Journal of Theoretical and Applied Information Technology
31st July 2024. Vol.102. No. 14

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

A NEW TECHNIQUE FOR DETECTING EMAIL SPAM RISKS USING LSTM- PARTICLE SWARM OPTIMIZATION ALGORITHMS

TAYSEER ALKHDOUR [1], RANA ALRAWASHDEH [2], MOHAMMED ALMAIAH [3], ROMEL AL-ALI [4] SAID SALLOUM [5] AND THEYAZAN H.H ALDAHYANI[6]

[1] College of Computer Science and Information Technology, King Faisal University, Al-Ahsa 31982, Saudi Arabia
[2]King Fahd of Petroleum and Mineral, Faculty of computer science and information system, Dhahran 31261, Saudi Arabia
[3] King Abdullah the II IT School, the University of Jordan, Amman 11942, Jordan
[4] Associate Professor, the National Research Center for Giftedness and Creativity, King Faisal University, Saudi Arabia
[5]Health Economic and Financing Group, University of Sharjah, Sharjah, United Arab Emirates
[6] Applied College in Abqaiq, King Faisal University, Al-Ahsa 31982, Saudi Arabia
Corresponding authors: m.almaiah@ju.edu.jo and talkhdour@kfu.edu.sa

ABSTRACT

Unwanted email spam involves sending messages to numerous recipients, typically to market products, services, or scams without the recipient's consent. These messages often contain false information. The goal of identifying email spam is to recognize and filter out undesired communications before they reach recipients' inboxes. Detecting spam emails is crucial for all involved parties, including users, companies, and email service providers. The detection of email spam impacts user satisfaction, security measures, trustworthiness, data security, network performance, cost management, adherence to regulations, reputation maintenance, industry norms, and the global email environment. By identifying and addressing email spam, individuals, businesses, and service providers can benefit from enhanced safety and effectiveness in the email network. The process of identifying email spam extends to email service providers, individuals, businesses, network managers, ISPs, security experts, regulatory bodies, data analysts, law enforcement agencies, cybersecurity entities, and developers of spam filtering software. Through the implementation of spam detection techniques, these entities can mitigate the risks associated with email spam and promote a secure and efficient email environment. In our methodology, we start by importing and preparing the data, followed by translating words into numerical sequences via word encoding. Subsequently, we train an LSTM network with a word embedding layer. We then select optimal solutions using the PSO algorithm and classify data using the trained LSTM network. Our results demonstrate that our approach enhances email spam detection and outperforms previous studies with metrics reaching up to 99.5%. We conclude that identifying email spam is essential for maintaining a smooth and reliable email platform. By detecting spam, users, companies, and email providers can improve user satisfaction, protect against cyber threats, conserve network resources, comply with regulations, and establish credibility with users.

Keywords: *Email spam; Cyber-Risks Cybersecurity attacks; LSTM; PSO; NLP.*

1. INTRODUCTION

Detecting email spam has long been a challenge, particularly with the increasing popularity of email. Spam, defined as unsolicited messages, significantly impacts user experience, security, and network efficiency [1]. Various methods have been developed to address this issue, including rule-based filters, Bayesian filtering, machine learning, heuristics, behavioral analysis, collaborative filtering, and blacklisting [2]. These methods have evolved alongside advancements in machine learning, natural language processing, and AI [3]. However, creating spam detection systems that can adapt to evolving spamming tactics remains an ongoing challenge that necessitates industry collaboration and

continuous research to ensure global email security [4].

While advancements in detecting email spam have been made, significant obstacles persist. Issues such as mistakenly flagging legitimate emails or allowing spam to evade detection remain prevalent. Spammers continually refine their tactics, utilizing techniques such as encryption and psychological manipulation, which necessitate ongoing updates to detection systems. Zero-day attacks, exploiting unknown vulnerabilities, further complicate detection efforts [5]. The complexity of spam detection is compounded by the presence of nuanced meanings and content variability, which can sometimes evade content-based analysis employed by spam filters. Additionally, the resource-intensive nature of processing poses challenges for service providers [6]. Adversarial attacks also pose a threat by manipulating emails to bypass filtering mechanisms, raising privacy concerns associated with email scanning. To enhance spam detection, ongoing research is essential, leveraging a combination of strategies including machine learning, user input, and industry collaboration [7]. These efforts are critical for advancing email security and effectively combating the evolving tactics of spammers.

