Journal of Cloud Computing:
Advances, Systems and Applications

RESEARCH Open Access

Next-generation cyber attack prediction for IoT systems: leveraging multi-class SVM and optimized CHAID decision tree

Surjeet Dalal[1], Umesh Kumar Lilhore[2*], Neetu Faujdar[3], Sarita Simaiya[2], Manel Ayadi[4], Nouf A. Almujally[4] and Amel Ksibi[4]

Abstract

Billions of gadgets are already online, making the IoT an essential aspect of daily life. However, the interconnected nature of IoT devices also leaves them open to cyber threats. The quantity and sophistication of cyber assaults aimed against Internet of Things (IoT) systems have skyrocketed in recent years. This paper proposes a next-generation cyber attack prediction framework for IoT systems. The framework uses the multi-class support vector machine (SVM) and the improved CHAID decision tree machine learning methods. IoT traffic is classified using a multi-class support vector machine to identify various types of attacks. The SVM model is then optimized with the help of the CHAID decision tree, which prioritizes the attributes most relevant to the categorization of attacks. The proposed framework was evaluated on a real-world dataset of IoT traffic. The findings demonstrate the framework's ability to categorize attacks accurately. The framework may determine which attributes are most crucial for attack categorization to enhance the SVM model's precision. The proposed technique focuses on network traffic characteristics that can be signs of cybersecurity threats on IoT networks and affected Network nodes. Selected feature vectors were also created utilizing the elements acquired on every IoT console. The evaluation results on the Multistep Cyber-Attack Dataset (MSCAD) show that the proposed CHAID decision tree can significantly predict the multi-stage cyber attack with 99.72% accuracy. Such accurate prediction is essential in managing cyber attacks in real-time communication. Because of its efficiency and scalability, the model may be used to forecast cyber attacks in real time, even in massive IoT installations. Because of its computing efficiency, it can make accurate predictions rapidly, allowing for prompt detection and action. By locating possible entry points for attacks and mitigating them, the framework helps strengthen the safety of IoT systems.

Keywords Anomaly detection, CHAID decision tree, IoT cyber attacks, Multistep attack, Security investigation, Zero-day attack

*Correspondence:
Umesh Kumar Lilhore
umeshlilhore@gmail.com
Full list of author information is available at the end of the article

Introduction

The term "Internet of Things" refers to a broad category of technology solutions and meaningful objects that interact with one another online, in addition to the big data that all objects produce. Automation, intellectual equipment in home automation, and essential infrastructure are all examples of IoT device equipment with various uses and complexity. IoT devices were created to improve safety and convenience among many facets of a person's life. In addition to greater comfort, the IoT introduces new cybersecurity-related issues and difficulties. The characteristics of a setting affect the security problems underlying the IoT infrastructure. An IoT framework is a potential IoT ecosystem component consisting of collections of advanced technologies with the same or equivalent technical specifications. If a specific device is vulnerable, such homogeneity magnifies the consequence.

A multi-stage cyber-attack is precisely what its name suggests: A cyber-attack that takes place in steps instead of an instantaneous attack. When a resource's integrity, confidentiality, or availability is compromised by an incursion [1], it is considered an intrusion. Intrusion detection systems are the first line of defence in crucial IoT networks. Anomalies in network traffic or signatures help them identify known threats. Security alarms are growing at an exponential rate as network traffic increases. However, sophisticated attacks elude IoT security systems by carrying out each attack step individually and dividing the attack into many consequential segments. As a result, modern cyberattacks are becoming more accurate, distributed and large-scale. Undetected cyberattacks can have devastating consequences. To secure vital resources now or in the future, a description and projection of the attack and documentation of the attacker's behaviour are helpful.

Similarly, a multi-stage cyber attack on an organization may include using a rogue employee who first recons for weaknesses in the network defences and might use his position within the organization to drop a malware payload that is activated at a reasonable time. The utilization of risky web servers, like telnet servers and File Transfer Protocols (FTP) servers, along with security flaws in devices and access control lists, are critical problems. Security flaws with policies and procedures employed by the communications infrastructure are also an issue. Even highly specialized vulnerable IoT equipment with resource constraints can be leveraged to track and collect information on the IoT to utilize crucially. As a result, the entire IoT infrastructure may be severely harmed by flaws in the protocols used by the IoT application. Depending on the ecosystems the vulnerable connected systems perform in, such effects' amid the challenges vary.

A supervised learning framework with a better classification performance than numerous different classification algorithms, but its application is restricted due to the extended training times required for massive data sets. Various feature selection methods are combined with SVM to acquire reduced dimensional statistics. A classification model needs minimal training time as just an outcome. An ideal set of characteristics is chosen using feature selection before constructing a model. A particular feature selection algorithm is used in the feature selection phase to assess the ranking of each possible characteristic, and the finest "k" characteristics are then determined. This process involves creating a ranked list of features from which a subset of factors can be chosen using various specific requirements. One of the most prevalent statistical methods is the CHAID, which forecasts imbalance from the predicted allocation if the feature occurrence is not highly dependent upon that categorical variable.

The performance of Smart IoT devices can be altered mainly by device manufacturing companies even without the customer's consent by changing the device's custom firmware, a significant IoT cyber threat hazard. It adds new security vulnerabilities that could enable the IoT device to accomplish unpleasant activities on the client device, like secretly capturing confidential user information and even inadequately altering capabilities.

This work proposes an IoT cybersecurity threat detection model that utilizes a multi-class SVM algorithm and CHAID feature screening for high precision, lower false positives, and optimistic factors. The proposed model optimizes a kernel parameter by calculating the variance for each attribute feature and determining the highest attribute variance. A high conflict will lead to a better kernel parameter if the kernel and variance are inversely related. This method is known as the variance optimization technique. The critical contribution of this research mainly includes:

a) The primary goals of the research were to investigate the potential for multi-stage cyber threat detection in IoT devices using load flow and a more in-depth network monitoring that considers IoT security protocol characteristics.
b) This research developed a model for early and automatic recognition of cyber security threats for IoT infrastructure based on the CHAID method, which creates locate and new secure paths.
c) This research attempts to improve cyber attack detection effectiveness through an SVM ML algorithm.
d) The proposed technique focuses on network activity characteristics that can be signs of cybercrime in the network ecosystem and vulnerable Smart systems.

The complete article is organized as follows: Related work section covers the related work in the field of IoT cyber security attack detection, Materials and methods section covers the materials and methods, Results and discussion section covers the results and analysis, including experimental details and performance metrics, and Conclusion section covers the conclusion and future scope of the IoT cyber security research.

Related work

Fundamentally, circumstances would gain from a method and language for exhibiting IoT cyber security threads [2] in the direction of robotized location and recognizability of proof of multistep digital assault. IoT architecture is an example of attack designs familiar with reusing nonexclusive modules in the assault. A prototype implementation of a scenario acknowledgement motor using Categorical Abstract Machine Language (CAML) was developed, which gradually consumed first-level security warnings and generated reports that differentiate multistep attack situations in the alarm stream.

Protecting IoT devices from top to bottom is described in [3], contributing to a greater capacity for mission-driven digital situational awareness. Therefore, the IoT cauldron plotted out all potential network vulnerabilities by linking, summarizing, standardizing, and interweaving data from diverse sources. It allowed for a more nuanced understanding of potential attack vectors, leading to mitigation suggestions. A flexible demonstration supported a multi-stage analysis of firewall rules and host-to-have vulnerabilities, including attack routes within the organization from the outside. They portrayed a prepared relationship because of Caldron assault charts and analyzed the impact of attacks on missions.

In [4], the authors examine a cyber security threat detection model for IoT devices based on a Hidden Markov Model (HMM). IoT devices relied on information mining to deal with warnings and generate input for the HMM. Given our acquired knowledge, their architecture could continuously stream Snort warnings and anticipate disruptions. With enough data, our approach might infer patterns in the multi-stage attack and rank aggressors accordingly. This allows our system to accurately predict attackers' behaviour and assess the relative danger of different groups of attackers.

In [5], the authors present a multistep signature language model for IoT device communication that can aid in attacking predetermined sites based on standardized log events collected from various applications and devices. In addition, the wordy language helps us integrate our understanding of external threats and reference up-to-date warning signs. Using this technology, they'd be able to manufacture generic sleep-boosting markings. Using this vocabulary, they could tell between various login animal power initiatives across multiple apps using a single, generic pattern. The researchers presented a review of previous research and a rigorous examination of several machine learning methods [6]. The paper also includes statistical data to compare the method recognition effectiveness of suspicious activities in IoT network systems. According to research observations, the random forest method generates the most detailed findings for the feature sets.

A cyber security model with an Intrusion Detection System (IDS) is discussed in IoT architecture, which utilizes alarms relating to unusual traffic to connect IoT devices. Because there are many possible permutations of attack time, risk assessment, and attack hub data in the IoT, this study presented a method to mimic multistep assault circumstances within the company. The results of the trials proved that the suggested technique could accurately reproduce multistep assault situations and trace them back to the original host. It might help senior leaders better express safety actions to employees, helping to make the workplace safer for everyone. The IoT network's attack recognition strategy is discussed in [7]. Its foundation is the application of advanced systems. A sequence of network architectures is used to create IoT solutions. The method uses the information gain, random forest classifier, correlation analysis, and feature global ranking to decrease the number of features. The additional investigation is based on three feature sets coupled using the suggested method to generate an optimized part and functionality.

Research [8] presents a method for IoT threat detection that relies on cloud technology software-defined networks (SDN). It uses a decentralized multiple SDN to prevent attacks within low-power wireless IoT equipment. The predetermined neighbourhood DNS server of the designated sector was used to carry out network activity dominion for each network interface field. The central component of the strategy is a unique regulator installed in a cloud infrastructure and linked to a base station.

According to research [9], Evaluation of cyber attack detection using a holistic strategy proposed to address the challenge of pinpointing novel, nuanced threats and the best ways to neutralize them. Particularly illustrative of this issue are zero-day attacks and multistep assaults, which consist of several steps, some malevolent and others not. To identify the multi-stage assault scenario, they present a substantially Boosted Neural Network in this study. The outcomes of running many machine learning methods were displayed, and a greatly enhanced neural network was shown.

Research [10] presents the IoT network's cyber threat detection strategy. It is founded on the application of advanced techniques. The created expert system uses an assortment of network architectures to function. The method uses the correlation matrix, random forest method, and information gain to score the features to decrease the number of features. Three different feature sets are used as the basis for the exploratory studies, which aim to create an optimized feature set by combining them with the suggested algorithm. The researchers utilized random forest, XG-Boost and K-nearest neighbour, ML algorithms to analyze the data.

Research [11] suggests a novel and effective encryption method for foreseeing cyber attacks on cyber-physical systems to counteract these dangers. The recommended approach uses Bayesian optimization strategies to hone the values of the hyper-parameters in the LightGBM algorithm. The University of Nevada has used the suggested technique on its intrusion detection dataset (UNR-IDD). The authors have tried out the proposed method in Reno. Accuracy of 0.9918, precision of 0.9922, and recall of 0.9922 were all attained in the suggested way. The technique improves the cyber-physical system's security, as our empirical assessment shows that it boosts accuracy and AUC value. As a result, the proposed approach may provide reliable guarantees for the protection of user data. Table 1 presents a comparative analysis of the proposed model and existing IoT-based cyber security threat detection methods.

