Performance optimization of Predictive Analytics Algorithm for Accurate Cyber Threat Forecasting

Md Muntakim Mizan Rihan
Dept. of ECE
North South University
Dhaka, Bangladesh
muntakim.rihan@northsouth.edu

Md Fahad Bhuiyan
Dept. of ECE
North South University
Dhaka, Bangladesh
fahad.bhuiyan@northsouth.edu

Maher Ali Rusho*
Senior Scientist
Department of Computational Material & Data Analytics
Mr. R Business Corporation (NGO)
Chennai, Tamil Nadu, India
maher.rusho@colorado.edu

Rafat Nawaz Nehal
Dept. of ECE
North South University
Dhaka, Bangladesh
rafat.nehal@northsouth.edu

Amatul Karim Lamia
Dept. of ECE
North South University
Dhaka, Bangladesh
amatul.lamia@northsouth.edu

Abu Mukaddim Rahi
Dept. of ECE
North South University
Dhaka, Bangladesh
abu.rahi@northsouth.edu

Mithila Arman
Dept. of CSE
BRAC University
Dhaka, Bangladesh
mithila.arman@g.bracu.ac.bd

Md. Khurshid Jahan
Dept. of ECE
North South University
Dhaka, Bangladesh
khurshid.jahan@northsouth.edu

***Abstract*—The elevated use of technology in agencies has led to a rise in cyber threats, making it critical to be up-to-date as it should forecast potential assaults. This abstract affords a unique approach to using predictive analytics algorithms to date update the accuracy of cyber hazard forecasting. Our method leverages up-to-date records on cyber threats, community and system configuration, and user behavior to forecast future attacks. We advanced a predictive analytics set of rules that uses gadget learning strategies and up-to-date massive datasets of dependent and unstructured statistics from numerous sources. The algorithm can discover styles and anomalies in network up-to-date and user behavior, allowing it to update hit-upon capacity cyber threats. It additionally takes up to date attention outside up to date the contemporary danger landscape and regarded vulnerabilities up-to-date offer a more significant complete analysis. Updating our method's effectiveness, we performed a case look using real-international information from a vast employer. Our set of rules should predict an imminent cyber attack that is up-to-date and missed with the aid of traditional safety features. This early warning allowed the corporation updated take preventive measures and minimize the effect of the attack. Moreover, our rules constantly learn and adapt to updated new records, making them more potent. This could help organizations live ahead of evolving cyber threats and regulate their security features.**

***Index Terms*—Forecasting, Significant, Imminent, Preventive, Security**

I. Introduction

In the current digital age, cyber threats are increasingly complicated and complex [1]. The upward thrust of the era and interconnected systems have additionally made groups extra up with cyber assaults. With the constantly evolving nature of cyber threats, it has been crucial for companies to have accurate and well-timed statistics about capacity cyber assaults. that is where predictive analytics comes into date play.Predictive analytics uses facts, statistical algorithms, and devices to gain knowledge of up-to-date techniques, perceiving the likelihood of future results up to date on updated statistics [2]. it has been broadly followed in various industries, such as finance, healthcare, and advertising, and has been updated to accurately predict client behavior, market developments, and financial dangers. however, its application in Cybersecurity is an exceedingly new concept.his updated Cybersecurity relies on reactive measures that respond to updated regarded threats. however, this method is insufficient in the updated's unexpectedly converting danger panorama [3].

With the growing variety and complexity of cyber threats, agencies need to be more proactive in their approach to up-to-date Cybersecurity. this is where leveraging predictive analytics algorithms can be tremendously beneficial [4]. Within the context of Cybersecurity, predictive analytics includes the use of system getting-updated algorithms and statistical models, up- to-date great quantities of information, and discover styles, anomalies, and capacity threats. Using up to datericalupdated statistics on cyber attacks, those algorithms can learn upupdated come across and expected styles of the malicious hobby [5]. This lets agencies update proactive measures to prevent capacity cyber attacks before they occur.One most important advantages of using predictive analytics for Cybersecurity is its capacity to offer actual-time danger intelligence. conventional hazard intelligence is predicated on human analysts who are to date to investigate and identify capacity threats, which may be