Email spam involves sending unsolicited emails to a number of recipients without their permission. These emails often include advertisements, scams, fake content, malware or other unwanted material [8]. Spammers get email addresses through methods such, as collecting them from websites buying email lists or using tools to generate addresses [9]. Once they have a list of addresses spammers send out messages in the hope of reaching as people as possible. The content of spam emails varies. Some promote. Services of quality or legality [10]. Others try to trick recipients by pretending to be entities for phishing attacks or to collect information. Spam emails may also have attachments or links that can infect computers with malware or lead to websites [11]. The prevalence of email spam creates problems for users, email services and organizations. It fills up inboxes making it hard to find messages and can decrease productivity [12]. Spam emails also pose security threats, with content that could jeopardize personal information, financial resources or overall online safety. To tackle the issue of email spam, a range of methods and tools have been created, such, as spam filters, blacklists, collaborative filtering, machine learning algorithms and behavioral analysis. These solutions work towards detecting and preventing spam emails to enhance user safety and optimize the email usage experience [13].

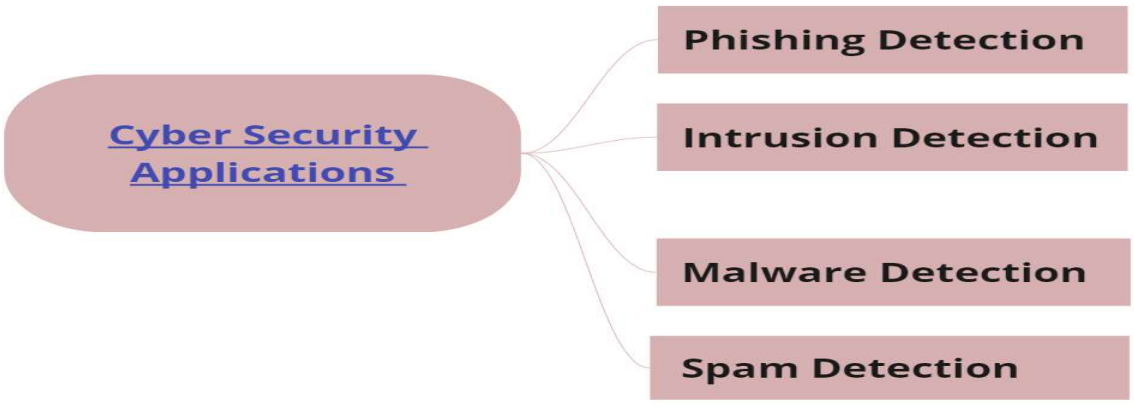

Figure 1: Cyber security Applications

The combination of Particle Swarm Optimization (PSO) and Long Short Term Memory (LSTM), in detecting email spam serves purposes Ray et al., [14]. One primary objective is to improve the accuracy of spam detection by enhancing the precision and dependability of identifying spam thereby reducing positives and false negatives [15]. Additionally, these methods are used to

tackle the complexity of patterns and sequences found in spam emails. By utilizing PSO and LSTM the system can effectively recognize structures and contextual hints allowing for a more comprehensive examination of the diverse patterns and sequences displayed in spam messages [16]. Another crucial goal is to adapt to evolving spam tactics enabling the developed models to adjust and effectively identify spamming strategies used by actors [17]. Furthermore, the utilization of PSO helps optimize efficiency and resource usage in detecting spam. This optimization involves refining detection algorithms adjusting model parameters and selecting features for identification of spam emails. Moreover, a key focus is, on achieving real time detection capabilities to ensure that detection models can quickly process emails in time leading to prompt identification and filtering of unwanted messages before they reach recipients mailboxes [18]. The combination of PSO and LSTM, in detecting email spam not focuses on enhancing accuracy and effectiveness but, on adjusting to the ever changing tactics of spammers all while ensuring prompt detection and filtering [19-22].

Research inquiries concerning the identification of email spam using Particle Swarm Optimization (PSO) and Long Short Term Memory (LSTM) could include; RQ1: Can PSO be effectively utilized to fine tune parameters, in LSTM models for detecting email spam? RQ2: How can the combination of PSO and LSTM be used to tackle patterns and sequences encountered in email spam detection? RQ3: Do PSO and LSTM have the ability to adapt to changing strategies used by spammers and consistently maintain detection effectiveness, over timeframes? The benefits of incorporating PSO and LSTM in identifying email spam are numerous. These include increased precision the ability to handle patterns, flexibility, in adapting to spam tactics, optimal use of resources and the capability for real time detection. PSO tunes LSTM settings to boost accuracy and reduce alarms. The sequential learning feature of LSTM is instrumental, in dissecting patterns found in spam messages. PSOs continuous adjustment of model parameters ensures it stays on top of evolving spam tactics. Efficient resource management is made possible by optimizing feature selection and model parameters with the help of PSO. By combining PSO and LSTM real time detection of spam is achievable safeguarding users from emails and bolstering email security overall.