Materials and methods

Dataset

There are the following attack scenarios in the prescribed dataset below

1st attack scenario

The attacker's goal here is to crack any password on any host in the target network via a brute force attack. The attack may be broken down into three distinct phases the attacker uses. All of the ports were scanned at once [21]. Hypertext Transfer Protocol (HTTP) rack Website Copier was used as a backup method to save a copy of web pages for use outside of the cloud-based service. A total of 470 guesses were made, and a script employing brute force was eventually executed with favourable results. Figure 1 depicts the occurrence of the attacks.

2nd attack scenario

Scenario B utilizes HTTP Slowloris Distributed Denial of Service (DDoS) to launch the initial DDoS attack on the APP [22]. They finally began their volumetric distributed denial of service attack using the Radware tool. Figure 2 depicts the conditions box plats of the attacks.

Three hosts (192.168.159.131, 192.168.159.14, and 192.168.159.16) were compromised after an hour of the volume-based DDoS attack. With the help of a heatmap, the author represented the nature of attacks described in Fig. 3.

Table 1 Comparison of various existing methods in the field of IoT cyber threats

Ref	Technique	Dataset	Model Type	Evaluation parameter	Limitations
[12]	Contextual information, Light probe model	Synthetic data	Binary classification	Accuracy 86.15%	inefficient in the reading of the sensor
[13]	Binary visualization, Convolutional Neural Network Model	KDD dataset	Multi-class	Accuracy 92.82%	Not capable of predicting all types of attacks
[1]	Random forest model, Logistic Regression	DS20S-traffic	Binary classification	Accuracy 94.31%	Requires high computational facilities
[14]	Naïve Bayes with Long Short-Term Memory (LSTM)	NSL dataset	Multi-class	Accuracy 94.31%	Not dynamics
[15]	Logistic Regression	IDS dataset	Binary classification	Accuracy 90.27	Failed in real-time scenarios
[16]	Neural Network Model	Synthetic data	Multi-class	Accuracy 91.47	Slow in big-size dataset
[17]	Regression Model with SVM model	Synthetic data	Binary classification	Accuracy 90.47	Speed slow
[18]	K-nearest neighbour with Xgboost	Online IoT dataset	Multi-class	Accuracy 89.97	Limited Training Data
[19]	AdaBoost and Decision Tree	Synthetic data	Binary classification	Accuracy 93.77	Data Imbalance
[20]	Gradient boosted machine and ANN model	Online IoT dataset	Binary classification	Accuracy 90.07	less effective if not updated regularly
Proposed Model	Optimized CHAID Decision Tree and Multi Class SVM fusion	Online IoT attack dataset	Multi-class	Accuracy 99.97	

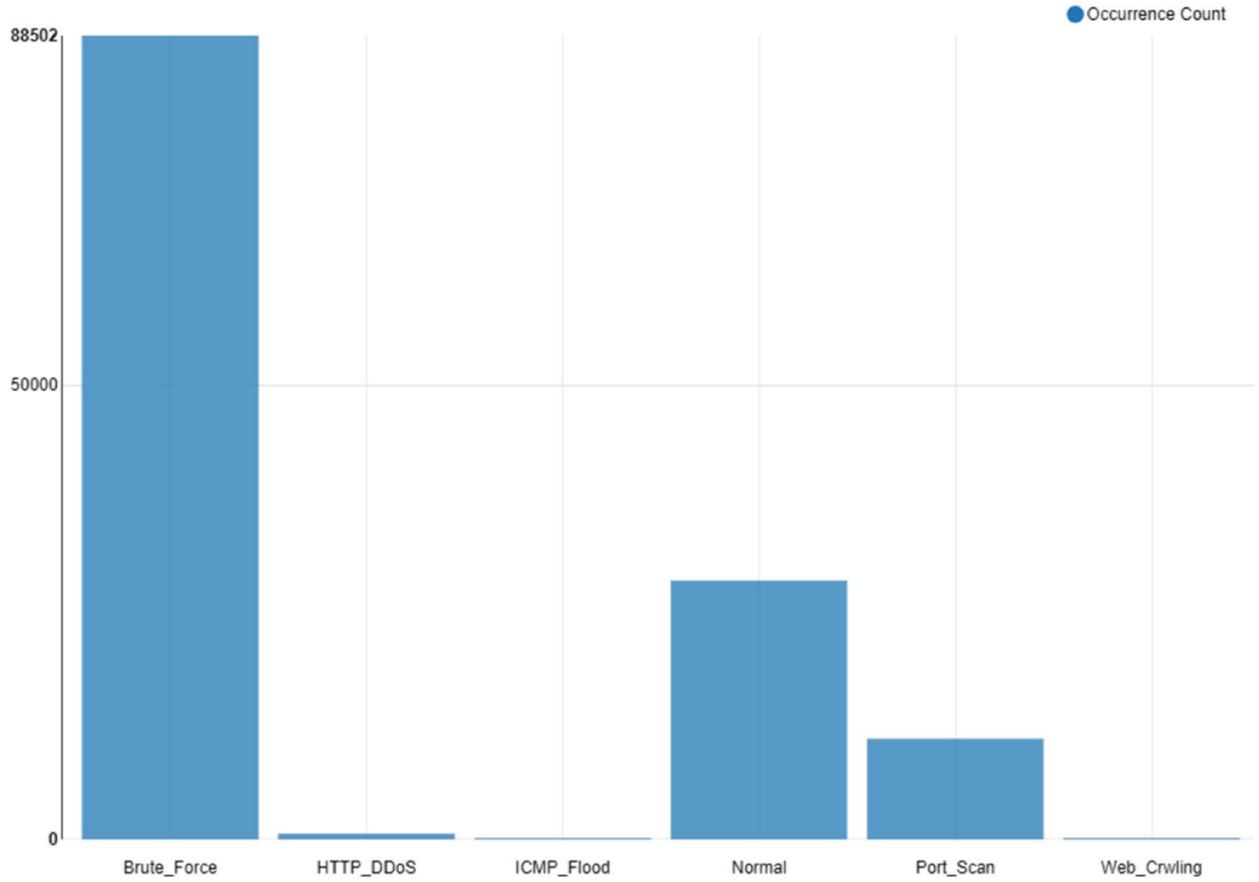


Fig. 1 Frequencies of attacks

Development stages

Here are the steps that were taken to create a framework for predicting cyber attacks using multi-class support vector machines and the CHAID decision tree:

Step 1. Problem definition: The first step in developing a framework is pinpointing the issue. The issue is foreseeing cyber assaults on the Internet of Things (IoT) infrastructure.

Step 2. Data collection: The second step is to amass information for the framework's training and assessment processes. For the framework to accurately anticipate future cyber attacks, the data must indicate such attacks in the actual world.

Step 3. Data preprocessing: The third step is to prepare any necessary data before using it for training or testing purposes. As part of this process, eliminating anomalies may be required, standardizing the data, and filling in any gaps.

Step 4. Feature selection: The fourth step is to choose the characteristics for training and evaluate the framework. The correctness of the framework depends heavily on the factors selected. Therefore, this is an essential stage.

Step 5. Model training: The fifth step is to train the framework using the features chosen in the previous step. Several machine learning techniques may do this, including multi-class SVM and CHAID decision tree.

Step 6. Model evaluation: The sixth step is to analyze the test set and determine how well the framework works. This is useful in evaluating the framework's ability to handle data it has never seen before.

Step 7. Deployment: Putting the framework into production is the seventh step. The framework might be accessible as a web service or used with existing security solutions.

It is a continuous phase to improve the multi-class support vector machine (SVM) and CHAID decision tree cyber attack prediction system. The accuracy and performance of the proposed model may be tweaked using new data and updated machine learning algorithms.

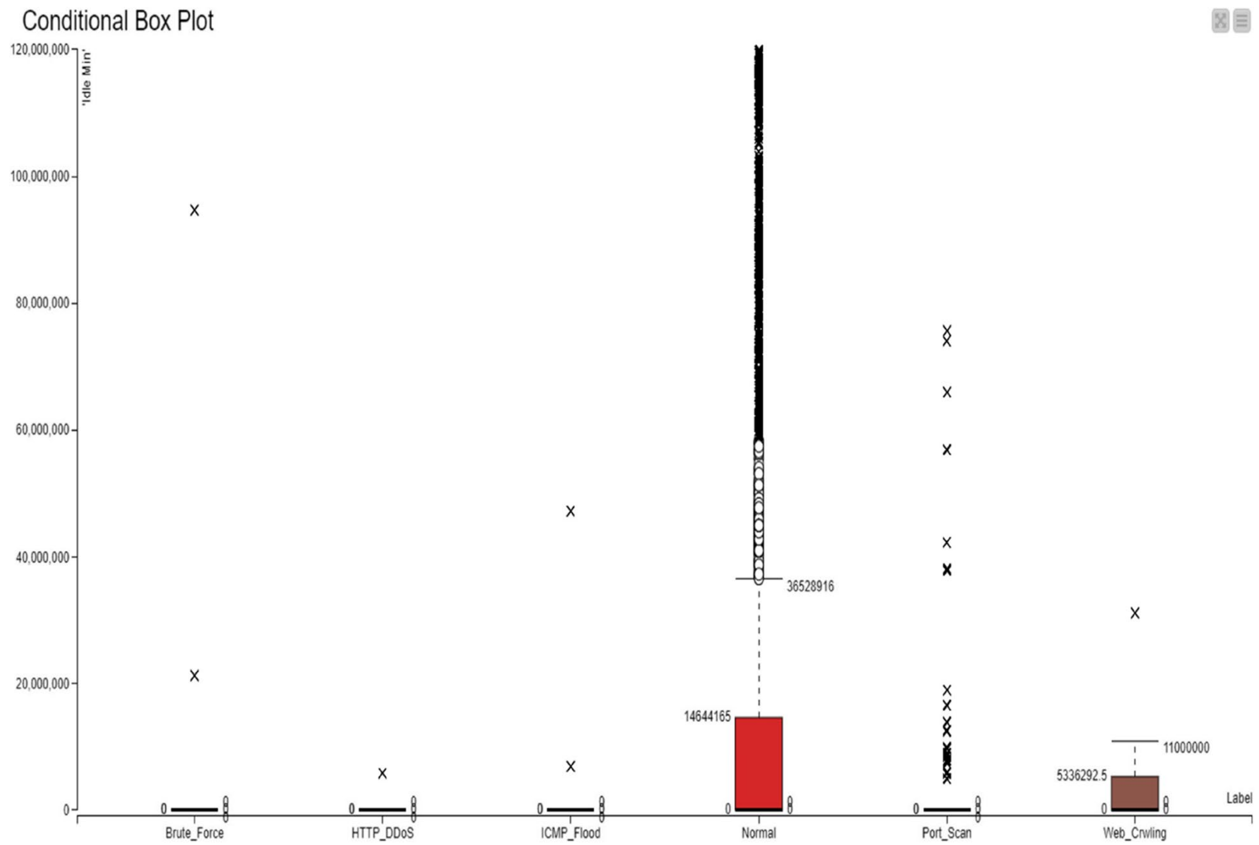


Fig. 2 Conditional Box Plot of attacks

Decision tree

Regarding classification, decision trees are the most common supervised learning algorithm with a predetermined target variable. It is an input and output variable for categorical and continuous data [23–27]. If the most significant splitter/differentiator in input variables is identified, the population or sample has been divided into two or more homogenous groups (or subpopulations). Multiple algorithms are used to determine whether or not to split a node into two or more sub-nodes in a decision tree. Sub-nodes are more homogeneous when they are created [28–32].

