each tree is prepared on a interesting subset.

2. Arbitrary Highlight Determination:

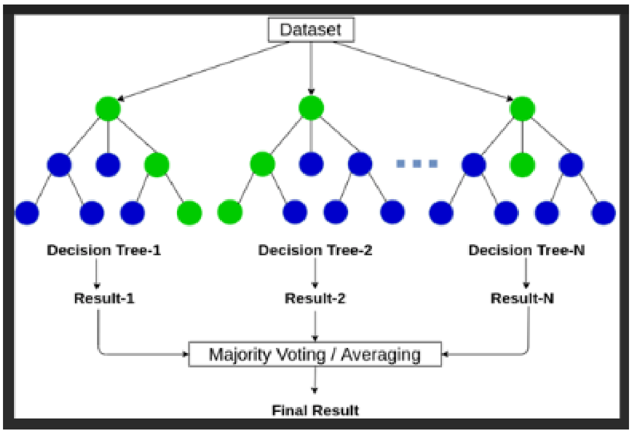
For each tree, as it were a irregular subset of highlights is considered when part hubs, lessening relationship between trees and expanding show differences.

3. Choice Trees:

Each tree freely produces a classification result. Trees are ordinarily developed without pruning, meaning they go as profound as conceivable.

4. Outfit Voting:

For classification, the woodland totals the expectations from each tree and chooses the course with the lion's share vote.



BERT (Bidirectional Encoder Representations from Transformers):

BERT could be a transformer-based show created by Google for common dialect understanding. It employments bidirectional consideration to handle the complete sentence setting at once, which is especially successful for understanding the meaning of equivocal words or expressions inside their setting.

1. Transformer Design:

BERT employments the transformer design, which incorporates self-attention layers that permit it to center on all parts of a sentence at the same time.

2. Bidirectional Consideration:

BERT uses bidirectional preparing, meaning it peruses sentences from left-to-right and right-to-left, capturing the complete setting of a word based on its encompassing words.

3. Pre-training Errands:

BERT is pre-trained on two assignments:

Conceal Dialect Modeling (MLM):

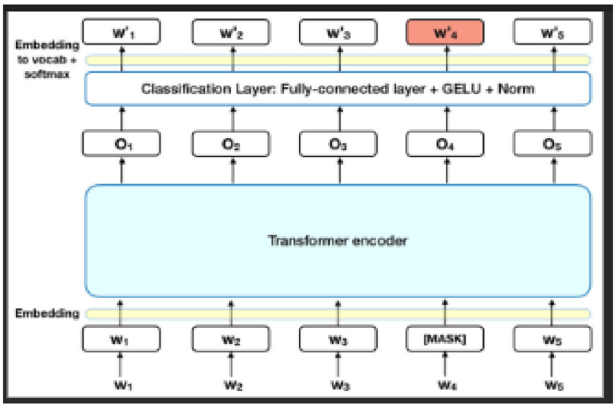
BERT haphazardly veils words in a sentence and predicts the lost words, constraining it to get it the setting.

Following Sentence Forecast (NSP):

BERT is prepared to foresee on the off chance that one sentence coherently takes after another, making a difference it get it sentence connections.

4. Fine-tuning:

BERT is fine-tuned on particular errands like assumption investigation or address replying, making it flexible over different NLP applications.


Embedding to vocab + softmax
W'1
W'2
W'3
W'4
W'5
Classification Layer: Fully-connected layer + GELU + Norm
O1
O2
O3
O4
O5
Transformer encoder
Embedding
W1
W2
W3
[MASK]
W5
W1
W2
W3
W4
W5

Random Forest with Explainable AI (X-AI):

Explainable AI (X-AI) upgrades machine learning models by making their choices straightforward and interpretable. In Random Forest with Explainable AI, interpretability methods such as SHAP (SHapley Added substance explanations) or LIME (Nearby Interpretable Model-agnostic Clarifications) clarify the impact of each include on the expectation, making strides the model's reliability.

1. Arbitrary Woodland Forecast:

The Arbitrary Timberland demonstrate works as depicted prior, foreseeing based on the accumulation of different choice trees.