The importance of detecting email spam is crucial, for safeguarding users securing data saving time and boosting productivity enhancing network efficiency and fostering trust and credibility [23]. It aids in shielding users from content defending data against breaches streamlining time management improving network functionality and nurturing trust [24]. Various stakeholders such as email service providers, businesses, individuals and regulatory entities are affected by the detection of spam emails [25-27]. Its applications encompass integration into email platforms, security tools, filtering systems, fraud prevention mechanisms and adherence, to regulations. In essence the identification of email spam brings about advantages with reaching effects and practical uses [28].

Detecting email spam through the use of natural language processing (NLP). Deep learning involves implementing strategies to boost the effectiveness of spam detection systems [29]. These methods encompass categorizing text, with Convolutional Neural Networks (CNNs) capturing relationships with Recurrent Neural Networks (RNNs) leveraging word embedding's to establish connections employing attention mechanisms to highlight crucial segments utilizing transfer learning with preexisting models combining multiple models for enhanced performance creating features that are relevant through feature engineering and refining models iteratively, with active learning. When these techniques are applied together or individually they significantly enhance the precision and efficiency of email spam detection systems [30]. In our work, the process of identifying email spam involves a blend of Natural Language Processing (NLP) Particle Swarm Optimization (PSO) and Long Short Term Memory (LSTM) methods. It includes preparing data extracting features, with NLP selecting features based on PSO building an LSTM model to recognize patterns and connections training and optimizing using PSO assessing performance, with metrics and detecting spam in time. This holistic method enhances the

precision and effectiveness of spam detection providing users with a filtering system.

The paper is organized in the manner; In Section 2 we mention the existing research, on detecting email spam using email data. Section 3 discusses the research subject and the hypothesis formulated for this study. Our methodology is explained in Section 4 and Section 5 describes the experiments carried out in this study. Finally, Section 6 concludes with a discussion of the results.

2. RELATED WORKS

In a study [31-33] the authors have introduced a new method for filtering spam emails that focuses on the interplay between the information gathered from the context of an email and its specific attributes. They use a network model called PV DM and the TF IDF framework to assign two representation vectors to each message. The final categorization is based on combining the classifications from both vectors. Their experiments clearly show that classifiers trained with the approach achieve results compared to both PV DM and Bow models. Additionally, their research indicates that the method is more robust against variations, in language structure and message coherence. The study [34] divided into two themes; identifying spam and analyzing sentiments, on Twitter through the application of machine learning and deep learning techniques. Spam detection entails the process of spotting and filtering out content, such as fake profiles, advertisements or irrelevant data from social media platforms, like Twitter. The authors use algorithms and strategies leveraging machine learning and deep learning methods to recognize and flag such spam or unwanted content in real time. Conversely sentiment analysis involves grasping and scrutinizing the emotions or viewpoints conveyed in tweets or other textual information. The authors mentioned that their objective is to ascertain whether a tweet conveys positivity, negativity or neutrality. The article could explore machine learning and deep learning methodologies to categorize and evaluate the sentiment of tweets in time.

Another study focused on evaluating and comparing how machine learning techniques work in detecting spam. Spam detection involves recognizing and removing harmful content, such as emails, fake profiles or ads. Machine learning techniques, which are algorithms that can learn from data patterns and make predictions can be used to automate the process of detecting spam [35]. This study may cover machine learning methods like decision trees support vector machines (SVM) naive Bayes or neural networks and assess their efficiency in identifying spam. It might explore how these methods are trained and tested using datasets labeled with both spam and spam samples. The assessment of effectiveness usually includes measuring the performance of machine learning techniques using metrics like accuracy, precision, recall and F1 score. The study may compare the outcomes of methods to determine which approach is more successful at distinguishing spam while minimizing false positives or false negatives. Moreover, the study mention the characteristics or attributes employed by machine learning models to differentiate between spam and non-spam content. These attributes could encompass elements, like keywords, email headers, sender details or linguistic patterns. The research paper in [36] delved into the utilization of machine learning methods, for screening and identifying spam and phishing emails. It tackles the issue of emails encompassing both spam messages and phishing schemes. Various machine learning strategies employed in email screening are discussed in the paper, where algorithms are trained on labeled datasets to categorize and detect spam and phishing emails. It examines how machine learning can be applied in this context by training algorithms on datasets to differentiate between unwanted emails. The paper also assesses established approaches like decision trees support vector machines, Bayes, random forests and neural networks analyzing their effectiveness, in detecting and screening emails. Evaluation metrics and methodologies used to gauge the performance of machine learning techniques are explored, comparing accuracy, precision, recall and F1 score. Additionally, novel or enhanced machine learning techniques might be suggested in the paper to enhance the accuracy and efficiency of email filtering systems. The study conducted by [37], which delved into the identifying and filtering out unwanted spam emails with a focus, on using transformers. These