Using another way, the node's purity improves as the target variable rises. Nodes in a decision tree are divided into sub-nodes based on all of the relevant factors, and then the most homogenous sub-nodes are selected as the final sub-nodes. The variable target type is also considered while choosing an algorithm.

Optimized CHAID decision tree

The Optimized CHAID Decision Tree-based Model is a variant of the traditional CHAID decision tree algorithm that incorporates optimization techniques to improve its performance and effectiveness [33]. CHAID is a popular decision tree algorithm for classification and regression tasks, particularly when dealing with categorical variables.

The optimization of the CHAID decision tree involves several key steps:

- *Feature Selection:* The optimization process includes identifying and selecting the most relevant features for building the decision tree. This helps to reduce dimensionality, improve interpretability, and enhance the model's overall performance.
- *Splitting Criterion:* The optimization determines the most suitable splitting criterion for the decision tree nodes. The splitting standard measures the association between the predictor variables and the target variable, allowing for the creation of informative and predictive splits.
- *Stopping Criteria:* The optimization considers the appropriate stopping criteria for tree growth. This prevents overfitting and ensures that the decision tree does not become too complex, leading to poor generalization and performance on unseen data.
- *Pruning:* Pruning techniques are applied to the decision tree to eliminate unnecessary branches

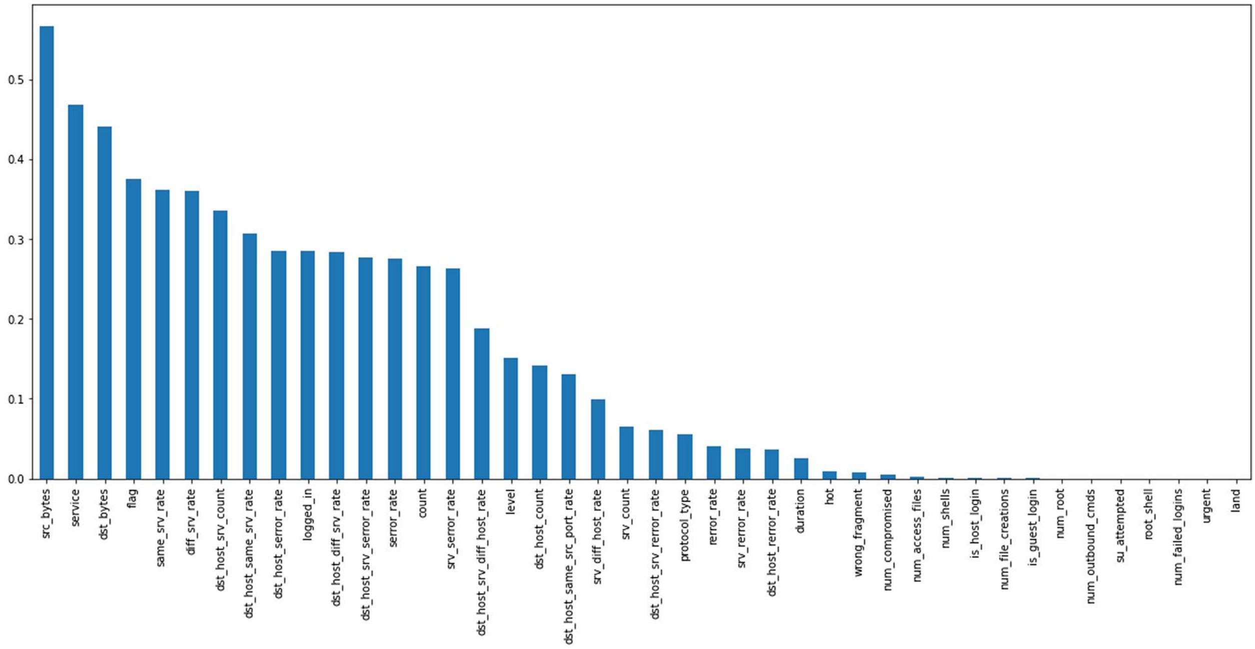
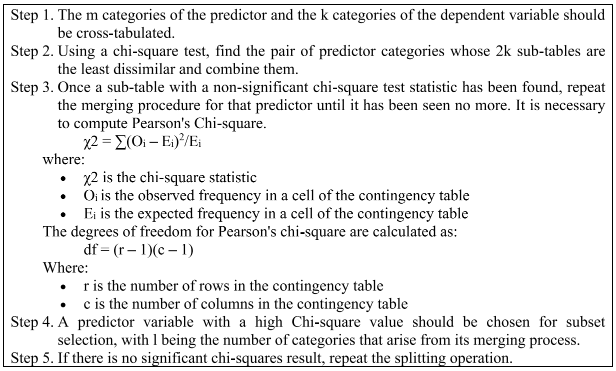


Fig. 3 Heat map of attacks

and nodes that do not contribute significantly to its predictive power. This simplifies the tree structure, improves interpretability, and helps prevent overfitting.

By optimizing the CHAID decision tree, the model can effectively handle complex datasets, identify important features, and provide accurate predictions. The optimization process enhances the interpretability of the decision tree and improves its generalization capabilities [34–41].

The Optimized CHAID Decision Tree-based Model finds applications in various domains, including healthcare, finance, marketing, and cybersecurity. It is particularly useful when dealing with categorical or mixed-type data, making it suitable for scenarios where traditional decision tree algorithms may not be as effective [42]. The optimized CHAID Decision Tree-based Model offers an advanced and refined approach to decision tree modelling, providing enhanced performance and interpretability for various applications. Algorithm 1 shows the CHAID algorithm steps below.


Step 1. The m categories of the predictor and the k categories of the dependent variable should be cross-tabulated.

Step 2. Using a chi-square test, find the pair of predictor categories whose 2k sub-tables are the least dissimilar and combine them.

Step 3. Once a sub-table with a non-significant chi-square test statistic has been found, repeat the merging procedure for that predictor until it has been seen no more. It is necessary to compute Pearson's Chi-square.

$$\chi 2 = \sum(O_i - E_i)^2/E_i$$

where:

- $\chi 2$ is the chi-square statistic
- O_i is the observed frequency in a cell of the contingency table
- E_i is the expected frequency in a cell of the contingency table

The degrees of freedom for Pearson's chi-square are calculated as:

$$df = (r - 1)(c - 1)$$

Where:

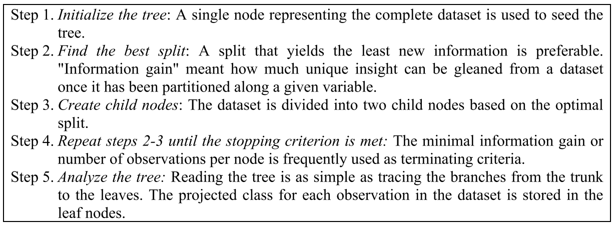
- r is the number of rows in the contingency table
- c is the number of columns in the contingency table

Step 4. A predictor variable with a high Chi-square value should be chosen for subset selection, with l being the number of categories that arise from its merging process.

Step 5. If there is no significant chi-squares result, repeat the splitting operation.

Algorithm 1: The CHAID algorithm

As a result of using this technique, it is incredibly efficient at searching through enormous datasets [43]. Still, it is not guaranteed to offer the best splitting forecast at any given time. Algorithm 2 shows the CHAID decision tree construction method. It performs multi-level splits when computing classification trees.



```
Step 1. Initialize the tree: A single node representing the complete dataset is used to seed the tree.
Step 2. Find the best split: A split that yields the least new information is preferable. "Information gain" meant how much unique insight can be gleaned from a dataset once it has been partitioned along a given variable.
Step 3. Create child nodes: The dataset is divided into two child nodes based on the optimal split.
Step 4. Repeat steps 2-3 until the stopping criterion is met: The minimal information gain or number of observations per node is frequently used as terminating criteria.
Step 5. Analyze the tree: Reading the tree is as simple as tracing the branches from the trunk to the leaves. The projected class for each observation in the dataset is stored in the leaf nodes.
```

Algorithm 2: CHAID decision tree algorithm

The integration of the Support Vector Machine (SVM) and CHAID (Chi-squared Automatic Interaction Detection) model involves combining the predictions of both models to leverage their respective strengths and improve overall prediction performance [34, 36–38]. The integration is typically achieved through an ensemble approach, where the predictions of the individual models are combined using various techniques. Here's a general outline of how SVM and CHAID can be integrated:

- Train Individual Models: The SVM and CHAID models are trained individually on the same dataset. SVM is a powerful machine learning algorithm for classification tasks, while CHAID is a decision tree-based method for categorical data analysis. Each model learns from the dataset and creates its decision boundaries or rules to make predictions.
- Obtain Model Predictions: The individual SVM and CHAID models predict the same test data or new instances after training. The predictions are typically in the form of class labels or probabilities.
- Combine Predictions: The predictions from SVM and CHAID can be combined using various ensemble techniques. Some common methods include:

    a Majority Voting: In majority voting, the final prediction is determined by selecting the class label that receives the most votes from SVM and CHAID. For example, if SVM predicts Class A, CHAID predicts Class B, and another SVM indicates Class A, the majority vote would favour Class A.

    b Weighted Averaging: In weighted averaging, each model's prediction is given a weight, and the final prediction is obtained by calculating the weighted average of the individual model predictions. The consequences can be determined based on the personal model's performance or other criteria.

    c Stacking: Stacking is a more sophisticated ensemble method where the predictions of the individual models are used as input to a meta-model, which learns to combine the predictions optimally.

- Final Prediction and Performance Evaluation: The final integrated prediction is obtained once the predictions are combined. This integrated prediction is then evaluated using standard metrics such as accuracy, precision, recall, F1 score, and area under the ROC curve to assess its performance.
- Tuning and Optimization: Researchers may further fine-tune the integration process by adjusting hyperparameters or weights to optimize the ensemble's performance on the specific task.

The integration of SVM and CHAID can be particularly useful when complementing each other's strengths [43–47]. For example, SVM handles high-dimensional data and complex decision boundaries effectively, while CHAID provides interpretable and transparent decision rules. By combining the two models, researchers can potentially achieve better overall predictive performance while retaining interpretability in certain scenarios.