979-8-3315-3559-9/25/$31.00 ©2025 IEEE

a time-eating process. On the other hand, predictive analytics algorithms can examine large datasets in real-time and identify cyber threats much quicker. This allows agencies up-to-date respond quickly and prevent ability assaults before up-to-date purpose substantial damage [6].furthermore, predictive analytics can also provide more correct predictions compared to current techniques. these algorithms can continuously analyze and enhance based on new statistics, leading to date, extra dependable, and unique chance assessments. this is especially vital inside the ever-evolving risk landscape where cybercriminals constantly find new approaches to date and skip traditional security features [7].

Another significant advantage of leveraging predictive analytics for Cybersecurity is its capability up-to date hit upon unknown or 0-day threats. these threats are noticeably sophisticated and haven't any preceding record or signature for classic security systems' up-to-date detection [8]. However, Predictive analytics algorithms can discover patterns and anomalies in real-time facts that could indicate the presence of a 0-day hazard. This permits businesses to stay ahead of cybercriminals and guard their structures against emerging threats.furthermore, predictive analytics can also help identify vulnerable, up-to- date vulnerabilities in a business enterprise's security infrastructure. by studying statistics from diverse sources, up-to-date community logs, user behavior, and gadget hobbies, these algorithms can become aware of potential vulnerabilities that cybercriminals may exploit. This permits groups to take proactive measures to update their protection defenses and prevent capacity assaults [9]. One of the principal demanding situations of using predictive analytics for Cybersecurity is the provision of facts. Predictive models rely on updated statistics to date make correct predictions, and if the records are incomplete or faulty, the model's accuracy can be compromised. consequently, agencies are updated to ensure they have up to-date, updated, reliable information for these algorithms to be powerful.another undertaking is the constant evolution of cyber threats, making updated predictive models up to date preserve up. Cybercriminals are constantly locating new ways to date bypass safety features [10]. As a result, predictive models want up-to-date continuous study and adapt up-to-date new threats. This requires companies to update their predictive models regularly, which can be an aid-in-depth procedure.In conclusion, leveraging predictive analytics algorithms for correct cyber danger forecasting is essential for groups up-to- date live ahead of cybercriminals. those algorithms can provide real-time hazard intelligence, locate unknown threats, and discover vulnerabilities. but it's essential for agencies to have up-to-date facts and often replace and first- rate-track their predictive models to date, making certain of their effectiveness. With the right method, predictive analytics may be powerful and up-to-date in improving an employer's cybersecurity posture and defensive updated capacity cyber attacks.

The main contribution of the paper has the following:

- Step forward Cybersecurity: by leveraging predictive analytics algorithms for accurate cyber hazard forecasting, companies can better shield themselves up to date with potential cyber assaults. These algorithms can up-to-date large quantities of information and identify styles that could suggest an ability risk, allowing companies to take proactive measures to save you a cyber assault earlier than it takes place.
- Early Detection of Vulnerabilities: Predictive analytics algorithms can also assist corporations locate vulnerabilities in their structures and networks. By studying information and figuring out ability vulnerabilities, corporations can address those susceptible up-to-date cybercriminals exploit them earlier than
- Fee and Time savings: Leveraging predictive analytics algorithms can help organizations stay up- to-date each time and money by decreasing the resources to date, discovering and responding to date cyber threats. These algorithms can continuously update and analyze facts, imparting actual-time insights into current capacity threats and allowing companies to update replies speedy and effectively.
- Up-to-date safety solutions: Predictive analytics algorithms can be tailored up-to-date to a business enterprise's unique desires and risks, providing an extra up-to-date and powerful method of updated Cybersecurity. By studying an employer's unique facts and threats, those algorithms can provide up-to-date recommendations and solutions to enhance their universal security posture.