transformers are network models that can grasp the meaning of words and phrases in context aiding in capturing linguistic patterns and contextual information found in spam emails. Additionally, the paper talks about how these transformers combined with machine learning algorithms like decision trees support vector machines, naive Bayes or random forests to harness their contextual understanding and classification capabilities. The effectiveness of this approach is likely assessed through experiments comparing algorithms paired with bidirectional transformers using metrics such as accuracy, precision, recall or F1 score to gauge performance. In essence the goal of the paper is to showcase how integrating bidirectional transformers, with machine learning classifiers can enhance spam detection systems by boosting accuracy through improved comprehension and recognizing patterns. In a study [38], the researchers focused into the issue of spotting and sifting through spam content, on Twitter. It stresses the importance of identifying spam tweets upon their posting. The paper delves into utilizing machine learning methods like decision trees, support vector machines, naive Bayes or random forests for detecting spam. It explores strategies and algorithms for detection and analyzes the attributes used to differentiate between spam and authentic tweets. The paper assesses the effectiveness of machine learning methods using metrics such as accuracy, precision, recall or F1 score. It also covers the considerations of scalability and efficiency when developing a spam detection system for a large scale platform, like Twitter. In essence the paper aims to showcase how machine learning techniques can effectively detect spam in time on Twitter while shedding light on feature selection, data gathering, and scalability and efficiency aspects of such a system.

Table 1. Review Of The Related Works

Ref	Techniques	Dataset	Accuracy	Limitations
[31]	Random forest Algorithm	Custom collection	95.2%	Without dataset.
[32]	The authors used selection features with modified naïve bayes	They use spam base and spam data	88%	Less accuracy
[33]	They used different algorithms like Bayes net ,NB, SVM	Facebook and twitter dataset	Almost 90% using svm	Limited number of features are used
[34]	Different algorithms like SVM,KNN, additive regression	Real life dataset	96%	The process of changing the spam filter features not reasonable
[35]	ID3 algorithm hidden Markova	Enron dataset	89%	The percentage of loss=11% not good
[36]	CART,REP tree	UCI dataset	95%	Limited number of features
[37]	Deep learning ,pso	UCI dataset	93%	Massive time taken
[38]	ELM,SVM	Enron dataset	94%	More time taken
[39]	SVM,KNN,DT	Health fitness data	93%	Interoperability not evaluated

3. METHODOLOGY

Detecting email spam using NLP, PSO, and LSTM involves employing these methods to

identify and filter emails. NLP analyzes email content to detect indicators of spam or legitimate messages. PSO optimizes parameters within machine learning models or NLP algorithms. LSTM, a type of recurrent neural network, constructs a classifier to recognize patterns in spam emails based on data. The process includes data preparation, feature extraction, model training, parameter optimization using PSO, and assessment testing. This integrated approach aims to establish an effective spam detection mechanism to protect users from malicious email communications. When feeding text into an LSTM network, start by converting text data into numerical sequences. This can be achieved using word encoding, which converts documents into sequences of indices. For optimal results, incorporate a word embedding layer in the network. Word embedding's represent words in a vocabulary with vectors instead of scalar indices. These embedding's capture nuances of words, ensuring that words with similar meanings are represented by similar vectors. The workflow begins by importing and preparing the data. Next, words are converted into numerical sequences through word encoding. Then, an LSTM network is trained with a word embedding layer. Finally, text data can be classified using the trained LSTM network.