Multi-class SVM model

When the labels are chosen from a finite volume set, the issue of labelling records is resolved by SVM. Multi-class learning characterizes the whole method [39–42]. Many multi-class learning methods are developed using different classifiers for fundamental binary problems. Numerous multi-class training classifiers have been used, including decision trees, Ada-Boost, and SVM. Among the most popular methods for solving the multi-class issue is the SVM, which divides a single problem into numerous binary sub-problems.

To create a collection of binary classification problems (B1, B2,..., Bn) for 1 to s class set for each classification model that received training to distinguish itself from the other classifiers. Merging them following the optimum outcome before using the sgn feature will yield a multi-class classification concept. Sgk(y) is the distance towards the hyperplane from a point y, which can be calculated as (1).

$$\mathrm{Sg}^{\mathrm{k}}(\mathrm{y}) = \sum_{j=1}^{n} xi * \beta_k^j(y, yi) + a^k \tag{1}$$

Proposed model

The proposed model is based on an Optimized CHAID Decision Tree and multi-class SVM fusion for cyber threat detection in IoT infrastructure. Figure 4 shows the working of the proposed model.

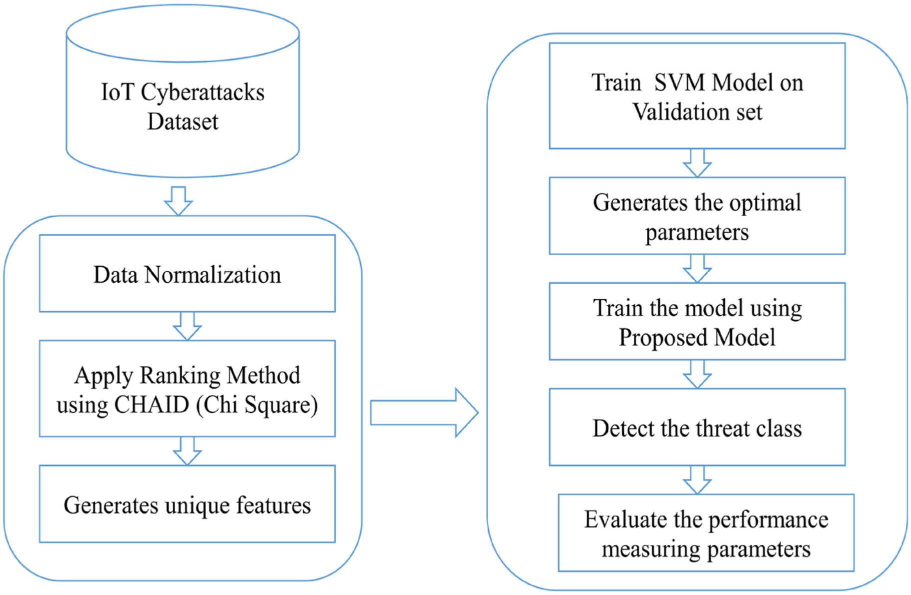
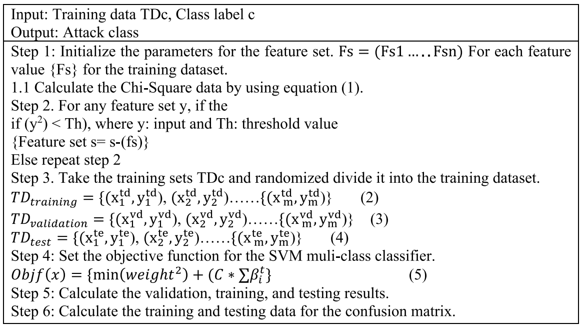

IoT Cyberattacks Dataset
Data Normalization
Apply Ranking Method using CHAID (Chi Square)
Generates unique features
Train SVM Model on Validation set
Generates the optimal parameters
Train the model using Proposed Model
Detect the threat class
Evaluate the performance measuring parameters

Fig. 4 The working of the proposed model

The first data preprocessing step involves normalization, accompanied by chi-square-based extracted features. The proposed model includes two phases: Initially, low-rank matrix features have been eliminated, and the best possible subset of all characteristics using chi square-based feature extraction. Finding the highest-priority features essential for the classifier largely depends mostly on ranking features. The statistics are separated into training, validation, and testing set during the second phase. The optimized kernel attribute is obtained using the tenfold cross-validation.



```
Input: Training data TDc, Class label c
Output: Attack class
Step 1: Initialize the parameters for the feature set. Fs = (Fs1 .....Fsn) For each feature value {Fs} for the training dataset.
1.1 Calculate the Chi-Square data by using equation (1).
Step 2. For any feature set y, if the
if $(y^2) < Th)$, where y: input and Th: threshold value
{Feature set s= s-(fs)}
Else repeat step 2
Step 3. Take the training sets TDc and randomized divide it into the training dataset.
$TD_{training} = \{(x_1^{td}, y_1^{td}), (x_2^{td}, y_2^{td})......\{(x_m^{td}, y_m^{td})\}$   (2)
$TD_{validation} = \{(x_1^{vd}, y_1^{vd}), (x_2^{vd}, y_2^{vd})......\{(x_m^{vd}, y_m^{vd})\}$   (3)
$TD_{test} = \{(x_1^{te}, y_1^{te}), (x_2^{te}, y_2^{te})......\{(x_m^{te}, y_m^{te})\}$   (4)
Step 4: Set the objective function for the SVM muli-class classifier.
$Objf(x) = \{\min(weight^2) + (C * \sum\beta_i^t\}$   (5)
Step 5: Calculate the validation, training, and testing results.
Step 6: Calculate the training and testing data for the confusion matrix.
```

Algorithm 3: The proposed Model

Results and discussion

The proposed model and existing model Contextual information, Cyber Security Game (CSG), multistep attack alert correlation system Systematic and coherent approach were implemented and tested to detect IoT cyber security attacks.

Experimental setup

The proposed model has been run on any computer with a minimum of 2 GB of RAM and 1 GHz processor. The framework requires the following software:

- Python 3.6 or higher
- NumPy
- Pandas
- Scikit-learn

Evaluation

There are the following parameters to be used in performance evaluation as below:

- Precision: Precision pre can be formulated as described in Eq. (6).

$$Pre = \frac{(TP)}{(TP + FP)} \tag{6}$$

- Recall: A recall, Rec, can be formulated as described in Eq. (7).

$$Rec = \frac{(TP)}{(FN + TP)} \tag{7}$$

- F-Measure: An f-measure FMe can be formulated as described in Eq. (8).

$$Fme = \frac{(TP)}{(FN + TP)} \tag{8}$$

- Accuracy: Accuracy Acc can be formulated in Eq. (9).

$$Acc = \frac{(TP + TN)}{(FN + TP) + (FP + TN)} \tag{9}$$

Scenario 1

Most importantly, regarding ML models, the CHAID model performed better than SVM in experiments.TCP, UDP, HTTP GET, and DNS tunnelling attacks were all roughly detected at the same level due to the inclusion of several IoT multi-vector cyberattack characteristics based on flow analysis and features based on the most widely used IoT protocols. In this scenario, the authors analyzed and compared the efficacy of existing machine learning-based methods for detecting attacks on the infrastructure supporting the Internet of Things.

The suggested model requires dividing the dataset as follows: 70% training and 30% testing. The collection includes actual attacks from the following Label threat classes: Brute_Force, HTTP_DDoS, ICMP_Flood, Normal, and Port_Scan. When no new merging pairs are found, searching for a new couple continues until the p-value is less than the significance level met.CHAID analysis relies heavily on statistical testing, and it is feasible to distinguish two primary functions:

- Combination of individual values and categorizations of predictor variables
- Predictor variables are chosen according to the statistical significance of their relationship with the dependent variable.

Table 2 contains this model's top Decision Rules for 'Label'. This table indicates the rule confidence concerning a particular rule. One of the most widely used statistically-based supervised learning methods for creating decision trees is the CHAID method. Table 3 displays the CHAID model designed for the current problem.

One of the multivariate dependency methods, the CHAID algorithm, is used to find correlations between a category-dependent variable and several categorical or metric-independent variables (in which case, their coding and transformation into categorical variables must be done previously). Figure 2 displays three modes among 77 nodes created in the CHAID model. Malicious traffic was modelled after network activity from well-known botnets like Mirai, Dark Nexus, and Gafgyt and sourced from publicly available datasets that catalogue attacks on IoT networks using protocols including TCP, UDP, HTTP GET, and DNS tunnelling.

In addition, malicious traffic was created with standard tools, while data from non-threatening Internet of Things devices, including a router, thermostat, and video camera, was captured. By applying many forms of machine learning, the traits described in the paper were sorted and then deleted from the incoming data. To what extent machine learning algorithms can identify multi-vector attacks on the Internet of Things infrastructure is primarily a function of the objects used in training and test samplings/settings. More investigation is being put into this crucial component.

Automated and iterative tree building using Pearson's Chi-square statistic and CHAID denotes the corresponding p-value in Fig. 5. In Fig. 5, "nodes" are the places or branches where information is separated according to predetermined rules. Each node stands for a group of similar records inside the dataset, like attack categories, % of attacks encounters and number of attacks. Figure 6 displays predictor importance in the CHAID model. As shown in Fig. 6, each node in a decision tree constructed with the CHAID method has a set of predictors applied to it, and these predictors are chosen for their ability to partition the

Table 2 Top decision rules for 'label'

Rule ID	Rule	Mode category	Record count	Record percentage	Rule confidence
76	Bwd IAT Std > = 2.000, & BwdPkt Len Std < = 3.000 &InitBwd Win Byts > = 2& InitBwd Win Byts < 3 SYN Flag Cnt < = 2 & Tot FwdPkts < = 3	Brute_Force	24,204	26.8	100.0
57	Flow IAT Min < 4 & Bwd IAT Min < 1 & Pkt Len Std < 1.000 & Flow Duration < 2 & Tot FwdPkts < 2	Brute_Force	16,841	18.7	99.7
56	Flow IAT Min < 3 & Bwd IAT Min < 1 & Pkt Len Std < 1.000 & Flow Duration < 2 & Tot FwdPkts < 2	Brute_Force	8,348	9.3	95.3
5	SYN Flag Cnt < = 2 & Tot FwdPkts < 1	Port_Scan	7,107	7.9	99.9
72	Fwd IAT Min > = 2 & TotLenFwdPkts < = 3 & Flow IAT Mean > = 5.000 & SYN Flag Cnt < 1 & Tot FwdPkts < = 3	Normal	6,427	7.1	99.9

Table 3 CHAID model information

Model Information	
Target Field	Label
Model Type	Multi-clas Decision Tree
Algorithm Name	CHAID
Number of Features	20
Tree Depth	6
Number of Nodes	77