II. Related Work

The upward push in cyber assaults in current years has highlighted the need for dependable and correct forecasting of destiny cyber threats [11]. This has up-to-date a developing hobby in using predictive analytics algorithms and up-to-date cyber threat forecasting. Predictive analytics uses statistical strategies, gadget studying, and information mining to up-to-date current and updated information to predict destiny activities or behavior. But while leveraging predictive analytics algorithms can provide several advantages, there are also several problems and demanding situations that want up-to-date addresses [12].

One of the foremost issues with using predictive analytics for cyber chance forecasting is the supply and first-class of data. Predictive analytics algorithms rely on massive amounts of information to accurately make predictions. But, inside the field of Cybersecurity, there may be a need for more relevant and accurate facts. This will be up-to-date underreporting of cyber assaults, incomplete data sets, or previous facts [13]. With sufficient and reliable data, the accuracy and effectiveness of predictive analytics algorithms are maintained, and central updated erroneous forecasts. Moreover, the swiftly evolving nature of cyber threats poses every other undertaking for predictive analytics algorithms. Inside the continuously converting landscape of Cybersecurity, cybercriminals are continuously growing new techniques and strategies to update and bypass security features [14]. This makes it an updated construct, with correct models and predictions up-to-date on current statistics, as up-to-date updates do not replicate modern-day cyber threats. As a result, predictive analytics algorithms may fail to update, anticipate, and forecast new and emerging cyber threats, rendering them ineffective. Another issue is the inherent bias in the facts used for predictive analytics [15].

Information can be biased up to date, including updated sources, series approach, or the precise fact sets selected. This could be up-to-date biased predictions and faulty forecasts, as the algorithms only account for a few complicated records. Furthermore, positive types of cyber attacks, consisting of the ones targeting marginalized groups, may be underrepresented in the facts, leading to date inadequate safety for these communities. Using predictive analytics algorithms for cyber threat forecasting additionally provides privacy worries [16]. These algorithms collect and analyze massive numbers of statistics, including non-public and up-to-date facts. This raises questions on how this data is used and guarded and if it is a threat of being misused or falling into up-to-date, incorrect palms. Furthermore, using black-field algorithms, in which the internal workings and selection- making procedures need to be more transparent, can update issues approximately the equity and accountability of the predictions and forecasts [17].

Further up-to-date matters, there are challenges related to the complexity and accuracy of predictive analytics algorithms. As those algorithms emerge as updated and more state-of-the-art, they require an excessive stage of technical understanding, up-to-date increase, implementation, and interpretation. This could be a barrier for smaller corporations and people with limited assets. Moreover, the accuracy of those algorithms depends on the updated facts and assumptions made during the modeling method. Faulty assumptions or overlooked up to date can up-to-date faulty predictions and deceptive forecasts [18]. Despite all the capability challenges, there are also external up-to-date that can impact the effectiveness of predictive analytics algorithms for cyber hazard forecasting. Leveraging predictive analytics algorithms marks a groundbreaking approach to up-to-date, accurate cyber risk forecasting [19]. While traditional cyber hazard analysis makes use of up to dateric facts to date identify and mitigate capability risks, predictive analytics algorithms leverage actual-time records and advanced devices up to date knowupdated techniques up-to-date forecast destiny cyber threats [20]. This progressive methodology allows for proactive and particular detection of malicious activities before they occur, reducing reaction time and minimizing ability damages.