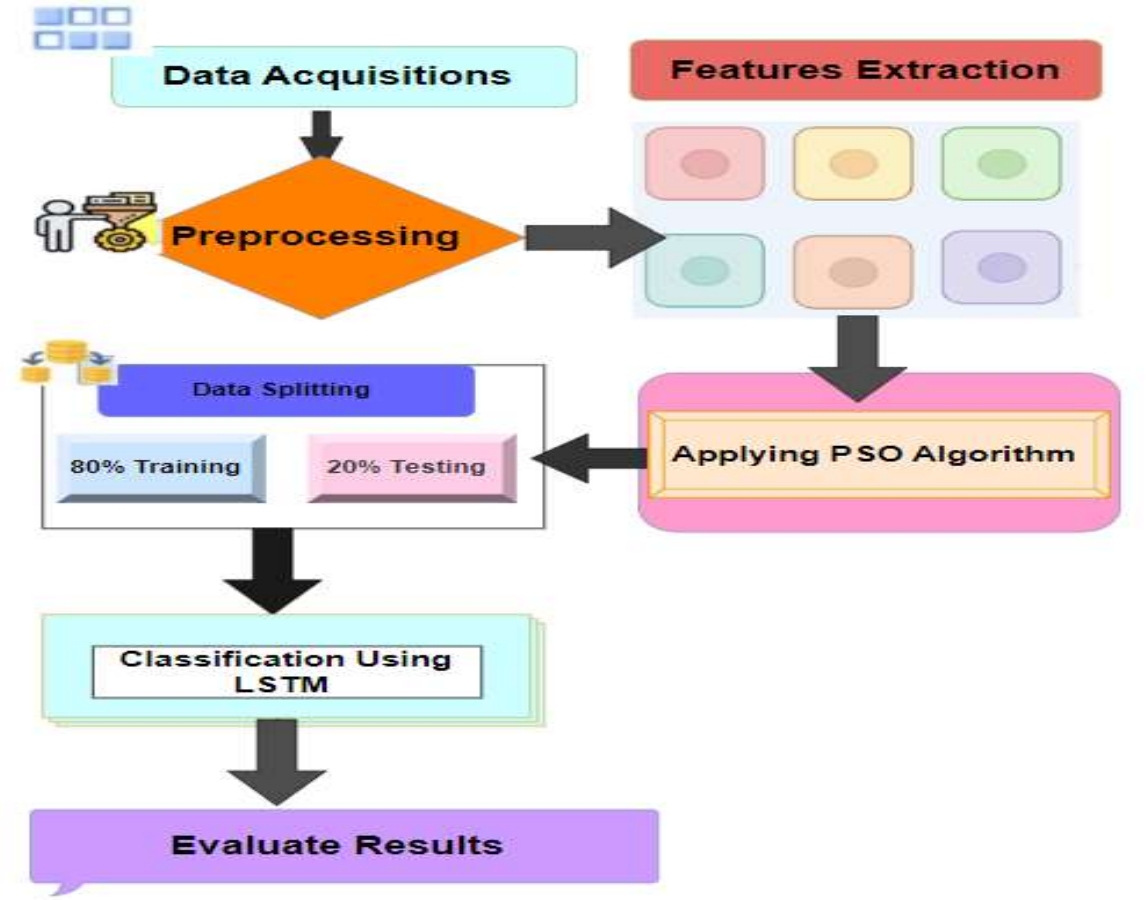

Figure 2: Our Approach Methodology Flowchart

3.1 Data Acquisition

The data are obtained from Kaggle website using this link" https://www.kaggle.com/datasets/yashpaloswal/spamham-email-classification-nlp". It's a set of labeled emails that have been sorted into spam (unsolicited emails) or ham (emails). This dataset

is designed for use, in tasks related to email classification in natural language processing (NLP). There are a total of 5,572 email examples, in the dataset each email being an entry. The data is organized in a format called CSV (Comma Separated Values) where each row represents an email and contains three columns; "email Text"; This column holds the text content of the email including the line, message body and other relevant textual information. "Label"; this column shows whether the email is marked as spam or ham. The "spam" label refers to unsolicited emails while "ham" signifies emails.

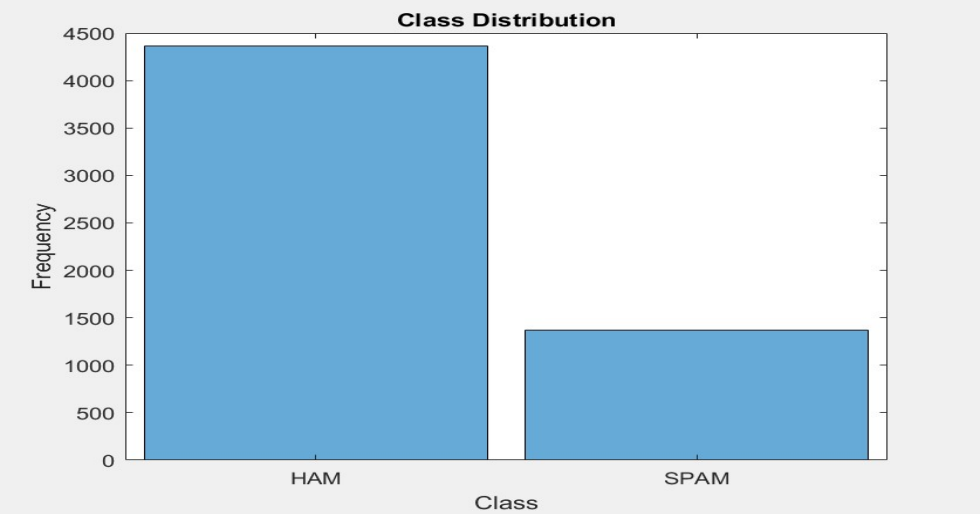

Figure 3: Class Distribution In Email Dataset

3.2 Preprocessing Data and Features Extraction

In this stage we start by tokenization, breaking down a block of text into units known as tokens is a process, in natural language processing (NLP). These tokens can take the form of words, sentences or even sub words depending on the desired level of detail. Tokenization plays a role in NLP activities such, as text analysis, machine learning, information retrieval and language modeling. Then when we talk about "changing the text to lowercase using NLP " it means altering all the letters, in the text to their lowercase versions with methods from Natural Language Processing (NLP).