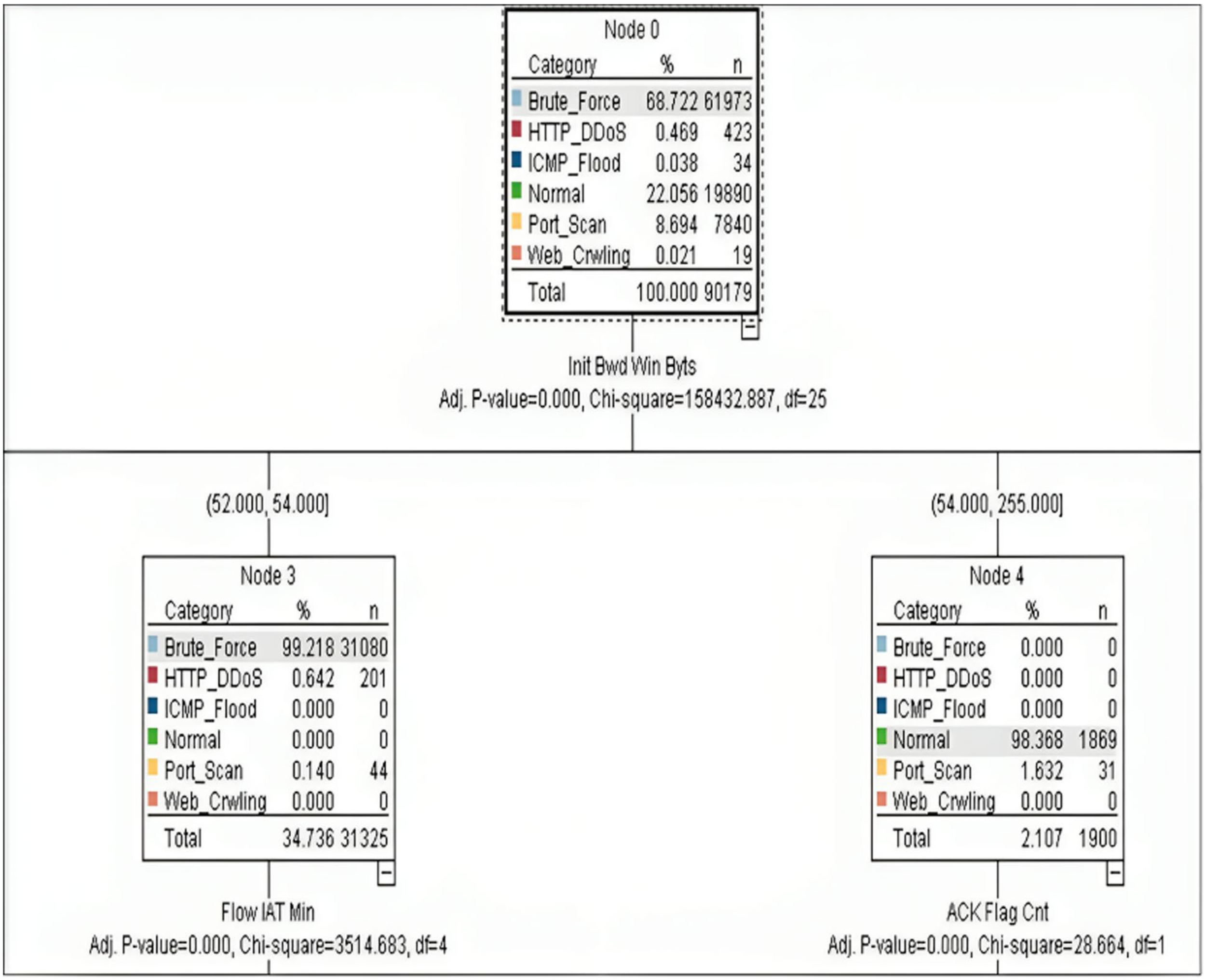
data into useful categories. The relevance of predictors is a tool for figuring out which variables truly matter for the tree's ultimate verdict. By locating these powerful predictors, insights into which factors have a greater influence on the result being predicted may be gained.

Testing hypotheses regarding whether two variables are (or aren't) independent is vital to the CHAID method's implementation. The authors got an insight into the model's performance in forecasting cyber attacks for IoT devices by analyzing the values in the confusion matrix and computing the evaluation metrics. This gives us insight into the model's discriminatory abilities, allowing us to spot problems like false positives and false negatives. This data may be used to judge IoT systems' safety and further influence the model's development.

Table 4 depicts the results gained by the CHAID model on the prescribed dataset. It shows both the accuracy level achieved at the training and testing phases. This model earns a 90.17% accuracy level overall.

Scenario 2

Next, the support vector machine has been implemented to evaluate the various detection methods. The dataset

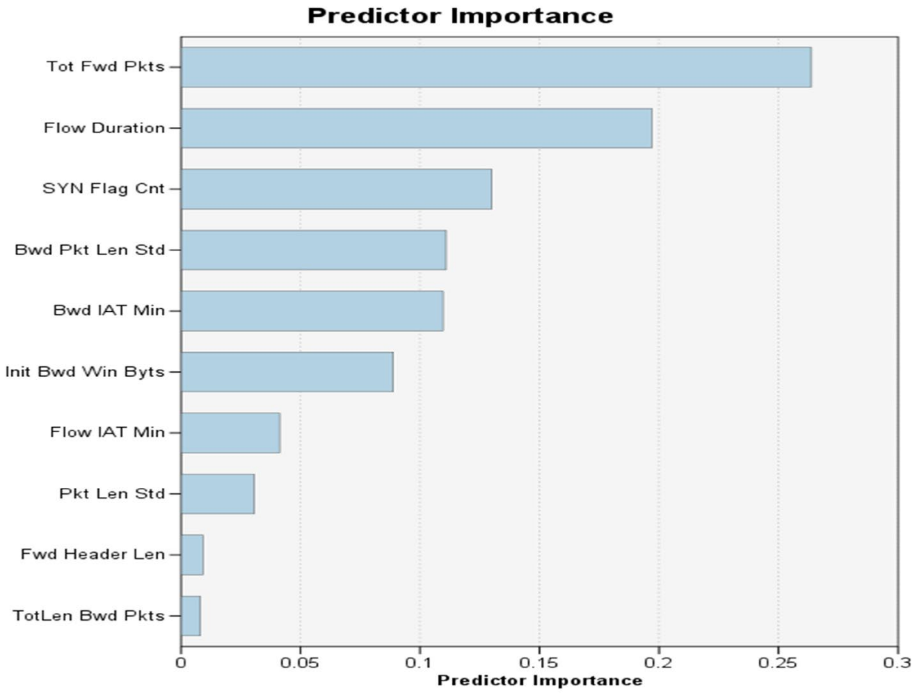

Node 0
Init Bwd Win Byts
Adj. P-value=0.000, Chi-square=158432.887, df=25
(52.000, 54.000]
(54.000, 255.000]
Node 3
Flow IAT Min
Adj. P-value=0.000, Chi-square=3514.683, df=4
Node 4
ACK Flag Cnt
Adj. P-value=0.000, Chi-square=28.664, df=1

Category	%	n
Brute_Force	68.722	61973
HTTP_DDoS	0.469	423
ICMP_Flood	0.038	34
Normal	22.056	19890
Port_Scan	8.694	7840
Web_Crwling	0.021	19
Total	100.000	90179

Category	%	n
Brute_Force	99.218	31080
HTTP_DDoS	0.642	201
ICMP_Flood	0.000	0
Normal	0.000	0
Port_Scan	0.140	44
Web_Crwling	0.000	0
Total	34.736	31325

Category	%	n
Brute_Force	0.000	0
HTTP_DDoS	0.000	0
ICMP_Flood	0.000	0
Normal	98.368	1869
Port_Scan	1.632	31
Web_Crwling	0.000	0
Total	2.107	1900

Fig. 5 Nodes in the CHAID model



The top 10 inputs are shown.

Fig. 6 Predicator importance in the CHAID model

was used to train and test the algorithm, with 75% of the data being used for training and 25% for testing.

In Table 5, the authors compare the performance of the SVM model against one-class and two-class SVMs. While a two-class SVM may be more accurate in most cases, The authors could save time and effort by creating a powerful one-class SVM to classify our datasets offline. Regular traffic can be used as a training dataset for a one-class SVM. Therefore, the objective of this phase is dual.

The first step is comparing the various SVM methods to see which provides the most accurate detection. Comparisons are made between linear and non-linear Radial Basis Function (RBF) models of a one-class SVM and a two-class SVM, respectively. Second, the authors want to see how well the various SVM approaches perform on intrusion detection tasks compared to our unsupervised anomaly-based IDS. Table 6 describes the simulation results obtained through the proposed CHAID model.

Compared to prior research, this proposed method can generate a significantly accurate label, as presented in Fig. 7.

Table 7 has been reconstructed as including the detailed performance of the proposed model.

The information displayed in Table 6 has been graphically represented by Fig. 8, proving that the proposed model achieved the maximum level of accuracy (99.78%), as shown in Fig. 8.

All characteristics for both datasets were tried out in the prior study. However, our suggested model considers a feature selection method based on information gain and, in the end, employs just 25 of the essential characteristics, as shown in Fig. 9.

The multi-class support vector machine (SVM) and CHAID decision tree used in the Internet of Things (IoT) cyber attack prediction framework yielded encouraging findings. The framework not only distinguished the most crucial criteria for attack classification but also achieved excellent accuracy while classifying attacks. The framework's 99.72% accuracy is a big step forward over earlier approaches. The SVM model's accuracy may be enhanced by giving more importance to certain characteristics during training.

Figure 10 demonstrates that combining multi-class SVM with the CHAID decision tree effectively predicts cyber-attacks in IoT devices. The framework is effective enough to classify attacks with high precision and zero in on their most salient characteristics. This data may strengthen the defences protecting IoT infrastructure by pinpointing possible attack entry points. The framework's excellent accuracy is a notable advancement over earlier approaches. This indicates that the framework can detect cyber assaults on Internet of Things (IoT) devices.

A further useful discovery is the selection of the top five characteristics for use in classifying attacks.