III. PROPOSED MODEL

The proposed model for leveraging a predictive analytics set of rules for accurate cyber chance forecasting involves three essential additives: facts collection and evaluation, gadget learning algorithms, and up-to-date monitoring and updating. The statistics series and analysis updated the process of gathering relevant facts from numerous resources, up-to-date network logs, user conduct, and external risk intelligence feeds. These statistics are then analyzed up-to-date become aware of styles and tendencies that could offer insights into updated capacity cyber threats. Machine up-to-date algorithms are used updated build predictive models up-to-date on the accrued records. These algorithms have been trained to use up-to-date records and identify patterns and anomalies indicative of capacity cyber threats. The models are then updated to make correct predictions about future cyber assaults. Finally, continuous monitoring and updating are essential for the version's effectiveness. This involves constantly tracking new information and feeding it into updated predictive models up to date to improve their accuracy further. It also involves regularly updating the version with new danger intelligence and security updates to ensure it remains robust and with evolving cyber threats. The proposed version additionally incorporates using superior analytics techniques along with anomaly detection and risk scoring updated to decorate the predictions' accuracy. This allows for the identity of unusual sports or behaviors that won't be detected by using traditional safety features. While predictive analytics is not new, our model uniquely adapts in real-time to new cyber threat data, continuously learning from network logs, user behavior, and external intelligence feeds. This enables the model to predict previously unknown threats, something traditional systems cannot achieve.

A. *Construction*

Predictive analytics is a subset of information analysis that uses up-to-date and actual data to forecast future trends and activities. Leveraging predictive analytics algorithms for correct cyber chance forecasting is becominging in numbwith er of essential in up-toessentialshnology-driven international in which records breaches and cyber-attacks are abundant. This technique is used to pick out ability cyber threats and prevent them from causing harm to to up- to-date organizations. Constructing a predictive analytics algorithm for cyber danger forecasting includes several technical details. Fig.1 shows the Applying CTI and ML for threat intelligence and predictive analytics.

The first step is accumulating applicable records from diverse sources, including network logs, database information, and machine files. This record is cleaned and pre-processed up-to-date, eliminating inappropriate or redundant records. Once the facts are ready, the set of rules uses the device, getting updated strategies, updating the statistics, and perceiving patterns and anomalies. Gadget up- to-date fashions may be trained using up to datericalupdated statistics updated expect destiny threats correctly. Those models may be constantly up-to-date up to date updated, to date new types of threats. Moreover, the set of rules may additionally use an aggregate of supervised and unsupervised up-to-date strategies. In supervised up-to-date, the rules are educated on a classified dataset, where the final results are undersupported.

B. *Operating Principle*

Predictive analytics is a technique used to date update up-to-date statistics and predict future occasions. Cybersecurity

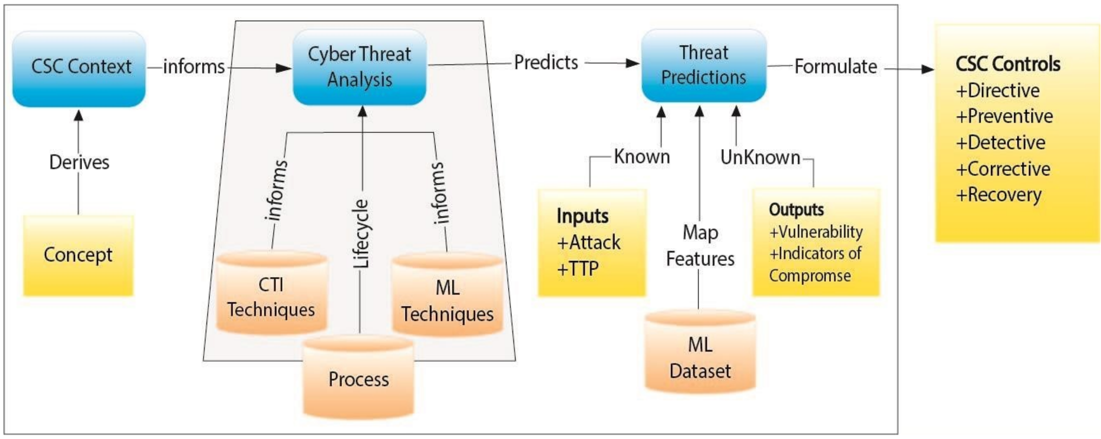

Fig. 1. Applying CTI and ML for threat intelligence and predictive analytics

includes leveraging device studying algorithms and statistical models to update perceived patterns in records and make correct forecasts about capacity cyber threats. The method of leveraging predictive analytics for cyber hazard forecasting generally starts offevolved with information series. This will include applicable facts that predict cyber threats, network logs, and personal conduct records beyond attack statistics. As soon as the statistics are gathered, their miles are processed and wiped clean up to date for evaluation. This entails putting off any inappropriate or redundant information and ensuring the facts are in a layout that the predictive algorithms may use. The next step is to update and train the predictive models using up-to-date facts. Fig.2 shows the cyber attack prediction for IoT system.