In NLP processes adjusting text to lowercase is a step. This step aims to standardize the text and make it insensitive to case. By converting the text to lowercase we ensure that words conveying the meaning. With different capitalization are considered as identical units. This aids, in minimizing the size of the vocabulary enhancing the effectiveness of NLP tasks and preventing information redundancy. Next erasing punctuation, in NLP it involves using methods from Natural Language Processing (NLP) to eliminate punctuation marks from the text. In NLP applications punctuation marks like periods, commas, question marks, exclamation points and quotation marks are often seen as noise for analyses or models. By getting rid of punctuation the text can be simplified, noise reduced and the efficiency and accuracy of NLP tasks improved. Removing punctuation is usually a step taken to clean up text data before analysis or modeling. This process is commonly carried out in conjunction, with tokenization, where punctuation marks are either separated into tokens or completely removed. Additionally, we Convert Document into Sequences in NLP involves the task of turning a document or text snippet into a series of numerical or categorical representations. These representations are then utilized as inputs, for Natural Language Processing (NLP) models and algorithms. In the field of NLP textual data must be transformed into either formats since the majority of machine learning and deep learning models function based on numerical information. Through the conversion of a document, into

sequences we make it possible to apply statistical methods to analyze and handle content.

3.3 Optimal Solution Selection using PSO

Particle Swarm Optimization (PSO) is a method, for optimization that draws inspiration from how social organisms like bird's flock or fish school. It has applications in fields, including the use of Natural Language Processing (NLP) for detecting emails. In our work, PSO can help with selecting features and optimizing parameters for NLP models. Feature Selection; in email detection NLP methods are often used to extract features from email content. These features may involve word frequencies, specific keywords or phrases, sentence structures or sentiment analysis scores. PSO can assist in selecting the features from a large pool by defining a fitness function that evaluates how well a feature subset performs. This way PSO can search for the combination of features to enhance email detection accuracy. Then it is used for Parameter Optimization; NLP models for email detection have parameters that require tuning for performance. For instance, in tasks like text classification parameters such, as learning rates, regularization strengths and hidden unit numbers in networks can significantly influence the models efficiency. Particle Swarm Optimization (PSO) can be utilized to explore the parameter space and discover the values that enhance performance metrics, like accuracy, precision, recall or F1 score. By creating a fitness function that assesses the NLP models performance, with parameter settings PSO can continuously adjust the parameters until they reach a state.

Algorithm 1 PSO pseud code

Step1. Initialization
for *eachparticlei* = 1 . . ., *NP* **do**

(a) Initialize the particle's position with a uniformly dis-tribution as Pi (0) U(LB, UB), where LB and UB representthe lower and upper bounds of the search space.
(b) Initialize to its initial position: pbest(i,0)=pi(0) .
(c) Initialize to the minimal value of theswarm: gbest (0) =argminf[pi(0)]
(d) Initialize velocity: Vi U(-|UB-LB|,|UB-LB|) .
end for

Step2. Repeat until termination criteria is met
for *eachparticlei* = 1 . . . , *NP* **do**

(a) Pick random numbers: r1, r2 U(0,1).
(b) Update particle's velocity. See formula (2).
(c) Update particle's position. See formula (3).
if f[pi(t)] > f[pBest(i,t)] **then**

(i) Update the best known position of particlei: pbest(i,t)=pi(t).
end if
if f[pi(t)] > f[gBest(i,t)] **then**

update the swarm's best known position:gbest(i,t)=pi(t)
end if end for
(e)t<-(t+1);
Step3. Output gbest(t) that holds the best found solution.
=0

3.4 Classification using LSTM

LSTM, known as Long Short Term Memory is a type of network (RNN) structure that aims to

