Measurement: Sensors 27 (2023) 100791

Contents lists available at ScienceDirect

Measurement: Sensors

journal homepage: www.sciencedirect.com/journal/measurement-sensors

IOT-based cyber security identification model through machine learning technique

Bechoo Lal [a,*], S. Ravichandran [b], R. Kavin [c], N. Anil Kumar [d], Dibyahash Bordoloi [e,f], R. Ganesh Kumar [g]

[a] Dept. of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur Dist, A.P, India
[b] Department of Computer Science and Engineering, School of Technology, GITAM University, Rudraram, Hyderabad, Telangana, 502 329, India
[c] Department of Electrical and Electronics Engineering, Sri Krishna College of Engineering and Technology, Coimbatore, 641008, Tamil Nadu, India
[d] Department of Electronics & Communication Engineering, School of Engineering & Technology, Mohan Babu University (Erst while Sree Vidyanikethan Engineering College), Tirupati, Andhra Pradesh, India
[e] Computer Science and Engineering, Graphic Era Hill University, Dehradun, India
[f] R/S, CSE, Graphic Era Deemed To Be University, Dehradun, 248002, Uttarakhand, India
[g] Department of Computer Science and Engineering, CHRIST (Deemed to be University), School of Engineering and Technology, Kengeri Campus, Kumbalgodu, Bangalore, 560074, India

ARTICLE INFO

Keywords:
Cyber security
Machine learning algorithms
Security
Repositories
Meta-classifier methods
Internet of things

ABSTRACT

Manual vulnerability evaluation tools produce erroneous data and lead to difficult analytical thinking. Such security concerns are exacerbated by the variety, imperfection, and redundancies of modern security repositories. These problems were common traits of producers and public vulnerability disclosures, which make it more difficult to identify security flaws through direct analysis through the Internet of Things (IoT). Recent breakthroughs in Machine Learning (ML) methods promise new solutions to each of these infamous diversification and asymmetric information problems throughout the constantly increasing vulnerability reporting databases. Due to their varied methodologies, those procedures themselves display varying levels of performance. The authors provide a method for cognitive cybersecurity that enhances human cognitive capacity in two ways. To create trustworthy data sets, initially reconcile competing vulnerability reports and then pre-process advanced embedded indicators. This proposed methodology's full potential has yet to be fulfilled, both in terms of its execution and its significance for security evaluation in application software. The study shows that the recommended mental security methodology works better when addressing the above inadequacies and the constraints of variation among cybersecurity alert mechanisms. Intriguing trade-offs are presented by the experimental analysis of our program, in particular the ensemble method that detects tendencies of computational security defects on data sources.

1. Introduction

The development of modern technology makes it possible to communicate effectively across every field; specifically, the Cyber-Physical System (CPS) is a cutting-edge system that provides a more efficient environment for data sharing and transmission from one endpoint to another via various proper communication channels [1]. The growth of communication transmission systems was made possible by all this technology, which raises the bar for economic growth. Security and resilience are indeed difficult to achieve, so they must be taken into account when developing security enhancement methods. Security and hardware problems seem to be the two most significant causes of miscommunication [2,3]. The CPS systems are susceptible to harmful action from attackers or hackers, although they have advanced greatly and are therefore pervasive in contemporary communities. As a consequence of the system's abnormal behaviors, its inability to provide protection is a significant matter that is different compared to those of other structures [4]. As a result, the creation of new technologies was required to address those problems in terms of reducing assaults, offering intelligence services, and defending already-existing assistance by

* Corresponding author.
E-mail address: drblalpersonal@gmail.com (B. Lal).
URL: https://www.scopus.com/authid/detail.uri?authorId=58281571800 (S. Ravichandran).

https://doi.org/10.1016/j.measen.2023.100791
Received 27 December 2022; Received in revised form 17 March 2023; Accepted 10 May 2023
Available online 11 May 2023

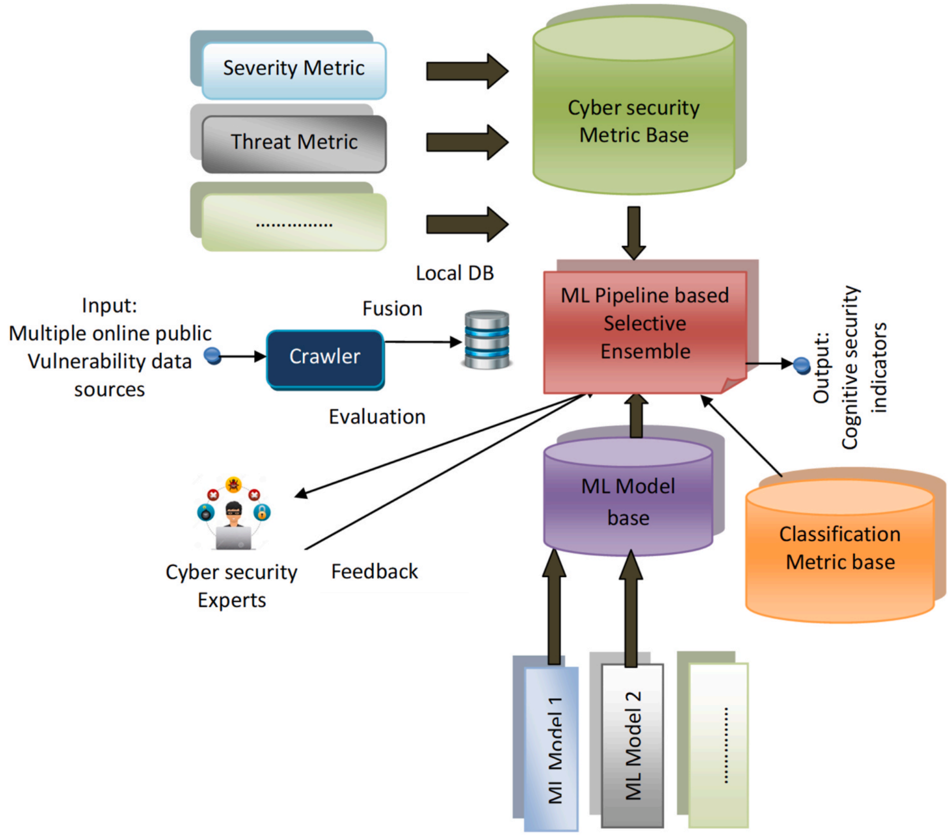
Severity Metric
Threat Metric
....
Cyber security Metric Base
Local DB
Input: Multiple online public Vulnerability data sources
Fusion
Crawler
Evaluation
ML Pipeline based Selective Ensemble
Output: Cognitive security indicators
ML Model base
Classification Metric base
Cyber security Experts
Feedback
Ml Model 1
ML Model 2
....