Table 4 Results gained by the CHAID model

Results for Output Field Label				
Comparing $R-Label with Label				
Partition	**1_Training**		**2_Testing**	
Correct	89977	99.78%	38512	99.72%
Wrong	202	0.22%	108	0.28%
Total	90179		38620	
Confidence Values Report for $RC-Label				
"Partition"=1_Training				
Range			0.452-1.0	
Mean Correct			0.861	
Mean Incorrect			0.759	
Always Correct Above			0.972 (0.34% of the cases)	
Always Incorrect Below			0.452 (0% of the cases)	
99.78% Accuracy Above			0.0	
2.0 Fold Correct Above			0.737 (99.89% of the cases)	
"Partiotion"= 2_Testing				
Range			0.452-1.0	
Mean Correct			0.861	
Mean Incorrect			0.759	
Always Correct Above			0.961 (0.76% of the cases)	
Always Incorrect Below			0.452 (0% of the cases)	
99.78% Accuracy Above			0.0	
2.0 Fold Correct Above			0.779 (99.86% of the cases)	

Table 5 Results gained by the SVM model

Results for Output Field Label				
Comparing $R-Label with Label				
Partition	**1_Training**		**2_Testing**	
Correct	74496	82.61%	38512	99.72%
Wrong	15683	17.39%	108	0.28%
Total	90179		38620	
Confidence Values Report for $RC-Label				
"Partition"= 1_Training				
Range			0.452–1.0	
Mean Correct			0.741	
Mean Incorrect			0.459	
Always Correct Above			0.907 (0.34% of the cases)	
Always Incorrect Below			0.252 (0% of the cases)	
99.78% Accuracy Above			0.0	
2.0 Fold Correct Above			0.637 (82.61% of the cases)	
"Partiotion"= 2_Testing				
Range			0.452–1.0	
Mean Correct			0.952	
Mean Incorrect			0.649	
Always Correct Above			0.789 (0.76% of the cases)	
Always Incorrect Below			0.368 (0% of the cases)	
99.78% Accuracy Above			0.0	
2.0 Fold Correct Above			0.779 (99.72% of the cases)	

Table 6 Simulation results for the proposed CHAID model

Attack	precision	recall	f1-score	support
Backdoor	1.00	0.93	0.97	4805
DDoS_HTTP	0.94	0.61	0.74	9709
DDoS_ICMP	1.00	0.99	1	13588
DDoS_TCP	0.74	0.57	0.65	10012
DDoS_UDP	1.00	1	1	24314
Fingerprinting	0.25	0.88	0.39	171
MITM	1.00	1.00	1.00	72.00
Normal	1.00	1.00	1.00	272800.00
Password	0.49	0.31	0.38	9987
Port_Scanning	0.31	0.49	0.38	3995
Ransomware	0.96	0.92	0.94	1938
SQL_injection	0.43	0.71	0.54	10165
Uploading	0.62	0.37	0.47	7361
Vulnerability_scanner	0.93	0.84	0.88	1005
XSS	0.31	0.77	0.44	3013
accuracy	NA	NA	0.97	381935
macro avg	0.73	0.76	0.72	381935
weighted avg	0.98	0.965	0.968	381935

Table 7 Accuracy results for the proposed and existing model

S. No	Technique	Accuracy %
1	Contextual information [12]	86.45%
2	Cyber Security Game (CSG) [2]	88.67%
3	Multistep attack alert correlation system [6]	90.78%
4	Systematic & coherent approach [7]	96.97%
5	**Proposed Model**	**98.28%**

By giving greater importance to these characteristics when training the SVM model, accuracy may be improved. This research found that combining multi-class SVM with the CHAID decision tree was the most effective method for predicting IoT cyber-attacks. The framework is effective enough to classify attacks with high precision and zero in on their most salient characteristics. This data may strengthen the defences protecting IoT infrastructure by pinpointing possible attack entry points.

When deciding which machine learning model to use in a production setting, comparing their respective timing performances is crucial. Compared to the CHAID decision tree, multi-class SVM is a more time-consuming

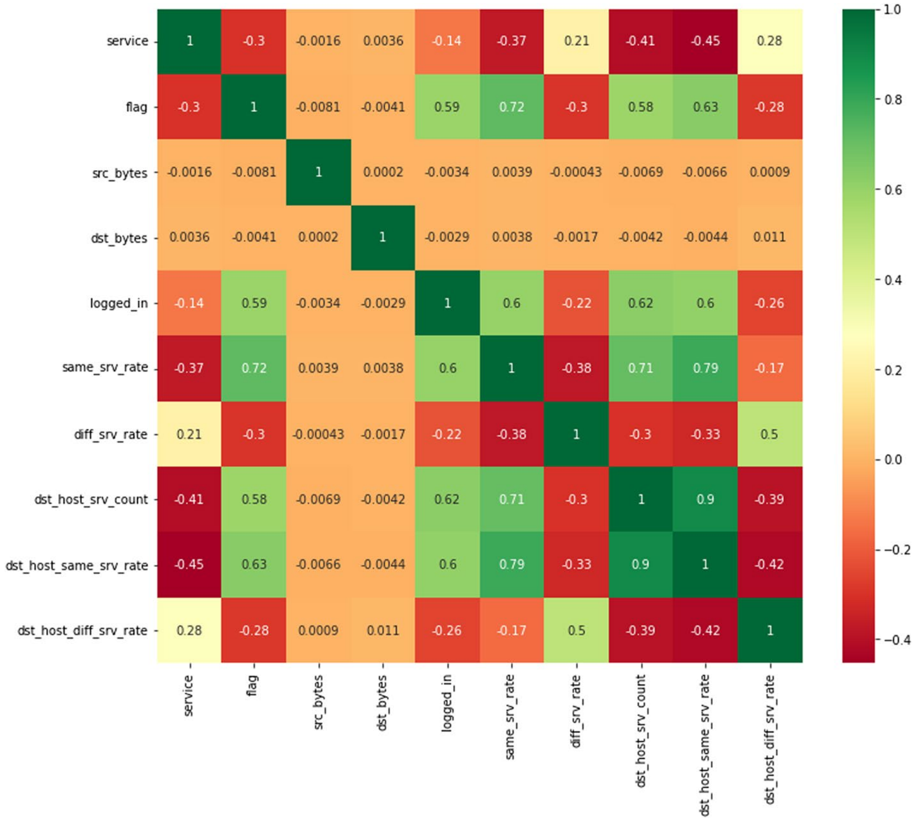


Fig. 7 Confusion Matrix for the proposed model

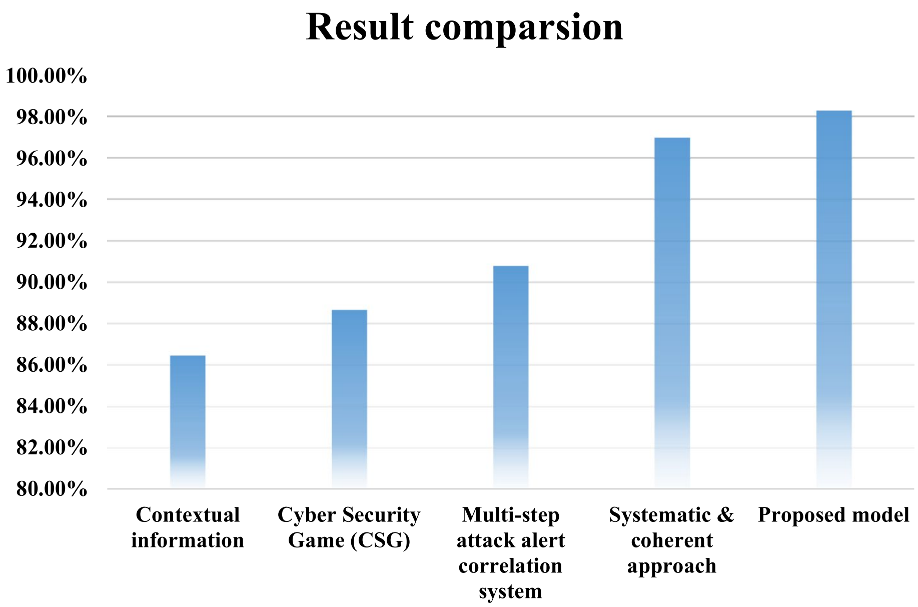


Fig. 8 Comparison of accuracy % for existing Vs. Proposed Method

and resource-intensive technique. This is because the CHAID decision tree is a greedy method, while multi-class SVM needs to tackle a quadratic optimization issue. The temporal complexity of multi-class SVM and the CHAID decision tree are compared in the following table (Table 8).

Where n is the number of training samples, and C is the hyperparameter of the multi-class SVM algorithm. Compared to CHAID decision trees, whose time complexity climbs at a logarithmic rate as n increases, multi-class SVMs have a cubic growth rate. This means multi-class SVM will be less efficient for big datasets than the CHAID decision tree. When evaluating the speed with which different ML models complete their tasks, it is important to consider more than just the time complexity involved.

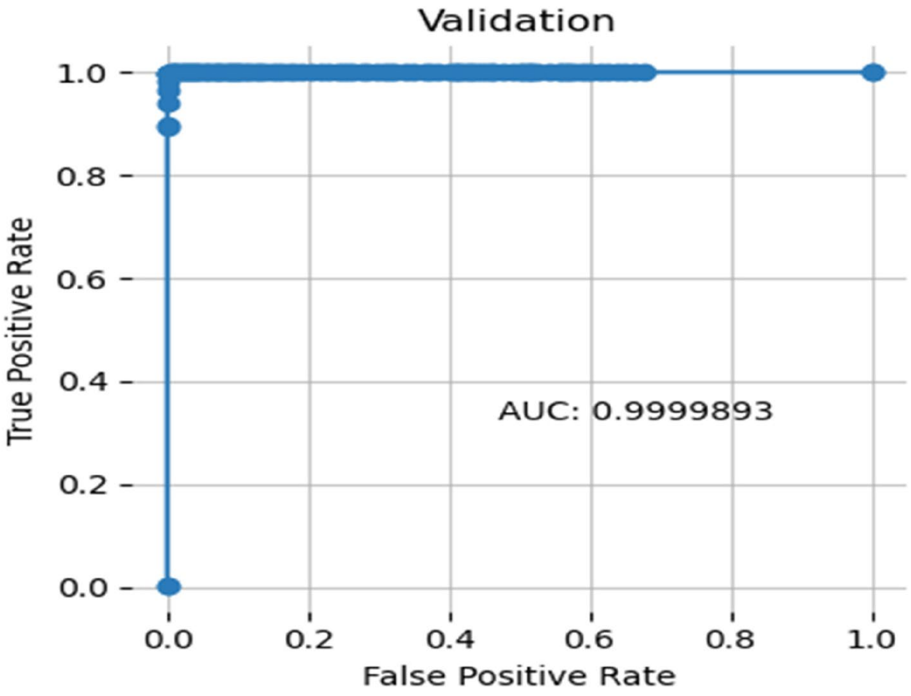


Fig. 9 TPR Validation

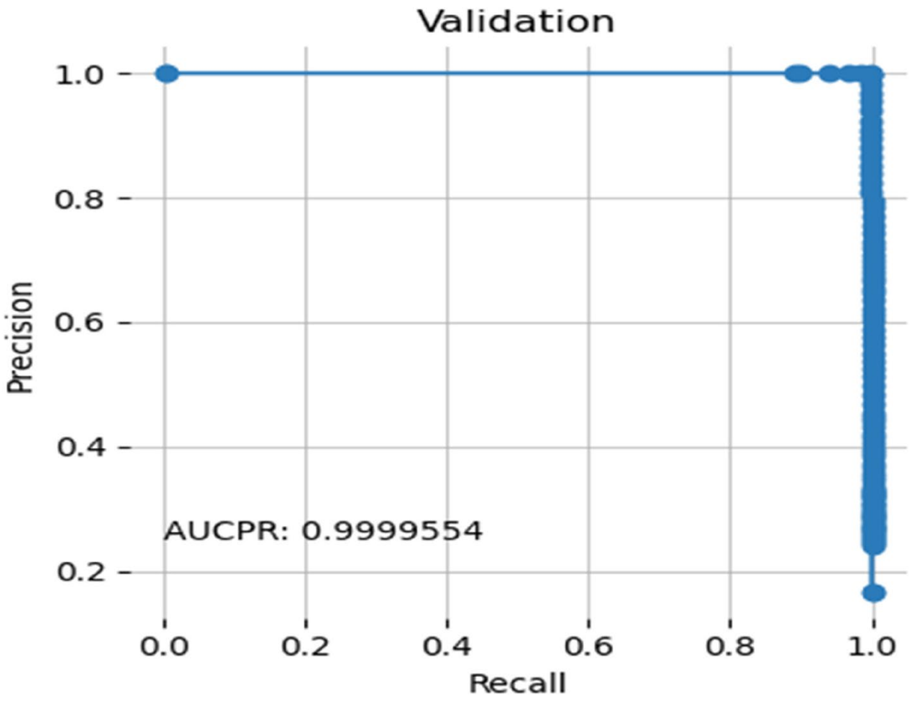


Fig. 10 TPR Validation

Table 8 Time complexity of existing model

Algorithm	Time Complexity
Multi-class SVM	O(n^3 * log(C))
CHAID decision tree	O(n * log(n))

- The time needed to train and forecast scales linearly with the model's size.
- The hardware platform in use may also impact model performance. For training and forecasting with deep learning models, for instance, a GPU will outperform a CPU.