overcome the limitations of traditional RNNs in recognizing long term connections, in sequential data [40-43]. LSTMs excel in managing data where relationships and dependencies between elements can span over extended periods. They have found application in natural language processing (NLP) tasks such as language modeling, machine translation, and sentiment analysis and text categorization [44-47]. The standout characteristic of LSTMs lies in their capacity to absorb and preserve information across sequences. This is made possible through a memory cell and a series of gates that manage the information flow. These gates. Including the input gate forget gate and output gate. Govern how information enters, exits and circulates within the memory cell. With the help of the memory cell LSTMs can intelligently [48-51]. Discard information based on context and input data. This unique ability allows them to capture connections and alleviate issues, like gradient vanishing commonly encountered in RNNs [52-55]. In processing data LSTMs operate by applying the gates and updating the state of the memory cell at each time step. At a time point the result produced by an LSTM unit can serve as input, for following LSTM units or act as the output of the LSTM layer. In natural language processing assignments LSTMs are frequently paired with methods like word embedding, attention mechanisms and connected layers, for categorization or prediction purposes. These models are taught using backpropagation through time (BPTT) a version of the backpropagation procedure tailored for recurrent neural networks [56-59]. Using Long Short Term Memory (LSTM) for sorting out email spam is a used method, in natural language processing and deep learning. LSTMs are great at handling sequences of data which makes them ideal for tasks like identifying email spam [60-63]. The general steps involved; Firstly, Data Preparation; Gather a labeled dataset of emails clean up details. Break down the text into individual words or sub words. Secondly, Word Embedding's; Transform the broken down words into vector representations known as word embedding. These embedding's capture meaning relationships. Help the LSTM grasp context better. Thirdly, Padding and Sequence Setup; Ensure that all input sequences have lengths by adding padding to emails or trimming longer ones to a fixed length using special tokens or specific length limits. Fourthly, Model Structure; Construct the LSTM model for spam detection consisting of an embedding layer, one or more layers to understand patterns and a final classification layer with softmax activation. Fifthly, Training; Divide the dataset into training and validation portions then train the LSTM model through descent to minimize a loss function while tuning hyper parameters for optimal results. Finally, Assessment; Evaluate how well your trained LSTM model performs on a test set by measuring metrics such, as accuracy, precision, recall and F1 score.

3.5 Evaluation the Results

Assessing the effectiveness of email spam detection involves analyzing how well the system can distinguish between spam and genuine emails. Various metrics, like accuracy, precision, recall and F1 score are utilized to gauge the models accuracy. To evaluate the model a distinct test dataset is employed to compare its predictions with established labels [64-69]. This evaluation aids in comprehending the systems performance identifying its strengths and weaknesses and guiding enhancements, for an email spam detection setup. In the field of detecting email spam, TP, FP, FN and TN serve as shorthand in a confusion matrix to depict outcomes of the models predictions.TP (True Positive); this indicates the count of spam emails that the model accurately identifies as spam [70-75]. Put simply it signifies when the model correctly flags an email, as spam if it truly is one. FP (False Positive); this represents the tally of ham) emails erroneously labeled as spam by the model [75-80]. It occurs when the model mistakenly categorizes an email as spam. FN (False Negative); this denotes the number of spam emails wrongly categorized as ham) by the model. It transpires when the model fails to recognize a spam email for what it's TN (True Negative); this signifies how many legitimate (ham) emails are correctly identified as, by the model. In essence it depicts instances where the model accurately identifies an email legitimate if it truly is one.

Table 3: Classes Value

Name	Classes value
TP	868
FP	11
FN	4
TN	262

When looking at email spam detection we can explain the values of TP, FP, FN and TN from the confusion matrix provided. True Positive (TP) = 868; this means that the model accurately identified 868 spam emails as spam. These instances show when the model correctly labeled emails, as spam and they were indeed spam. False Positive (FP) = 11; the model classified 11 ham) emails, as spam. These are cases where legitimate emails were wrongly tagged as spam causing alarms or false positives. False Negative (FN) = 4; the model categorized 4 spam emails as ham). These are situations where the model missed labeling spam emails correctly resulting in negatives. True Negative (TN) = 262; this shows that the model correctly identified 262 emails as not being spam. In these cases, the model accurately recognized emails as not falling under the category of spam. The model shows a number of positive classifications (TP) effectively identifying a notable portion of spam emails. The instances of positives (FP) are quite minimal suggesting that the model is effective, in distinguishing emails, from spam. Moreover, the occurrences of negatives (FN) are also limited indicating the models capability to accurately recognize the majority of spam emails. Yet there are some cases where spam emails get mistakenly labeled as legitimate. On the hand the true negatives (TN) show a high rate illustrating that the model accurately identifies a significant portion of legitimate emails as not spam. Then we measure accuracy, sensitivity, and specificity as follow: Accuracy, it measures the number of correctly classified samples/total number of samples. Furthermore, it can be represented according to the following formula. Sensitivity (TPR), it measures the number of truly discovered positive samples / all number of actual positive samples, and it can be represented according to the following formula. Specificity (TNR), it measures the number of correctly detected negative samples/ total number of actual negative samples. It can be represented according to the following formula. Precision is the ratio of identified spam emails, to all emails labeled as spam. It assesses how well the model can prevent mistakenly labeling emails as spam. The F1 score is a metric that combines precision and recall, in a way offering an assessment of the models performance regarding both precision and recall.