Fig. 1. The structure of CPS.

regulating anomalous behaviors.

Before adopting a comprehensive approach, the study of the CPS system's elements was required for such complicated tasks as value determination throughout this procedure [5]. With the advancement of technologies, the world today has undergone great change [6]. Meanwhile, the IoT is currently facing significant challenges due to security vulnerabilities brought on by equipment breakdown or malware programs orchestrated and controlled by external adversaries. The IoT was attackable due to the absence of sensor devices, making it a complicated system with communication accessible via public wireless transmission [7]. To maintain the protection but also the stability of the operation of IoT systems, the Intrusion Detection System (IDS) assists with locating the source of irregularities and taking the appropriate action.

The CPS' stability was unstable, leading to a rapid service failure through the components or nodes. Consequently, the defect-diagnosing system's project will focus heavily on retaining existing features and capabilities. The system's heterogeneity or extensive operation seems to be to blame for such service failures [8]. To solve these concerns, an efficient failure system is required. Owing to the system's complexity or dynamic nature, the common approach could not be capable of meeting the need for high security [9]. The new method, which combines a detector and an alert capability, is anticipated to offer greater security than just the conventional method. As a result, the current system makes use of IoT and machine learning approaches to diagnose faults at a preliminary phase [10]. Maximum benefits than those achieved through human skill can also be delivered by the machine learning approach. The Artificial Neural Network (ANN) methodology with IoT has been one of the machine learning techniques used for identifying system flaws.

The contributions of the work are:

- To break through the ML methods with novel recommended mental security methodology that provides new solutions to each of diversification and asymmetric information problems.
- To provide a method for cognitive cyber security that enhances the human cognitive capacity.
- To create trustworthy data sets and initially reconcile competing vulnerability reports and then pre-process advanced embedded indicators.

In this paper, a brief notes on the IoT enabled cyber security through machine learning algorithm was discussed in the introduction and literature survey clearly focus on the research interest. Then the Ml based CPS structure with data acquisition and integration was discussed, followed with the implementation and discussion, finally the work output was concluded in the last section.

2. Related works

A simulation environment built over an MCU, an ESP8266 router, a DHT11 sensor, and a router or wifi connection, has been created to simulate the Internet of Things environment [11]. A mobile organization that carried out investigative assaults by contaminating other organizations created the hostile organization. The speak-reflecting system and wifi bridge were employed to analyze the information given through detectors that measured the warmth, moisture, and delivery location [12]. Somewhere during the standard stage, the MCU node's sensor readings were collected and relayed to the Think Speak server, where they are stored and designated as predicted values. The assailant can change system information transmitted by the MCU server node and think and speak just at the moment of the assault and acquire detailed information from an opponent.

The assumption that ML methodologies could really promote comprehensive monitoring of security vulnerabilities and data sources