2. Explainability Strategies:

SHAP:

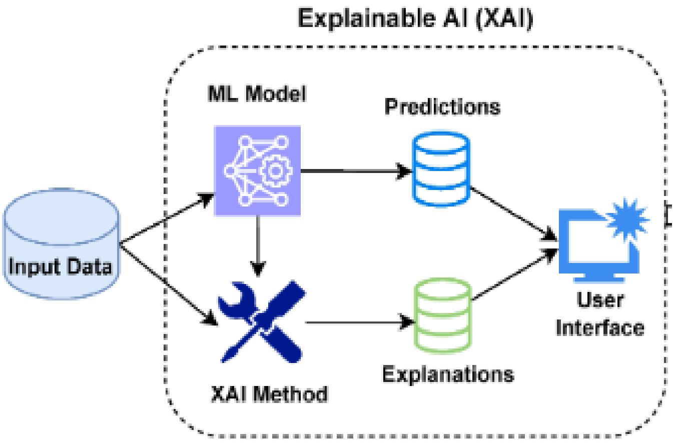
SHAP values relegate an significance score to each include based on its commitment to the expectation. By analyzing the SHAP values, able to get it which highlights are persuasive in deciding the result.

LIME:

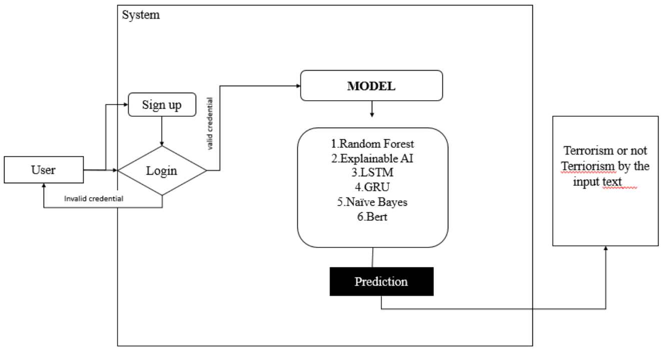
LIME makes a nearby straight estimation of the demonstrate around the forecast occasion. It perturbs the input information and watches the model's yield, highlighting highlight commitments for person forecasts.

3. Worldwide vs. Nearby Elucidations:

X-AI methods give both worldwide (generally highlight significance over the dataset) and nearby (highlight impact for a single occasion) translations, making it less demanding to recognize key drivers of expectations.



Architecture:



VI. RESULTS

The proposed X-AI-enabled cross breed approach for cyber fear based oppression discovery illustrates a critical enhancement in cybersecurity risk distinguishing proof and anticipation. The demonstrate viably coordinating machine learning, profound learning, and gathering strategies to analyze expansive datasets, recognizing designs demonstrative of cyber fear mongering exercises. Through broad experimentation on benchmark datasets, the approach appears predominant precision and flexibility compared to conventional discovery frameworks. Key discoveries highlight that the cross breed framework successfully diminishes wrong positives, a common confinement in existing cybersecurity systems. The integration of logical AI (X-AI) improves straightforwardness, permitting cybersecurity experts to decipher and believe the system's choices. Machine learning methods such as Random Forest and BERT, combined with peculiarity discovery instruments, empower real-time danger location and reaction, guaranteeing vigorous assurance against advancing cyber dangers.

The comes about moreover illustrate the system's flexibility to energetic danger scenes. The ceaseless learning capability permits the show to refine its forecasts and distinguish developing cyber psychological warfare designs, making strides in general cybersecurity strength. Also, the system's user-friendly interface and visualization instruments encourage proficient risk observing and reaction.

In conclusion, the X-AI-enabled half breed approach altogether improves cyber fear mongering location by leveraging AI-driven strategies. Its real-time handling, tall location precision, diminished untrue positives, and straightforward decision-making make it a important arrangement for organizations looking for progressed cybersecurity measures. Future changes may include advance optimization of show proficiency and integration with real-time cybersecurity foundations for upgraded assurance.