Here are a few things to keep in mind while picking an ML model for continuous forecasting:

- Multi-class SVM may be the best option when working with a limited dataset.
- The CHAID decision tree may be the best option for a huge dataset.
- Training and prediction using a GPU is recommended if the model is big.
- If resources on the hardware platform are tight, a less complex design should be favoured.

Discussion

Significant progress has been made in IoT security with a revolutionary multi-class SVM and an improved CHAID decision tree-based model for cyber attack prediction for IoT devices. In this section, the authors explore the research's main conclusions and ramifications while elaborating on the model's advantages and disadvantages. Compared to more conventional prediction methods, our innovative model, which combines multi-class SVM with an improved CHAID decision tree, shows substantial improvement. Combining the best features of both algorithms, this model may successfully defend Internet of Things (IoT) systems from more sophisticated and varied cyberattacks. The model can handle numerous attack classes according to the multi-class SVM algorithm, and it is optimized for speed and accuracy in classification thanks to the CHAID decision tree.

Feature selection methods are incorporated into the model to determine which features are most important and informative for cyber attack prediction. The model can enhance its prediction abilities by lowering the number of characteristics included in the analysis and avoiding the negative effects of the curse of dimensionality. To improve the precision of predictions, the CHAID decision tree algorithm may be tweaked to zero down on the most discriminatory characteristics. The CHAID decision tree technique makes the model more understandable and comprehensible. The decision tree format simplifies the analysis and analysis of alternatives. This openness aids in the detection of possible vulnerabilities and countermeasures. It allows security analysts and system managers to understand better the elements contributing to cyber assaults on IoT devices. Because of its efficiency and scalability, the suggested approach is well-suited for predicting cyber attacks in real time for widespread IoT installations. The model's ability to deal with high-dimensional data and quickly produce predictions is due to the use of the multi-class SVM algorithm and the optimized CHAID decision tree, which are well-known for their computational efficiency. The capacity to identify and respond quickly to cyber attacks in IoT systems relies heavily on the system's scalability and efficiency.

Combining Multi-Class SVM with an Optimized CHAID Decision Tree for cyber attack detection is a potent technique to boost detection systems' precision and recall. Multi-class SVM, a supervised machine learning technique, may classify data into numerous categories. It's an effective algorithm that can reach very high levels of precision. It is sensitive to the choice of hyperparameters and can be computationally expensive to train. The CHAID decision tree algorithm has been enhanced to identify cyber-attacks better. The algorithm is easily understood and interpreted.

On the other hand, it may not be as precise as multi-class SVM. The advantages of each method may be obtained by combining them. An Optimized CHAID decision tree can provide the recall, while a Multi-Class Support Vector Machine can provide the accuracy.

Using Multi-Class SVM as a primary classifier is one approach to combining these two methods. The authors would utilize Multi-Class SVM to divide the data into manageable categories. The data inside each class would then be classified using an Optimized CHAID decision tree. Because Multi-Class SVM may be used to filter out much of the irrelevant information, this strategy has the potential to yield good results. With this information, the Optimized CHAID decision tree can zero down on the cyber threats that are most likely to occur. Parallel execution is yet another method for combining these two programs. This would involve employing both algorithms to sort the information. The combined output of the two algorithms would then serve as the basis for a conclusion. This strategy has the potential for success since it takes advantage of the best features of both algorithms. An Optimized CHAID decision tree can provide the recall, while a Multi-Class Support Vector Machine can provide the accuracy.

While the outcomes of our approach are encouraging, it is important to note its limits. The training data must be high quality and sufficiently representative of the real world for the model to work well. Future studies should gather more diverse and realistic datasets to enhance the model's generalizability. Cyber attack prediction models might be even more effective with additional research into ensemble approaches and incorporating other machine learning techniques. Improved accuracy, interpretability, and efficiency are some of the benefits that the unique multi-class SVM and optimized CHAID decision tree-based model bring to the problem of cyber attack prediction for IoT devices. By working together, these algorithms improve the handling of multi-class situations, feature optimization, and decision clarity. Future studies should aim to develop and improve this model to increase its usefulness and the security of IoT systems against cyber threats.

There is scepticism about the added complexity introduced by employing many classifiers in an ensemble model. As time has progressed, however, processing units like mobile devices have become progressively quicker, and memory resources have become increasingly inexpensive; this has led to the possibility of a wide range of algorithms, including ensemble approaches, being used for fog computing. Efficient resource allocation in fog computing is another area of study. Moreover, studies have developed fog system designs that may use ensemble learning without significantly increasing latency. It is argued that the design and efficient resource allocation method explored in this article may be used to implement the stacking strategy. Since missing a cyberattack is associated with a high cost, the discovery that stacking can beat single classifiers for counterattack detection in IoT Smart city applications has significant value despite modest increases in complexity.

Conclusions

To forecast cyber-attacks in IoT systems, the authors provide a unique multi-class support vector machine (SVM) and improved CHAID decision tree-based model. In addition to enhanced prediction accuracy, this model boasts enhanced interpretability, scalability, efficiency, and optimized feature selection. The proposed model gains the highest accuracy level (98.28%). It is maximum accuracy achieved in both the training and testing phases. Using multi-class support vector machines (SVMs) and improved CHAID decision tree algorithms, various attack classes may be handled efficiently and with complete clarity. The model incorporates feature selection approaches to zero in on the most important aspects for cyber attack prediction, lowering the dimensionality and increasing the efficiency with which the model operates. By improving interpretability, the CHAID decision tree method gives security analysts a deeper understanding of attack vectors and weak spots. A potential topic of study is the combination of Multi-Class SVM and Optimized CHAID decision tree for detecting cyber attacks. Combining the best features of these two algorithms allows for the creation more effective and trustworthy systems for detecting cyber attacks. The study found the following additional results:

- Accuracy and recall in detecting cyber attacks can be enhanced by combining Multi-Class SVM with an Optimized CHAID decision tree.
- Multi-Class SVM may be used as a first-stage classifier in integrating these two techniques, or the two can be used simultaneously.
- Organizational requirements should guide the selection of an integration strategy.

Improving the accuracy and reliability of cyber attack detection systems by integrating Multi-Class SVM and Optimized CHAID decision tree is a promising field of research.

Due to its efficiency and scalability, the model may be used for real-time prediction in massive IoT rollouts. Its computing performance allows for rapid forecasts and faster cyber threat detection and mitigation. Our model has potential, but it is not without caveats. Training data is crucial to the model's success; thus, it's important to use a wide variety of data that accurately represents the target domain. Investigating ensemble approaches and incorporating additional machine learning techniques in future studies might improve the resilience and accuracy of the model.

Our unique multi-class support vector machine (SVM) and improved CHAID decision tree-based model both add to the development of cyber attack prediction in IoT systems. It's a helpful resource for countering online dangers and protecting sensitive data. More work will improve and broaden the model, leading to stronger defences for Internet of Things devices. Thus, a CHAID-based paradigm is proposed for predicting multi-stage cyber threat detection for IoT communication. In this research, the authors investigate whether the proposed CHAID method can be used to detect cyberattacks in IoT-based Smart city applications. Through testing with the most up-to-date IoT attack database, we have found that this technique, mainly stacking, outperforms individual models in distinguishing malicious from benign data. Using a feature selection method informed by information gain, the authors can zero in on the data that will impact the model's performance most. Additionally, our proposed technique with the SVM technique leads to higher performance than the single or other models employed in recent publications in categorizing attack types in terms of accuracy, precision, recall, and F1-score metrics. In the future, the authors want to investigate deep learning strategies that might significantly improve the effectiveness of IoT threat detection.

Finally, as automated systems and Smart cities gain popularity, they will also face increased cyber attacks. Suppose citizens are denied access to or otherwise have their privacy invaded within an automated system. In that case, it can have severe consequences for them as individuals and be expensive for the government to fix. System failures in managing emergencies (such as accidents and fires) can potentially endanger people's health. Our findings that stacking classifiers can improve the detection of cyberattacks in smart city networks have ramifications beyond technological contributions, including economic and societal ones.

More information will be gained in this regard from studies to be conducted in the future. To better identify cyber-attacks, new machine learning algorithms may be created. Because they will be customized to the unique traits of cyber assaults, these algorithms may be more accurate and trustworthy than their predecessors. Cyber attack detection systems may be more effective using additional data sources like network traffic data and system logs. This information can be utilized to spot trends in cyber assaults that aren't picked up by currently available databases. It is possible to build automated reaction systems responding to cyber threats. The authors may use these technologies to quarantine compromised machines, stave off harmful traffic, and roll back to a prior configuration.

Acknowledgements
The authors thank Princess Nourah bint Abdulrahman University Researchers Supporting Project number (PNURSP2023R410), Princess Nourah bint Abdulrahman University, Riyadh, Saudi Arabia.

Authors' contributions

UKL & S.D. were responsible for Validation, Software, Data Curation, and Writing - Original Draft. N.F. & S.S. was responsible for Conceptualization, Writing - Original Drafts. MA & NA was responsible for Writing - Original Draft, Visualization. NF & NA were responsible for Writing - Review & Editing. SD & MA were responsible for Formal Analysis. A.K. was responsible for Writing - Original Draft, Resources, and Supervision. The author(s) read and approved the final manuscript.

Funding
The funding of this work was provided by Princess Nourah bint Abdulrahman University Researchers Supporting Project number (PNURSP2023R410), Princess Nourah bint Abdulrahman University, Riyadh, Saudi Arabia.

Availability of data and materials

Publicly available datasets were analyzed in this study.

Declarations

Ethics approval and consent to participate
Not applicable.

Consent for publication
Not applicable.

Competing interests
The authors declare no competing interests.