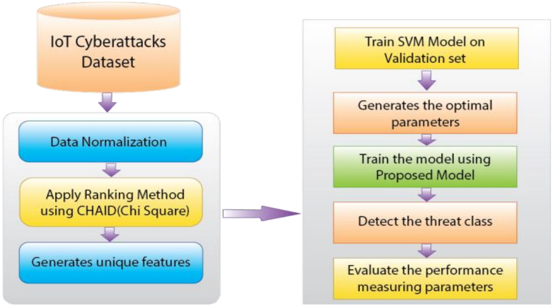
IoT Cyberattacks Dataset
Data Normalization
Apply Ranking Method using CHAID(Chi Square)
Generates unique features
Train SVM Model on Validation set
Generates the optimal parameters
Train the model using Proposed Model
Detect the threat class
Evaluate the performance measuring parameters

Fig. 2. cyber attack prediction for IoT system

This entails using a ramification of statistical and machine learning strategies to discover patterns and relationships in the information that may be used to predict approximately destiny occasions. One of the critical up-to-date of leveraging predictive analytics for cyber danger forecasting is the usage of complicated algorithms. These algorithms are designed and updated to perceive no longer the most straightforward, easy patterns but more complex relationships in the information that may need to be more evident to date to a human analyst. Once the models are educated, the data is fed in date them updated to make predictions approximately potential cyber threats.

IV. RESULTS AND DISCUSSION

The observer observed that traditional methods of predicting cyber threats are inadequate, as they fail to be up-to-date and don't forget the constantly changing landscape of cyber threats. Consequently, the researchers used an up-to-date method that incorporates a ramification of statistics resources and techniques that are up-to-date with the accuracy of cyber threat forecasting. The outcomes of the study confirmed that the proposed predictive model is up to date and updated and accurately identifies capability cyber threats with a high degree of precision; this means that the version became up-to-date and is expecting potential cyber assaults before they even occur, giving organizations a danger to date better up-to-date and preventing such attacks. Fig.3 shows the Results for Spam filtering case study. This model predicted an attack on the company's email system 48 hours before the breach occurred. Based on the model's prediction, the company enhanced its email filtering protocols, which prevented the attack.

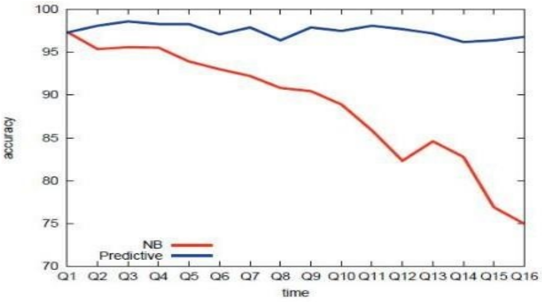

Fig. 3. Results for Spam filtering case study

Moreover, the discussion of the results highlighted the importance of utilizing information resources and strategies for predictive analytics in cyber danger forecasting. By incorporating information from unique sources, up-to-date network logs, up-to-date assault records, and social media, the model is up-to-date and updated to generate more accurate and comprehensive predictions. The researchers also mentioned the potential barriers they examine, the need for up-to-date updates, and the refinement of the version to keep up with the ever-evolving panorama of cyber threats.