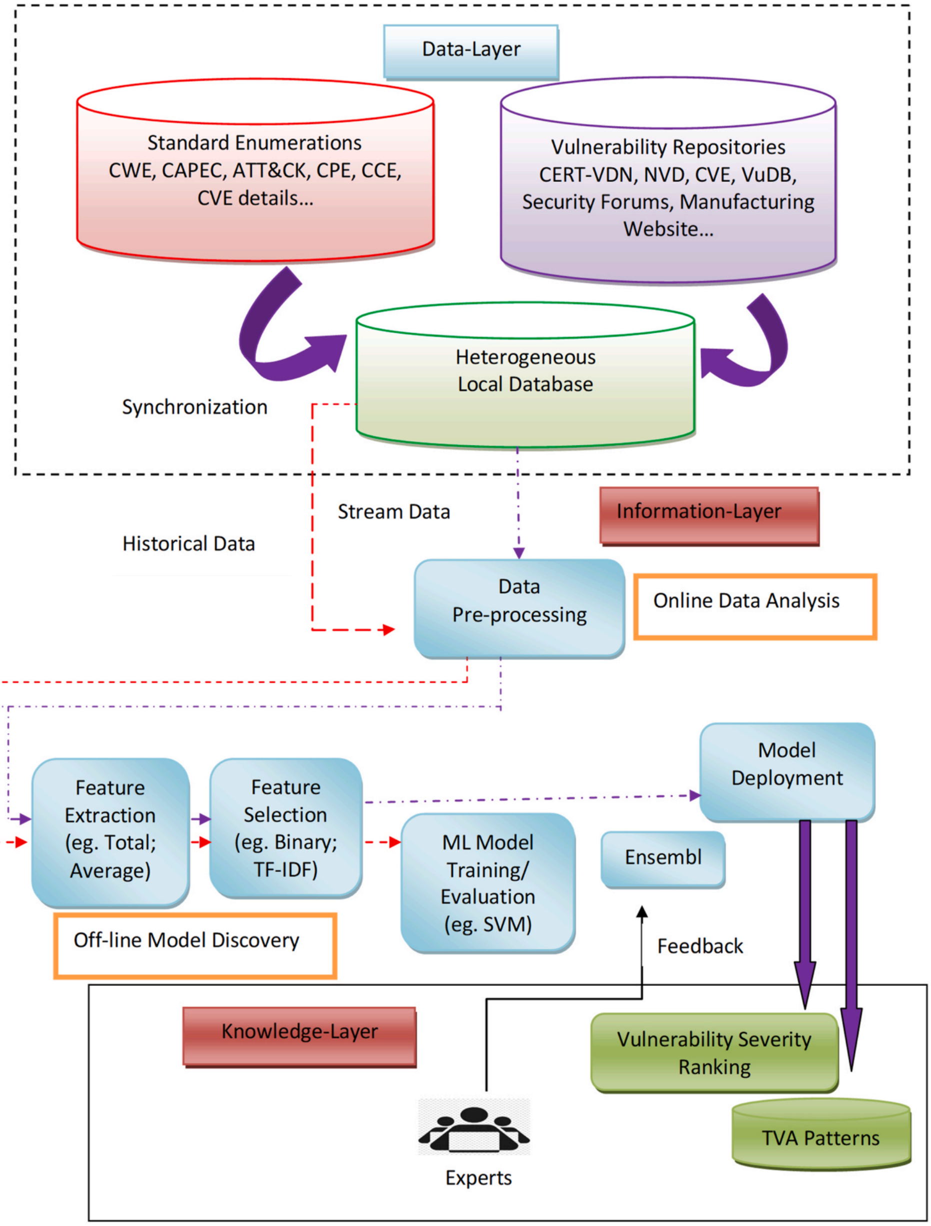

Fig. 2. CPS knowledge generation using ML.

and thereby ease a number of the above-mentioned cybersecurity challenges arising from the changing field of cyber attacks is becoming more widely accepted among many cybersecurity professionals [13]. A change in the management of massive amounts of vulnerable personal information by security specialists and toward certain digital alternatives is anticipated as a result of advancements in machine learning-induced security solutions. Recent studies demonstrate modest gains in productivity and efficiency when ML approaches are used to perform security tasks such as cybersecurity warning management and associated event investigation. To speed up different cybersecurity tasks like threat categorization and associated severity evaluation, ML approaches are still underdeveloped. For instance, various ML approaches may be needed in multi-label and multi-class classification, while alternative validation measures could be used [14].

The choice of an appropriate option seems overwhelming because of the potential cybersecurity dangers that might also emerge from employing the incorrect ML model since there are no one-size-fits-all ML-based options for automating security activities. This work [15] addresses the conundrum of selecting the best machine learning model that proactively mitigates the more sophisticated threats. The objective seems to be to equip cybersecurity experts with current, varied, and accurate information about national security and the public to improve their tactical awareness [16]. Therefore, to ensure smooth cybersecurity research and keep intelligence officials informed of the methodology, our proposed cybersecurity architecture blends study strikes from computational linguistics, machine learning, and data gathering. To achieve this paradigm was adopt IBM's inspiring concept of intellectual cybersecurity to address the cognitive aspect of cybersecurity [17].

By including a human operator in the cybersecurity assessment circuit, our strategy effectively links ML advancements to natural neuroscience to improve the effectiveness of automation techniques with professional knowledge [18]. For instance, to ensure that such ML models are targeted to issues in particular cybersecurity areas, cybersecurity specialists are consulted during the image segmentation and positive affirmation selection processes. Our strategy provides ML tools to cybersecurity operators. This methodology continuously monitors and maximizes the use of internet cybersecurity data repositories.