Author details
[1]Department of Computer Science and Engineering, Amity University Haryana, Gurugram, India. [2]Department of Computer Science and Engineering, Chandigarh University, Mohali, Punjab 1404133, India. [3]Department of Computer Engineering and Applications, GLA University, Mathura (UP)-281406, India. [4]Department of Information Systems, College of Computer and Information Sciences, Princess Nourah Bint Abdulrahman University, P.O. Box 84428, 11671 Riyadh, Saudi Arabia.

Received: 12 June 2023 Accepted: 10 September 2023
Published online: 29 September 2023

References
1. Abdullahi M, Baashar Y, Alhussian H, Alwadain A, Aziz N, Capretz LF, Abdulkadir SJ (2022) Detecting cybersecurity attacks in internet of things using artificial intelligence methods: a systematic literature review. Electronics 11(2):198
2. Chukwudi AE, Udoka E, Charles E (2017) Game theory basics and its application in cyber security. Adv Wireless Commun Net 3(4):45–49
3. Abu Al-Haija Q, Krichen M, Abu Elhaija W (2022) Machine-learning-based darknet traffic detection system for IoT applications. Electronics 11(4):556
4. Lombardi M, Pascale F, Santaniello D (2022) Two-step algorithm to detect cyber-attack over the can-bus: a preliminary case study in connected vehicles. ASCE-ASME J Risk and Uncert in Engrg Sys Part B Mech Engrg 8(3):031105
5. Rawat R, Mahor V, Garg B, Chouhan M, Pachlasiya K, Telang S (2022) Modeling of cyber threat analysis and vulnerability in IoT-based healthcare systems during COVID. In Lessons from COVID-19. Academic Press, pp. 405–425
6. Wang X, Gong X, Yu L, Liu J (2021) MAAC: Novel alert correlation method to detect multi-step attack. In 2021 IEEE 20th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom). IEEE, pp. 726–733
7. Kimani K, Oduol V, Langat K (2019) Cyber security challenges for IoT-based smart grid networks. Int J Crit Infrastruct Prot 25:36–49
8. Pacheco J, Hariri S (2016) IoT security framework for smart cyber infrastructures. In 2016 IEEE 1st International workshops on Foundations and Applications of self* systems (fas* w). IEEE, pp. 242–247
9. Dalal S, Manoharan P, Lilhore UK, Seth B, Simaiya S, Hamdi M, Raahemifar K (2023) Extremely boosted neural network for more accurate multi-stage Cyber attack prediction in cloud computing environment. J Cloud Computing 12(1):1–22
10. Sontowski S, Gupta M, Chukkapalli SSL, Abdelsalam M, Mittal S, Joshi A, Sandhu R (2020) Cyber attacks on smart farming infrastructure. In 2020 IEEE 6th International Conference on Collaboration and Internet Computing (CIC). IEEE, pp. 135-143
11. Dalal S, Poongodi M, Lilhore UK, Dahan F, Vaiyapuri T, Keshta I, Aldossary SM, Mahmoud A, Simaiya S (2023) Optimized LightGBM model for security and privacy issues in cyber-physical systems. Trans Emerging Telecommun Technol 25:e4771
12. Tran MQ, Elsisi M, Liu MK, Vu VQ, Mahmoud K, Darwish MM, Abdelaziz AY, Lehtonen M (2022) Reliable deep learning and iot-based monitoring system for secure computer numerical control machines against cyber-attacks with experimental verification. IEEE Access 10:23186–23197
13. ÖZALP AN, ALBAYRAK Z, ÇAKMAK M, ÖZDOĞAN E (2022) Layer-based examination of cyber-attacks in IoT. In 2022 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA). IEEE, pp. 1–10
14. Shahin M, Chen FF, Hosseinzadeh A, Bouzary H, Rashidifar R (2022) A deep hybrid learning model for detecting cyber attacks in industrial IoT devices. The Int J Adv Manuf Technol 123(5):1973–1983
15. Yazdinejad A, Kazemi M, Parizi RM, Dehghantanha A, Karimipour H (2023) An ensemble deep learning model for cyber threat hunting in industrial internet of things. Digit Commun Networks 9(1):101–110
16. Ismail S, Reza H (2022) Evaluation of Naïve Bayesian Algorithms for Cyber-Attacks Detection in Wireless Sensor Networks. In 2022 IEEE World AI IoT Congress (AIIoT). IEEE, pp. 283–289
17. Ahmad T, Zhang D (2021) Using the Internet of things in smart energy systems and networks. Sustain Cities Soc 68:102783
18. Le K-H, Nguyen M-H, Tran T-D, Tran N-D (2022) IMIDS: An Smart intrusion detection system against cyber threats in IoT. Electronics 11(4):524
19. Semwal P, Handa A (2022) "Cyber-attack detection in cyber-physical systems using supervised machine learning." In Handbook of Big Data Analytics and Forensics. Cham, Springer, pp 131–140
20. Raimundo RJ, Rosário AT (2022) Cybersecurity in the internet of things in industrial management. Appl Sci 12(3):1598
21. Chakrabarty S, Engels DW. "A secure IoT architecture for smart cities." In 2016 13th IEEE annual consumer communications & networking conference (CCNC), pp. 812–813. IEEE, 2016.
22. Koroniotis N, Moustafa N, Schiliro F, Gauravaram P, Janicke H (2020) A holistic review of cybersecurity and reliability perspectives in smart airports. IEEE Access 8:209802–209834
23. Ansere JA, Han G, Wang H, Choi C, Wu C (2019) A reliable energy efficient dynamic spectrum sensing for cognitive radio IoT networks. IEEE Internet Things J 6(4):6748–6759
24. Onyema EM, Dalal S, Romero CAT, Seth B, Young P, Wajid MA (2022) Design of intrusion detection system based on cyborg intelligence for security of cloud network traffic of smart cities. J Cloud Computing 11(1):1–20
25. Dalal S, Seth B, Jaglan V, Surbhi MM, Dahiya N, Rani U, Le DN, Hu YC (2022) An adaptive traffic routing approach toward load balancing and congestion control in Cloud–MANET ad hoc networks. Soft Computing 26(11):5377–5388
26. Krundyshev, Vasiliy, and Maxim Kalinin. "Hybrid neural network framework for detection of cyber attacks at smart infrastructures." In Proceedings of the 12th International Conference on Security of Information and Networks, pp. 1–7. 2019.
27. Saheed YK, Arowolo MO (2021) Efficient cyber attack detection on the internet of medical things-smart environment based on deep recurrent neural network and machine learning algorithms. IEEE Access 9:161546–161554
28. Seth B, Dalal S, Jaglan V, Le D-N, Mohan S, Srivastava G (2022) Integrating encryption techniques for secure data storage in the cloud. Trans Emerging Telecommun Technol 33(4):e4108
29. Shafiq M, Tian Z, Sun Y, Xiaojiang Du, Guizani M (2020) Selection of effective machine learning algorithm and Bot-IoT attacks traffic identification for internet of things in smart city. Futur Gener Comput Syst 107:433–442
30. Masud RM (2019) IoT-based electric vehicle state estimation and control algorithms under cyber attacks. IEEE Internet Things J 7(2):874–881
31. Seth B, Dalal S, Le DN, Jaglan V, Dahiya N, Agrawal A, Sharma MM, Prakash D, Verma KD (2021) Secure cloud data storage system using hybrid paillier–blowfish algorithm. Computers Materials Continua 67:1
32. Gochhayat SP, Lal C, Sharma L, Sharma DP, Gupta D, Saucedo JAM, Kose U (2020) Reliable and secure data transfer in IoT networks. Wireless Net 26(8):5689–5702
33. Liu PY, Wu KR, Liang JM, Chen JJ, Tseng YC. "Energy-efficient uplink scheduling for ultra-reliable communications in NB-IoT networks." In 2018 IEEE 29th Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC), pp. 1–5. IEEE, 2018.
34. Ghosh S, Dagiuklas T, Iqbal M, Wang X (2022) A cognitive routing framework for reliable communication in iot for industry 5.0. IEEE Trans Industr Inf 18(8):5446–5457
35. Rathore MS, Poongodi M, Saurabh P, Lilhore UK, Bourouis S, Alhakami W, Osamor J, Hamdi M (2022) A novel trust-based security and privacy model for internet of vehicles using encryption and steganography. Comput Electr Engi 102:108205
36. Conti M, Kaliyar P, Lal C. "REMI: a reliable and secure multicast routing protocol for IoT networks." In Proceedings of the 12th International Conference on Availability, Reliability and Security, pp. 1–8. 2017.

37. Maddikunta PKR, Pham QB, Prabadevi B, Deepa N, Dev K, Gadekallu TR, Ruby R, Liyanage M (2022) Industry 5.0: A survey on enabling technologies and potential applications. J Industrial Inform Integ 26:100257
38. Khan WU, Ihsan A, Nguyen TN, Ali Z, Javed MA (2022) NOMA-enabled backscatter communications for green transportation in automotive-industry 5.0. IEEE Transact Industrial Inform 18(11):7862–7874
39. Hassan A, Prasad D, Khurana M, Lilhore UK, Simaiya S (2021) Integration of internet of things (IoT) in health care industry: an overview of benefits, challenges, and applications. Data Sci Innovations Smart Syst 30:165–180
40. Liu Y, Wu H, Rezaee K, Khosravi MR, Khalaf OI, Khan AA, Ramesh D, Qi L (2022) Interaction-enhanced and time-aware graph convolutional network for successive point-of-interest recommendation in traveling enterprises. IEEE Transact Industrial Inform 19(1):635–643
41. Qi L, Liu Y, Zhang Y, Xiaolong Xu, Bilal M, Song H (2022) Privacy-aware point-of-interest category recommendation in internet of things. IEEE Internet Things J 9(21):21398–21408
42. Liu Y, Li D, Wan S, Wang F, Dou W, Xiaolong Xu, Li S, Ma R, Qi L (2022) A long short-term memory-based model for greenhouse climate prediction. Int J Intell Syst 37(1):135–151
43. Abu Al-Haija Q, Al-Fayoumi M. "An intelligent identification and classification system for malicious uniform resource locators (URLs)." Neural Computing and Applications (2023): 1–17.
44. Al-Haija QA, McCurry CD, Zein-Sabatto S. "Intelligent self-reliant cyber-attacks detection and classification system for IoT communication using deep convolutional neural network." Selected Papers from the 12th International Networking Conference: INC 2020 12. Springer International Publishing, 2021.
45. Abu Al-Haija Q, Badawi AA, Bojja GR (2022) Boost-defence for resilient IoT networks: a head-to-toe approach. Expert Syst 39(10):e12934
46. Abu Al-Haija Q, Alohaly M, Odeh A (2023) A lightweight double-stage scheme to identify malicious DNS over HTTPS traffic using a hybrid learning approach. Sensors 23(7):3489
47. Al-Haija QA (2023) Cost-effective detection system of cross-site scripting attacks using hybrid learning approach. Results Eng 19:101266

Publisher's Note

Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.