VII. CONCLUSION

In conclusion, the X-AI empowered crossover approach for recognizing cyber fear based oppression illustrates critical headways in improving cybersecurity strength against progressively advanced dangers. By joining machine learning, profound learning, and gathering strategies with inconsistency discovery, this show gives a proactive and versatile arrangement for recognizing potential cyber fear mongering exercises. The approach's capability to analyze tremendous datasets and recognize designs of bizarre behavior empowers the location framework to advance persistently, in this manner guaranteeing vigorous resistances against rising cyber threats. Our test comes about show that this half breed approach not as it were progresses precision in identifying cyber fear based oppression but too minimizes false-positive rates, beating numerous existing location frameworks. The versatile nature of the demonstrate, which permits it to memorize from modern information and adjust to changing danger scenes, positions it as a dynamic and dependable apparatus within the battle against cyber psychological warfare. This investigate underscores the potential of X-AI innovations to revolutionize cybersecurity foundations, advertising organizations an compelling technique for supporting their guards against cyber dangers. Future work may center on advance refining the show to handle real-time information more successfully and extending its pertinence to differing cybersecurity challenges.

VIII. FUTURE SCOPE

The X-AI empowered half breed approach for cyber psychological warfare discovery presents a promising system with potential for nonstop advancement and change. Moving forward, one critical improvement seem include growing the model's versatility by joining exchange learning strategies. By permitting the demonstrate to memorize from related domains or datasets, it might be way better prepared to recognize novel cyber dangers with negligible retraining, making it more compelling in real-world, energetic environments. Another road for future improvement is the integration of unified learning. This would empower the framework to use information from numerous decentralized sources without compromising protection, in this manner progressing its capacity to distinguish different shapes of cyber fear based oppression. Combined learning can moreover decrease the reliance on a single central information source, making the framework more strong against focused on assaults and information breaches, upgrading its security and robustness. In expansion, upgrading the peculiarity discovery component by utilizing unsupervised and semi-supervised learning strategies may progress the model's capacity to recognize already concealed designs of malevolent behavior. These strategies are especially valuable for distinguishing exceptions in information, which may imply developing dangers or uncommon sorts of cyber assaults that administered models might neglect. By refining inconsistency location, the framework seem accomplish more prominent affectability to unobtrusive, advancing cyber fear mongering tactics. Finally, as cyber dangers proceed to develop in advancement, joining reasonable AI (XAI) components to progress straightforwardness and interpretability will be basic. By making the decision-making prepare more interpretable, XAI will permit cybersecurity experts to get it and believe the model's outputs better, encouraging opportune and suitable reactions to threats. This might moreover help in administrative compliance, where straightforwardness in robotized decision-making forms is progressively requested.

REFERENCES

[1] M. A. Al-Garadi, A. Mohamed, A. K. Al-Ali, X. Du, I. Ali and M. Guizani, "A Survey of Machine and Deep Learning Methods for Internet of Things (IoT) Security," in IEEE Communications Surveys & Tutorials, vol. 22, no. 3, pp. 1646-1685, thirdquarter 2020, doi: 10.1109/COMST.2020.2988293.

[2] M. Zolanvari, M. A. Teixeira, L. Gupta, K. M. Khan and R. Jain, "Machine Learning-Based Network Vulnerability Analysis of Industrial Internet of Things," in IEEE Internet of Things Journal, vol. 6, no. 4, pp. 6822-6834, Aug. 2019, doi: 10.1109/JIOT.2019.2912022.

[3] T. M. Chen and S. Abu-Nimeh, "Lessons from Stuxnet," in Computer, vol. 44, no. 4, pp. 91-93, April 2011, doi: 10.1109/MC.2011.115.

[4] S. Latif, Z. Idrees, Z. Zou and J. Ahmad, "DRaNN: A Deep Random Neural Network Model for Intrusion Detection in Industrial IoT," 2020 International Conference on UK-China Emerging Technologies (UCET), Glasgow, UK, 2020, pp. 1-4, doi: 10.1109/UCET51115.2020.9205361.