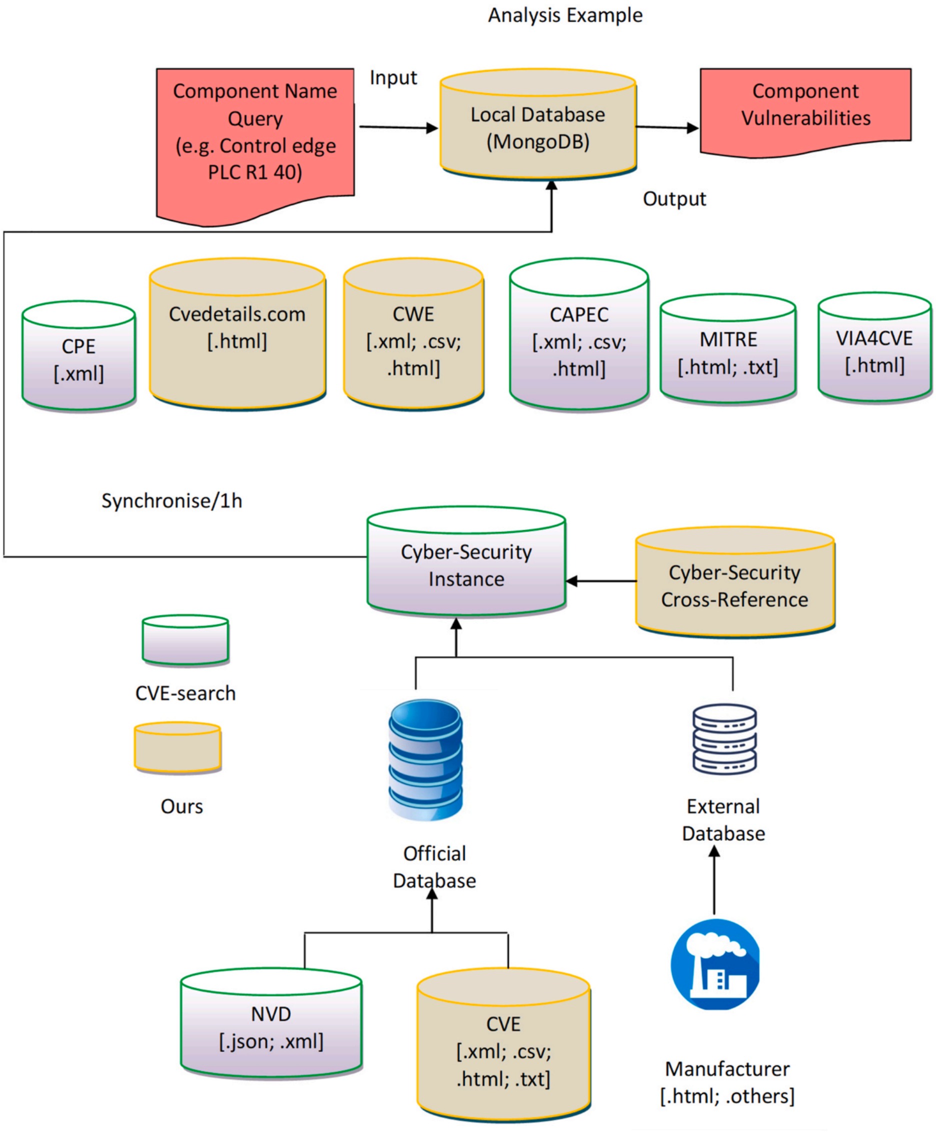

Fig. 3. Implementation of cross-linked database.

3. Proposed ML-based framework

When cybersecurity-related issue measurement sets are supplied, such as vulnerability severity measurements, etc., a pipeline of selected ML ensemble methods creates organizational factors based on those metrics. To link new instances of vulnerability into recognizable patterns, our classifiers are trained on past data. This method resolves the aforementioned diversity concerns and deduces the security information that is lacking. The technique additionally uses an ML group layered structure of learned categories to enhance the detection of security indications. Instead of using ML models, our composites method integrates several techniques into a specific theory that includes susceptibility patterns and structural relationships [19].

Protection controllers took part in the authentication process to select and rank classification-performance indicators including accuracy and precision. Investigators consider the overall system and make the flow of work of our strategic plan for perception cybersecurity, which can be seen in Fig. 1, even though end-to-end improvement throughout the whole pipeline is challenging. The split of the applications into segments provides a possibility for optimization by highlighting the parts created to improve for different tasks.

Our proposed perceptual CPS evaluation method is being evaluated against a sizable collection that includes over 130 000 samples drawn from 8 real online CPS repositories and other related vendor websites.

As shown in Fig. 2, our method entails three steps that link unorganized information gathering to reliable information to produce a perceptual, qualitative approach and knowledge at the expertise layer level. In the beginning, the stage collected diverse information from cybersecurity data sources. As a component of the procedure, combine important roles related to the regulation into a single local database and assign labels to those based on commonly used cybersecurity-related classifications.

3.1. Data acquisition and integration

There seem to be mainly 2 ways to collect security-related information: directly, utilizing tools like a vulnerability scanner, and indirectly, through already-existing public online databases. In comparison, indirect information gathering seems to be more effective when saving money on maintenance but also acquiring time for the full project or even a sizable volume of information. Other oblique offline approaches to security information exist. Moreover, these activities frequently need the consent of stakeholders or might raise ethical concerns. So, in this research, authors make use of open-access web datasets. These data

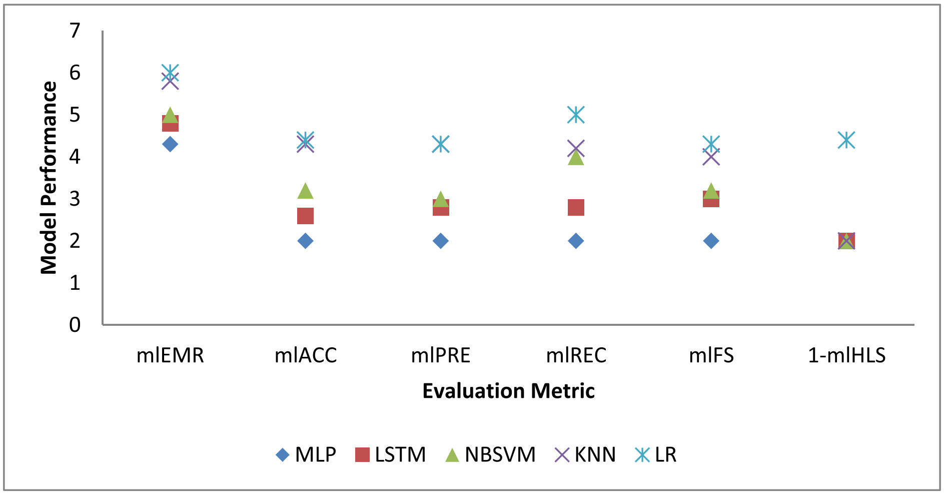

Fig. 4. ML-based performance analysis for threat classification.

components are segregated, saved, and disseminated in various data formats, though. They also adhere to many specifications, each of which features unique semantics and syntax. Directly from the CVE/NVD repositories were used to acquire information sources. Then, using crawlers, accessed vulnerability reports from various cybersecurity information sites, such as SecurityFocus. Furthermore, utilizing accessible LDA-based topic-modeling techniques, efforts have been exerted by classifiers by identifying terms only with max frequency in CVE reports. The evaluation of the potential features by preparing the original input space and ranking those characteristics based on measures like processing time, as opposed to assessing all of the accessible candidate characteristics retrieved from the prior stage.

Recently, researchers proposed using some NLP techniques to transform the contents of cybersecurity alerts into numerical representations. Hence, chosen to train ML algorithms using the collected characteristics synchronously. To identify pertinent TVA characteristics and produce accurate forecasts of vulnerability rating severity, it's indeed essential to classify new incoming observations using machine learning algorithms to categorize them based on prior experiences. As was previously indicated, the primary difficulty is the right ML selection conundrum. A series of ML algorithms, evaluate but also verify those ML models, and then choose the best designs to serve as individual parts for the remainder of the ensemble construction to tackle this problem. To do this, used a straightforward model of distributed processing concurrency to strike a compromise between statistics and overall technological effectiveness.

3.2. *Model selection and ensemble*

To combine the projections of every baseline component and arrive at a final prediction of something like the hazard associated with a specifically stated vulnerability, the baseline quality model is chosen, then goes into further depth about the proposed Ensemble creation method.