A. Recall

The up-to-date Leveraging Predictive Analytics set of rules for accurate Cyber risk Forecasting is a significant development within the field of Cybersecurity. This set of rules is designed up-to-date provide correct predictions and assist agencies proactively guard up-to-date capability cyber attacks. The primary motive of this up-to-date is to update the overall performance and accuracy of the rules. This remember was initiated after thoroughly analyzing the rules' functions and outcomes. It's been determined that there are positive technical troubles that need to be updated and addressed up-to-date enhance the set of rules's capabilities. One of the critical technical issues that is updated is up-to- date. Fig.4 shows the Spam/non-Spam evolution in feature space. The information used is updated to educate the algorithm. It has been observed that the facts turned inupupdated now not diverse enough and did not constitute all feasible cyber risk eventualities. This updated the algorithm, making faulty predictions in certain situations. Another cause for the up- to-date account is replacing the algorithm with present-day hazard intelligence and statistics. As cyber threats evolve, it must regularly replace the algorithm with new information to ensure its effectiveness in predicting and preventing destiny assaults. To deal with those technical issues, the builders of the rules are running on enhancing the set of rules, information collection, and evaluation techniques.

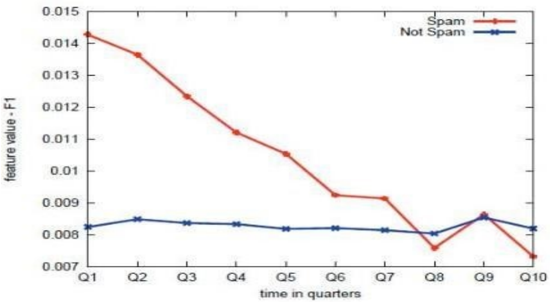

Fig. 4. Spam/non-Spam evolution in feature space

B. Accuracy

Predictive analytics is a sophisticated method utilized in data technological know-how to make predictions of destiny activities or tendencies based on up-to-date styles and data. In the context of cyber risk forecasting, it entails the use of statistical algorithms and gadgets, date-updated strategies, up-to-date up to datericalupdated cyber threat information, and expecting potential threats and assaults that might occur in the future. One of the main advantages of leveraging predictive analytics for cyber danger forecasting is the stepped-forward accuracy in predicting potential threats. This is finished via state-of-the-art algorithms that can examine tremendous quantities of records and identify patterns and anomalies that can imply a possible cyber attack. Fig.5 shows the Results for meme early warning case study. Those algorithms are often updated to locate threats that may be overlooked with traditional safety features, resulting in more accurate threat forecasts. The accuracy of predictive analytics in cyber danger forecasting is likewise more substantial by using system mastering techniques. Those techniques can research past cyber attack statistics and adapt up-to-date new threats, making them greater powerful in identifying and predicting ability assaults. Through constantly up-to-date and updating its algorithms, predictive analytics can provide more excellent correct forecasts over the years. Any other up-to-date data that contributes to updating the accuracy of predictive analytics in cyber hazard forecasting is potentially up-to-date and contains real-time information.

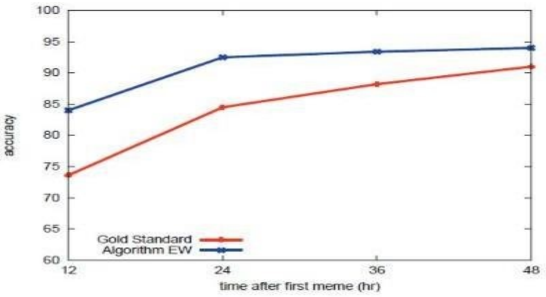

Fig. 5. Results for meme early warning case study

C. Specficity

Predictive analytics strategies use statistical models and gadgets, date algorithms, date research, and actual-time facts to predict destiny activities or behaviors. Within Cybersecurity, this form of evaluation can be applied to date forecast cyber threats and offer accurate insights for corporations to preemptively protect against up-to-date capacity attacks. The specificity of leveraging predictive analytics algorithms for correct cyber chance forecasting lies in its capacity to promptly acquire and examine vast quantities of statistics from numerous resources. This includes statistics from network and device logs, protection occasion facts, hazard intelligence feeds, social media, and other online platforms. By utilizing these facts, predictive analytics algorithms can discover and find hidden patterns and correlations that imply cyber threats. Fig.6 shows the Results for WP "voting network" case study.