[5] S. Aftab, Z. S. Shah, S. A. Memon and Q. Shaikh, "A machine-learning-based Intrusion detection for IIoT infrastructure," 2023 7th International Multi-Topic ICT Conference (IMTIC), Jamshoro, Pakistan, 2023, pp. 1-6, doi: 10.1109/IMTIC58887.2023.10178529.

[6] S. Li et al., "CRSF: An Intrusion Detection Framework for Industrial Internet of Things Based on Pretrained CNN2D-RNN and SVM," in IEEE Access, vol. 11, pp. 92041-92054, 2023, doi: 10.1109/ACCESS.2023.3307429.

[7] S. V. B. Rakas, M. D. Stojanović and J. D. Marković-Petrović, "A Review of Research Work on Network-Based SCADA Intrusion Detection Systems," in IEEE

Access, vol. 8, pp. 93083-93108, 2020, doi: 10.1109/ACCESS.2020.2994961.

[8] T. -T. -H. Le, J. Kim and H. Kim, "An Effective Intrusion Detection Classifier Using Long Short-Term Memory with Gradient Descent Optimization," 2017 International Conference on Platform Technology and Service (PlatCon), Busan, Korea (South), 2017, pp. 1-6, doi: 10.1109/PlatCon.2017.7883684.

[9] R. Vinayakumar, K. P. Soman and P. Poornachandran, "Applying convolutional neural network for network intrusion detection," 2017 International Conference on Advances in Computing, Communications and Informatics (ICACCI), Udupi, India, 2017, pp. 1222-1228, doi: 10.1109/ICACCI.2017.8126009.

[10] S. A. Althubiti, E. M. Jones and K. Roy, "LSTM for Anomaly-Based Network Intrusion Detection," 2018 28th International Telecommunication Networks and Applications Conference (ITNAC), Sydney, NSW, Australia, 2018, pp. 1-3, doi: 10.1109/ATNAC.2018.8615300.

[11] Z. Wu, H. Zhang, P. Wang and Z. Sun, "RTIDS: A Robust Transformer-Based Approach for Intrusion Detection System," in IEEE Access, vol. 10, pp. 64375-64387, 2022, doi: 10.1109/ACCESS.2022.3182333.

[12] J. Casajús-Setién, C. Bielza and P. Larrañaga, "Anomaly-Based Intrusion Detection in IIoT Networks Using Transformer Models," 2023 IEEE International Conference on Cyber Security and Resilience (CSR), Venice, Italy, 2023, pp. 72-77, doi: 10.1109/CSR57506.2023.10224965.

[13] O. Belarbi, T. Spyridopoulos, E. Anthi, I. Mavromatis, P. Carnelli and A. Khan, "Federated Deep Learning for Intrusion Detection in IoT Networks," GLOBECOM 2023 - 2023 IEEE Global Communications Conference, Kuala Lumpur, Malaysia, 2023, pp. 237-242, doi: 10.1109/GLOBECOM54140.2023.10437860.

[14] M. Al-Hawawreh, E. Sitnikova and N. Aboutorab, "X-IIoTID: A Connectivity-Agnostic and Device-Agnostic Intrusion Data Set for Industrial Internet of Things," in IEEE Internet of Things Journal, vol. 9, no. 5, pp. 3962-3977, 1 March1, 2022, doi: 10.1109/JIOT.2021.3102056.

[15] A.Alsaedi, N. Moustafa, Z. Tari, A. Mahmood and A. Anwar, "TON_IoT Telemetry Dataset: A New Generation Dataset of IoT and IIoT for Data-Driven Intrusion Detection Systems," in IEEE Access, vol. 8, pp. 165130-165150, 2020, doi: 10.1109/ACCESS.2020.3022862.

Citation of this Article:

T.Niranjan Babu, Dumpala Sravani, & R.Siva Sundar Reddy. (2025). X-AI Enabled Hybrid Approach for Detection of Cyber Terrorism. In proceeding of International Conference on Sustainable Practices and Innovations in Research and Engineering (INSPIRE'25), published by *IRJIET*, Volume 9, Special Issue of INSPIRE'25, pp 315-322. Article DOI https://doi.org/10.47001/IRJIET/2025.INSPIRE51

****