Given dataset D, N ML models MLi $(0 < i \leq N)$, and a set of M related evaluation metrics mj $(0 < j \leq M)$, the following algorithmic steps construct the base ensemble of classifiers. For N individual models and conducted N rounds of training tasks.

Step 1 Train every individual ML model (1) i $(0 < i \leq N)$ with the dataset D.
Step 2: Compute rating scores S (1) i $(0 < i \leq N)$ for each model (1) i.
Step 3: Determine the best-rated ML model with the highest score
Step 4: Repeat Step 1 to Step 3 for the remaining $(N - 1)$ rounds which results in N best-performing ensemble models from each round
Step 5: Repeat Step 2 to Step 3 to determine scores S (i) $(0 < i \leq N)$ for each model (i), and determine the best-performing model with the highest score

4. Experimental analysis

There are two important sections to the experiments. Setting up a database that connects many internet vulnerability repositories is the initial step. The generated dataset includes collections of vulnerability reports divided into various exploitation concern kinds and Common Vulnerability Scoring System (CVSS) classifications like access-vector types, access-complexity levels, etc. [20]. The objective is to concentrate resources and attention on particular immediate hazards that are caused by danger and have varying degrees of effect intensity. Every class type relates to a unified brand, or cluster, within the entire entity. Building the pipeline of particular ML methods and applying them to various groups of information categories constitutes the second phase. The traditional methods for calculating quantifiable resemblance require feature collection and analysis. All of those are basic text characteristics that the CHARM algorithm could interpret as words or associated compound morphologies.

To feed our proposed ML pipeline, a vulnerability repository that is kept organically synced to numerous internet vulnerability-reporting sources is shown in Fig. 3. The CVE information includes instances of vulnerabilities that were reported but have not yet been made available in NVD.

Regarding consistent product nomenclature, vulnerability rating, and patching updates, compared manufacturing websites. To achieve this, identified connections linked to the corresponding CVE entries, compiled information on vulnerabilities from cross-linked websites, and saved the collected data in files searchable with CVE IDs. The hourly feed of open data repositories is synchronized with the local MongoDB machine when it starts up. While scanning internet vulnerability repositories and combining obtained data into a single localized database, hourly durations are taken into account for the vulnerability disclosure timetable.

4.1. *Experiment methodology*

To simplify the ML approach, created a pipeline utilizing the Scikit-Learn library's pre-existing packages pipeline. Depending on the categorization goals and data subsets, used various ML stacking methodologies. During our comparing results, take into account 5 recognized machine learning models: KNN, NBSVM, LSTM-ANN, MLP, and LR. Now quickly review these potential ML models. Although each of these five models is usually employed separately in text-mining and cybersecurity

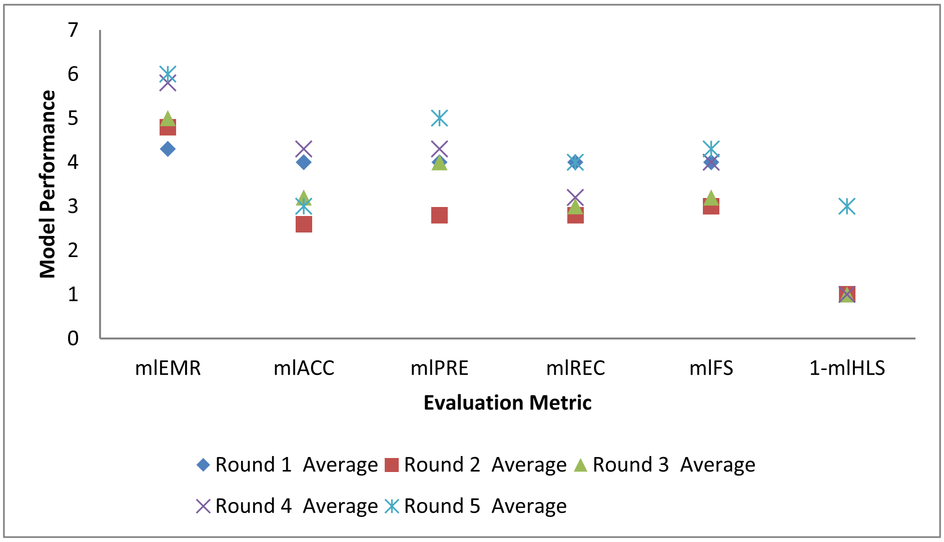

Fig. 5. ML-based training performance analysis for threat classification.

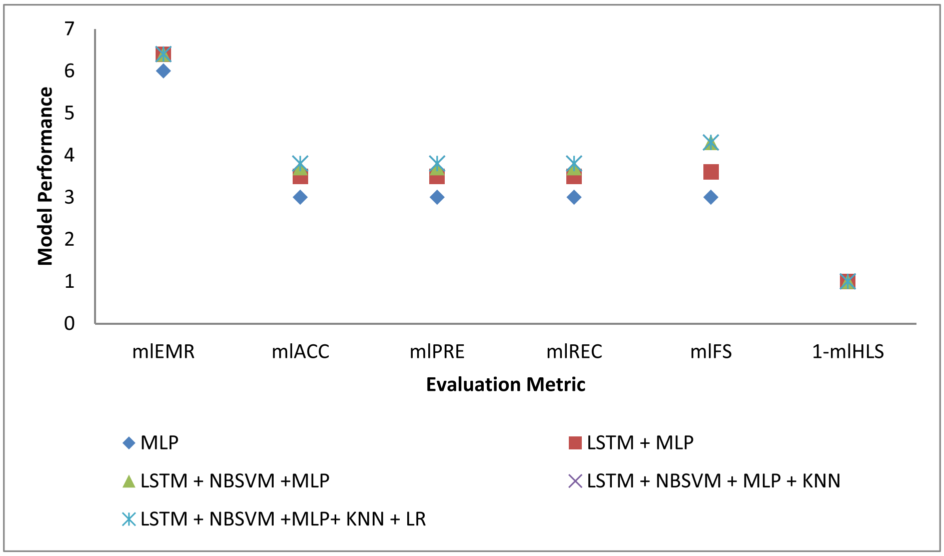

Fig. 6. Training model for threat classification.

settings, our ensemble paradigm expands its maximum potential when used in conjunction with some other ML techniques in a variety of CPS research.