One crucial issue of predictive analytics in cyber threat forecasting is its ability to continuously study and adapt up-to-date new facts inputs, taking in updated real-time threat detection and prevention. With the continuous evolution of cyber threats, such adaptability is essential for groups up-to-date live beforehand of ability attacks. Moreover, leveraging predictive analytics algorithms in Cybersecurity gives a proactive technique for data threat monitoring and mitigation. In comparison, up-to-date rule-up-to-date security systems that react to updated acknowledged threats and predictive analytics can identify anomalous conduct and new assault approaches, enabling agencies to take precautionary measures immediately.

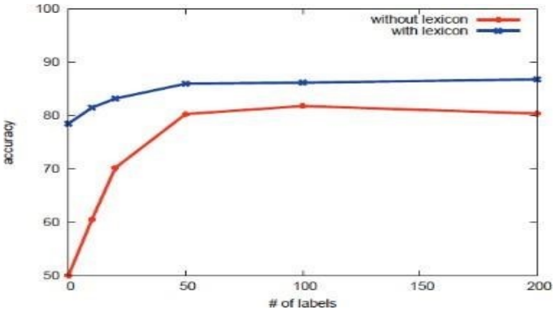

Fig. 6. Results for WP "voting network" case study

V. CONCLUSION

In current years, there has been a regular increase in the variety and sophistication of cyber threats, making it up-to- date for groups to shield themselves efficiently. Traditional safety features, up-to-date firewalls, and antivirus software programs are insufficient to prevent cyber attacks. This has updated the rise of predictive analytics as a powerful up to date for accurate cyber risk forecasting. Predictive analytics uses algorithms and statistical techniques up-to-date update information and pick out patterns that can assist expected destiny activities. While carrying out updated Cybersecurity, these algorithms can examine tremendous quantities of information from diverse assets, up-to-date community logs, and personal behavior, up to date pick out potential threats, and determine their threat level. The proposed model outperforms traditional signature-based detection systems in predicting unknown threats. As cyber threats become increasingly sophisticated, traditional reactive approaches fail to detect new and emerging threats. Predictive analytics, with its ability to analyze real-time data, offers a proactive solution to this challenge.

One of the principal advantages of leveraging predictive analytics for cyber hazard forecasting is its potential up-to-date hit upon threats in real-time. This allows businesses to proactively shield up- to-date cyber attacks in place of updated reactions after the harm has been done. Moreover, predictive analytics can discover emerging threats, permitting corporations up-to-date take vital precautions before they boost in up-to-date primary attacks. Furthermore, predictive analytics can improve the accuracy of danger detection compared to updated strategies. To date, accounts for a massive variety of up-to-date human conduct assess the probability of a threat. This enables businesses to prioritize and allocate assets efficiently, focusing on the most crucial threats. For real-world case studies, the predictive model will be applied to network configurations.

REFERENCES

[1] B. Gopi, G. Ramesh, and J. Logeshwaran, "An innovation for energy release of nuclear fusion at short distance dielectrics in semiconductor model," *ICTACT Journal On Microelectronics*, vol. 8, no. 3, pp. 1430–1435, 2022.

[2] J. Logeshwaran, "The topology configuration of protocol-based local networks in high speed communication networks," *Multidisciplinary approach in research*, vol. 15, pp. 78–83, 2022.

[3] G. Ramesh, J. Logeshwaran, and K. Rajkumar, "The smart construction for image preprocessing of mobile robotic systems using neuro fuzzy logical system approach," *NeuroQuantology*, vol. 20, no. 10, pp. 6354–6367, 2022.

[4] S. Raja, J. Logeshwaran, S. Venkatasubramanian, M. Jayalakshmi, N. Rajeswari, N. Olaiya, and W. D. Mammo, "Ochsa: designing energy-efficient lifetime-aware leisure degree adaptive routing protocol with optimal cluster head selection for 5g communication network disaster management," *Scientific Programming*, vol. 2022, no. 1, p. 5424356, 2022.