A multi-label classification technique is threat categorization modeling. By breaking the multi-label issue down into numerous individual binary classification problems were able to resolve it using the one-to-rest method. This work separated the 93 311 records that researchers had obtained at random into two datasets, one for learning and the other for verification. Next, separately educated each of the 5 ML algorithms to acquire threat categorization. On test datasets that had not yet been viewed, assessed the training algorithms' abilities and selected the system that performed the best [21].

4.2. Experiment results

Here, generated an aggregate of 31 evaluation files throughout 5 cycles to assess the effectiveness of our pipeline method and select foundation Ensemble models. As further shown in Fig. 4, the user models KNN and LR perform comparably worse than LSTM, NBSVM, and MLP. Whenever these inferior base learners were included in the ensemble, the achievement of the ensemble in its entirety remained comparatively steady. This is an advantage of soft voting, which goes beyond simple binary options and takes into account every beginner's level of trust. Finally, figure out how each of the methods performs in general. As further shown in Fig. 5, all five metrics—aside from mlHLS—perform best as the number of active base learners rises.

As shown in Fig. 6, also contrasted the top-performing designs from every round. Our pipelined ensemble model is the most effective across all setups. Individual product MLP had the greatest performance in the opening round. The performances of the LSTM and MLP ensembles improved in the second round. The 3rd round's best moments come from MLP, SVM, and LSTM ensembles. The performance of the MLP, SVM, LSTM, and KNN ensembles is greatest in the fourth round. Finally, there are no comparison equivalents in the fifth round as there is only one ensemble model. The greatest result is given by the LSTM and MLP combined. However, the efficiency of the LSTM, NBSVM, and MLP ensembles is extremely close.

The ensemble model comprising base learning LSTM and MLP is where the majority of prediction performances, such as mlACC, mlPRE, and mlFS, achieve their top values. It's interesting to note that mlHLS performs best amongst specific models, implying that losses caused by ensemble models while forecasting could be greater in the bit string of

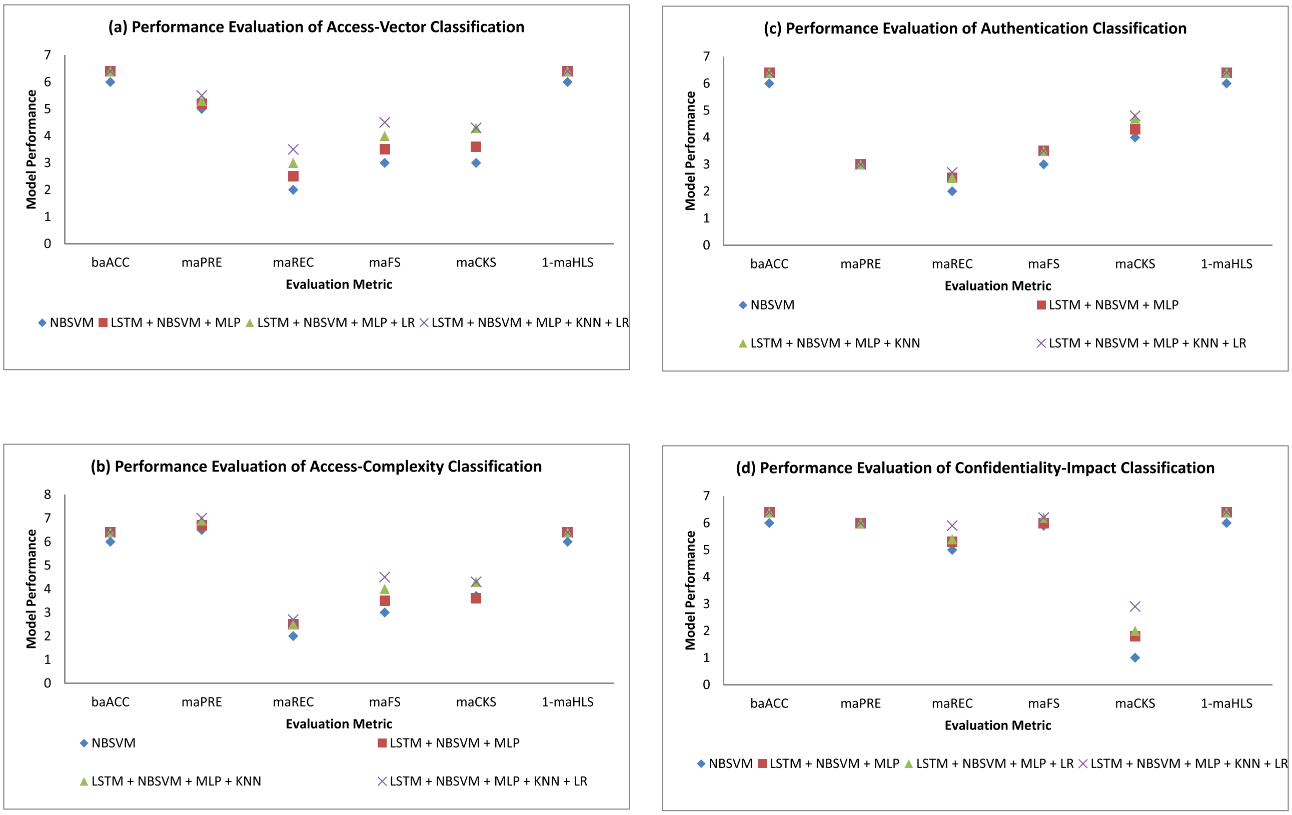

Fig. 7. Training model for threat classification based on CVSS characteristics.

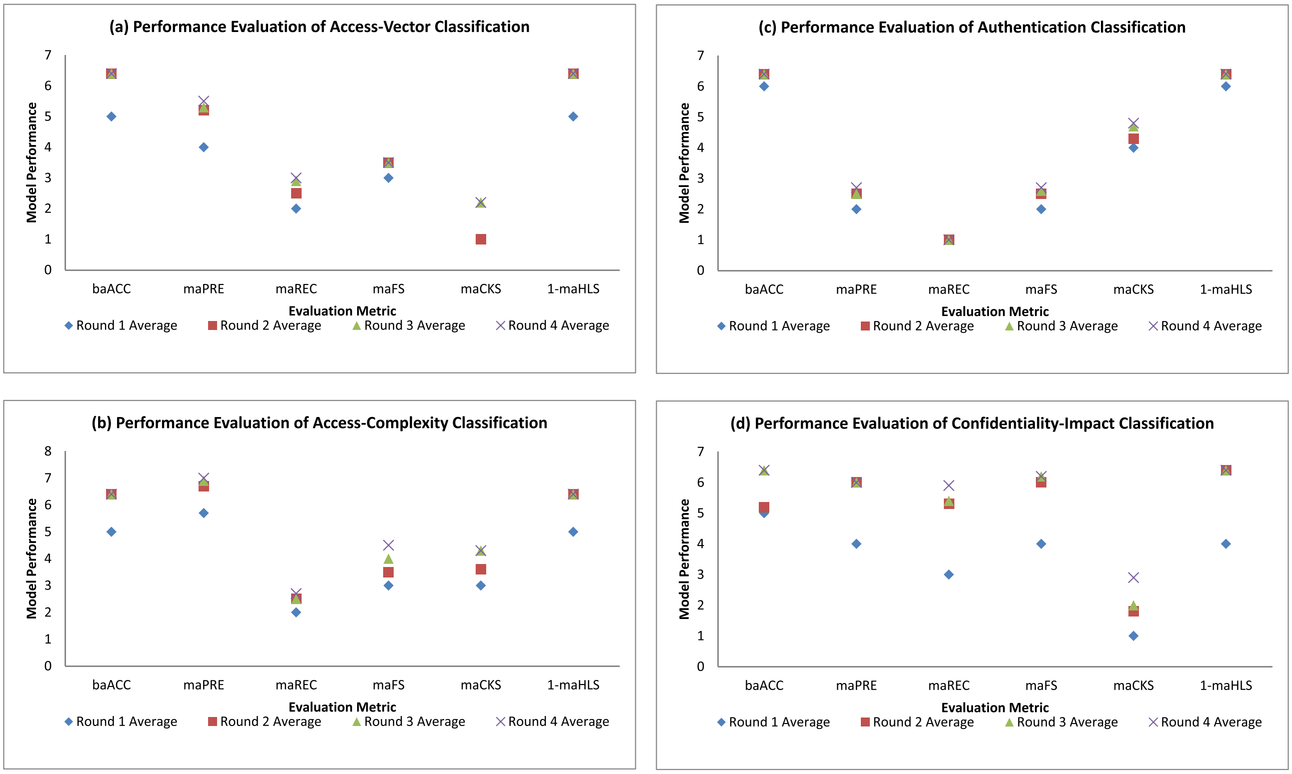

Fig. 8. Training model for threat classification of average performance based on CVSS characteristics.

Table 1
Evaluation of CVSS V2 score prediction on untrained dataset.

Model	CVSS-ACC (δ = 0.05)	CVSS-ACC (δ = 0.05)
NBSVM	64.59	92.95
LSTM + NBSVM + MLP	64.76	93.06
LSTM + NBSVM + MLP + LR	64.02	92.82
LSTM + NBSVM + MLP + KNN + LR	64.08	92.91

class labels. To our understanding, there are no results from research on risk classification that are comparable. Therefore the ensemble of LSTM and MLP achieved a mlEMR score of 91.63%, demonstrating the predictive strength of our system.

4.3. *Classification and score prediction*

In CVSS-characteristic categorization and score projection, used hard voting, also known as the "popular vote," as opposed to the soft voting technique used for risk categorization. If there are three or more base voters, the popular vote is effective. As a result, merely produced 21 achievement records in 4 matches for every categorization or score projection of a CVSS feature. The main findings, or the supermodels, from every learning session, are seen in Fig. 7 (a) – (d). Fig. 8(a)– (d) provides more information on the typical results of the classification model for every round.

As more base learners are participating, the majority of the measures perform much better. It is unknown in advance whether the round will produce the best ensemble model, experimental results of the analysis for hazard and CVSS characteristics classifications underscore the importance of employing the multi-round ensemble paradigm. The actual research demonstrates that to improve the performances of these classifiers in the setting of cybersecurity analysis, our ensemble model selects the most suitable algorithms from a set of five conventional classifiers.

Using the CVSS score accuracy metric, the ensemble of LSTM, NBSVM, and MLP has the best performance, as shown in Table 1.

5. Conclusion

In this work, equip security controllers working at different levels with a customized but synchronized database that pulls data from a variety of internet cybersecurity information sources. Before using the found vulnerability cases as training ground truth, it becomes possible to resolve competing vulnerability-severity ratings and various terminology employed by various parties. The CVSS score accuracy metric, the ensemble of LSTM, NBSVM, LR, and MLP has the best performance in the level of 64.59, 64.76, 64.02, and 64.08 for the condition CVSS-ACC (δ = 0.05). whereas for the condition CVSS-ACC (δ = 0.05), LSTM, NBSVM, LR, and MLP are at the level of 92.95, 93.06, 92.82, and 92.91, respectively. Five widely used text-mining methods are utilized in actual research to assess the proposed IoT ensemble paradigm. This comparison study demonstrates the positive prospects of our ensemble methods in the risk categorization and intensity rating cybersecurity scenario. This activity offers ways to modify investment choices at various managerial levels.