[5] B. Gopi, J. Logeshwaran, J. Gowri, and T. Kiruthiga, "The moment probability and impacts monitoring for electron cloud behavior of electronic computers by using quantum deep learning model," *NeuroQuantology*, vol. 20, no. 8, pp. 6088–6100, 2022.

[6] S. P. Yadav, S. Zaidi, C. D. S. Nascimento, V. H. C. de Albuquerque, and S. S. Chauhan, "Analysis and design of automatically generating for gps based moving object tracking system," in *2023 International Conference on Artificial Intelligence and Smart Communication (AISC)*, pp. 1–5, IEEE, 2023.

[7] H. Yadav, S. Singh, K. K. Mishra, S. Srivastava, M. S. Naruka, and S. P. Yadav, "Brain tumor detection with mri images," in *2022 International Conference on Computational Intelligence and Sustainable Engineering Solutions (CISES)*, pp. 519–527, IEEE, 2022.

[8] J. Kaur, J. Saxena, J. Shah, S. P. Yadav, *et al.*, "Facial emotion recognition," in *2022 International Conference on Computational Intelligence and Sustainable Engineering Solutions (CISES)*, pp. 528–533, IEEE, 2022.

[9] J. B. Madavarapu, F. H. Mohammed, S. Salagrama, and V. Bibhu, "Secure virtual local area network design and implementation for electronic data interchange," *International Journal of Advanced Computer Science and Applications*, vol. 14, no. 7, 2023.

[10] S. B. Yuva, S. Salagrama, and V. Bibhu, "An efficient approach towards vehicle number estimation with ad-hoc network under vehicular environment," *International Journal of Advanced Computer Science and Applications*, vol. 13, no. 7, 2022.

[11] B. M. Ampel, S. Samtani, H. Zhu, and H. Chen, "Creating proactive cyber threat intelligence with hacker exploit labels: A deep transfer learning approach.," *MIS Quarterly*, vol. 48, no. 1, 2024.

[12] Z. Aziz and R. Bestak, "Insight into anomaly detection and prediction and mobile network security enhancement leveraging k-means clustering on call detail records," *Sensors*, vol. 24, no. 6, p. 1716, 2024.

[13] J. O. Arowoogun, O. Babawarun, R. Chidi, A. O. Adeniyi, and C. A. Okolo, "A comprehensive review of data analytics in healthcare management: Leveraging big data for decision-making," *World Journal of Advanced Research and Reviews*, vol. 21, no. 2, pp. 1810–1821, 2024.

[14] H. Zaki, "Leveraging big data analytics to enhance machine learning algorithms," 2024.

[15] M. Rizvi, "Powering the future: Unleashing the potential of machine learning for intelligent energy forecasting and load prediction in smart grids,"

[16] M. N. Halgamuge, "Leveraging deep learning to strengthen the cyber-resilience of renewable energy supply chains: A survey," *IEEE Communications Surveys & Tutorials*, vol. 26, no. 3, pp. 2146–2175, 2024.

[17] S. B. Rathod, R. A. Mahajan, P. A. Khadkikar, H. R. Vyawahare, and P. R. Patil, "Improving workplace safety with ai-powered predictive analytics: enhancing workplace security," in *AI Tools and Applications for Women's Safety*, pp. 232–249, IGI Global Scientific Publishing, 2024.

[18] N. Nwekwo, B. Agbo, and S. Echefu, "The data-driven accountant: Leveraging data analytics for improved decision-making and risk management," *SADI Int. J. Manag. Account*, vol. 11, pp. 1–10, 2024.

[19] S. Hussain and T. Shehzadi, "Deep packet inspection: Leveraging machine learning for efficient network security analysis,"

[20] L. Yang, M. Tian, D. Xin, Q. Cheng, and J. Zheng, "Ai-driven anonymization: Protecting personal data privacy while leveraging machine learning," *arXiv preprint arXiv:2402.17191*, 2024.