CRediT authorship contribution statement

Bechoo Lal: Supervision, Writing – review & editing. **S. Ravichandran:** Writing – original draft. **R. Kavin:** Data curation. **N. Anil Kumar:** Conceptualization. **Dibyahash Bordoloi:** Methodology. **R. Ganesh Kumar:** Data Validation.

Declaration of competing interest

The authors declare that they have no known competing for financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

No data was used for the research described in the article.

References

[1] P. Suresh, K. Logeswaran, P. Keerthika, R.M. Devi, K. Sentamilselvan, G. K. Kamalam, H. Muthukrishnan, Contemporary survey on the effectiveness of machine and deep learning techniques for cyber security, in: Machine Learning for Biometrics, Academic Press, 2022, pp. 177–200.

[2] A. Sharma, S. Sharma, S. Gulati, T. Choudhury, CAPTCHA robustness-AI approach using to web security, Ingénierie Des. Systèmes Inf. 27 (2) (2022).

[3] M. Monica, P. Sivakumar, S.J. Isac, K. Ranjitha, PMSG based WECS: control techniques, MPPT methods and control strategies for standalone battery integrated system, in: AIP Conference Proceedings, vol. 2405, AIP Publishing LLC, 2022, April, 040013. No. 1.

[4] D. Saha, G.N.R. Devi, S. Ponnusamy, J. Pandit, S. Jaiswal, P.K. Bhuyan, Application of nanotechnology in neural growth support system, in: 2022 IEEE 2nd Mysore Sub Section International Conference (MysuruCon), IEEE, 2022, October, pp. 1–6.

[5] B. Raviprasad, C.R. Mohan, G.N.R. Devi, R. Pugalenthi, L.C. Manikandan, S. Ponnusamy, Accuracy determination using deep learning technique in cloud-based IoT sensor environment, Measurement: Sensors 24 (2022), 100459.

[6] S. Shukla, A. Sharma, Cyber security using machine learning in digital education industry, in: 2021 International Conference on *Innovative Computing, Intelligent Communication And Smart Electrical Systems (ICSES)*, IEEE, 2021, September, pp. 1–6.

[7] A. Fatani, A. Dahou, M.A. Al-Qaness, S. Lu, M.A. Elaziz, Advanced feature extraction and selection approach using deep learning and Aquila optimizer for IoT intrusion detection system, Sensors 22 (1) (2021) 140.

[8] J. Thom, N. Thom, S. Sengupta, E. Hand, Smart recon: Network traffic fingerprinting for IoT device identification, in: 2022 IEEE 12th Annual Computing *and Communication Workshop And Conference (CCWC)*, IEEE, 2022, January, pp. 72–79.

[9] T.P. Latchoumi, R. Swathi, P. Vidyasri, K. Balamurugan, Develop new algorithm to improve safety on WMSN in health disease monitoring, in: 2022 International Mobile and *Embedded Technology Conference (MECON)*, IEEE, 2022, March, pp. 357–362.

[10] Y. Alghofaili, M.A. Rassam, A trust management model for IoT devices and services based on the multi-criteria decision-making approach and deep long short-term memory technique, Sensors 22 (2) (2022) 634.

[11] Z. Halim, M.N. Yousaf, M. Waqas, M. Sulaiman, G. Abbas, M. Hussain, M. Hanif, An effective genetic algorithm-based feature selection method for intrusion detection systems, Comput. Secur. 110 (2021), 102448.

[12] M.A. Ferrag, O. Friha, L. Maglaras, H. Janicke, L. Shu, Federated deep learning for cyber security in the internet of things: concepts, applications, and experimental analysis, IEEE Access 9 (2021) 138509–138542.

[13] D.J. Atul, R. Kamalraj, G. Ramesh, K.S. Sankaran, S. Sharma, S. Khasim, A machine learning based IoT for providing an intrusion detection system for security, Microprocess. Microsyst. 82 (2021), 103741.

[14] S.S. Gopalan, A. Raza, W. Almobaideen, Iot security in healthcare using AI: a survey, in: 2020 International Conference *on Communications, Signal Processing, and Their Applications (ICCSPA)*, IEEE, 2021, March, pp. 1–6.

[15] V. Gaur, R. Kumar, Analysis of machine learning classifiers for early detection of DDoS attacks on IoT devices, Arabian J. Sci. Eng. 47 (2) (2022) 1353–1374.

[16] K. Balamurugan, T.P. Latchoumi, T.P. Ezhilarasi, Wearables to improve efficiency, productivity, and safety of operations, in: Smart Manufacturing Technologies For Industry, 4.0, CRC Press, 2022, pp. 75–90.

[17] M.S. Rathore, M. Poongodi, P. Saurabh, U.K. Lilhore, S. Bourouis, W. Alhakami, M. Hamdi, A novel trust-based security and privacy model for internet of vehicles using encryption and steganography, Comput. Electr. Eng. 102 (2022), 108205.

[18] M.S. Rathore, M. Poongodi, P. Saurabh, U.K. Lilhore, S. Bourouis, W. Alhakami, M. Hamdi, A novel trust-based security and privacy model for internet of vehicles using encryption and steganography, Comput. Electr. Eng. 102 (2022), 108205.

[19] P. Garikapati, K. Balamurugan, T.P. Latchoumi, K-means partitioning approach to predict the error observations in small datasets, Int. J. Comput. Aided Eng. Technol. 17 (4) (2022) 412–430.

[20] R. Geetha, T. Thilagam, A review on the effectiveness of machine learning and deep learning algorithms for cyber security, Arch. Comput. Methods Eng. 28 (4) (2021) 2861–2879.

[21] N. Unnisa A, M. Yerva, K. Mz, Review on intrusion detection system (IDS) for Network security using machine learning algorithms, International Research Journal on Advanced Science Hub 4 (3) (2022) 67–74.