Accuracy = (TP + TN) / (TP + TN + FP + FN)

Sensitivity = (TP) / (TP + FN)

Specificity = (TN) / (TN + FP)

Precision = TP / (TP + FP)

F1-score = 2 * (Precision * Recall) / (Precision + Recall)

4. ANALYSIS OF THE RESULTS

In figure 4, the model precision of 98.7% indicates that all emails classified as spam were indeed spam showing its ability to correctly distinguish emails, from spam. A high precision means error in labeling emails as spam. Regarding sensitivity at 99.5% the model accurately identified the majority of spam emails demonstrating its skill in spotting spam without mistakenly flagging legitimate messages. A higher sensitivity suggests a chance of mislabeling spam as legitimate. In terms of specificity with a rate of 95.9% the model

effectively recognized ham) emails as such reducing positives for genuine messages. A higher specificity indicates instances where real emails are marked as spam incorrectly. The accuracy level stands at 98.6% reflecting how well the model predicted both types of emails in the dataset overall. It means that all email classifications were correct based on positives and true negatives. Lastly the F measure, at 99.1% combines precision. Recall into a metric to provide an overall assessment of the models performance. The models performance is evaluated based on a combination of positives and false negatives providing an assessment. A higher F measure signifies an equilibrium, between precision and recall. In general, the findings suggest that the model excels in identifying email spam. It demonstrates precision, sensitivity and specificity indicating errors in classifying spam and non-spam emails. The high accuracy rate indicates that most email predictions are correct. The F measure showcases a rounded performance in considering both precision and recall aspects. These outcomes highlight the models efficacy, in categorizing spam and legitimate emails.

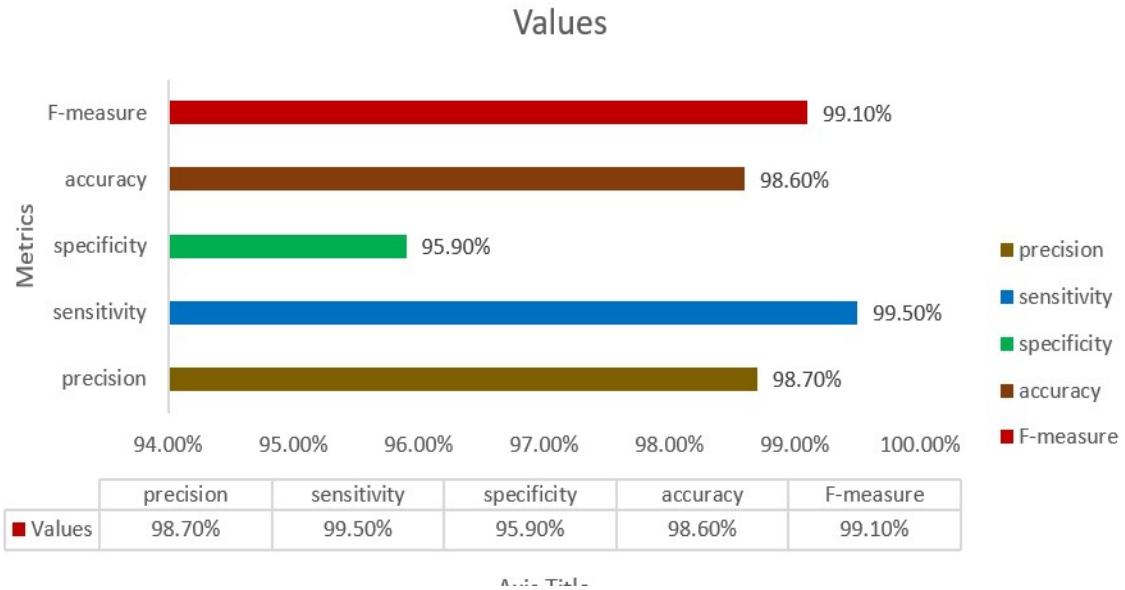

Figure 4: Results Of Our Approach For Spam Email

In figure 5, the models precision of 98.4% shows that when it flags an email, as spam it is 98.4% of the time. This high precision means there are alarms as it can spot spam without mistaking legitimate emails for spam. In terms of sensitivity (recall) the model identifies 95.9% of spam emails correctly. This indicates a rate of missing spam capturing spam without labeling them as real emails. Regarding specificity, the model accurately recognizes 99.5% of ham) emails. This high specificity points to errors where real emails are marked as spam. Overall accuracy stands at 98.6% showing how well the model classifies both types of emails, in the dataset. The F measure at 97.2% combines precision. Recall to offer an assessment considering both false positives and false negatives. A higher F score suggests a mix of accuracy and completeness. In general, the findings show that the model does a job, at spotting email spam. It shows accuracy, selectivity and correctness indicating categorization of both spam and valid emails. While the sensitivity is a bit lower than measures the overall F score remains high signaling a tradeoff between accuracy and completeness. These outcomes imply that the model is efficient, in flagging spam emails while reducing identifications.

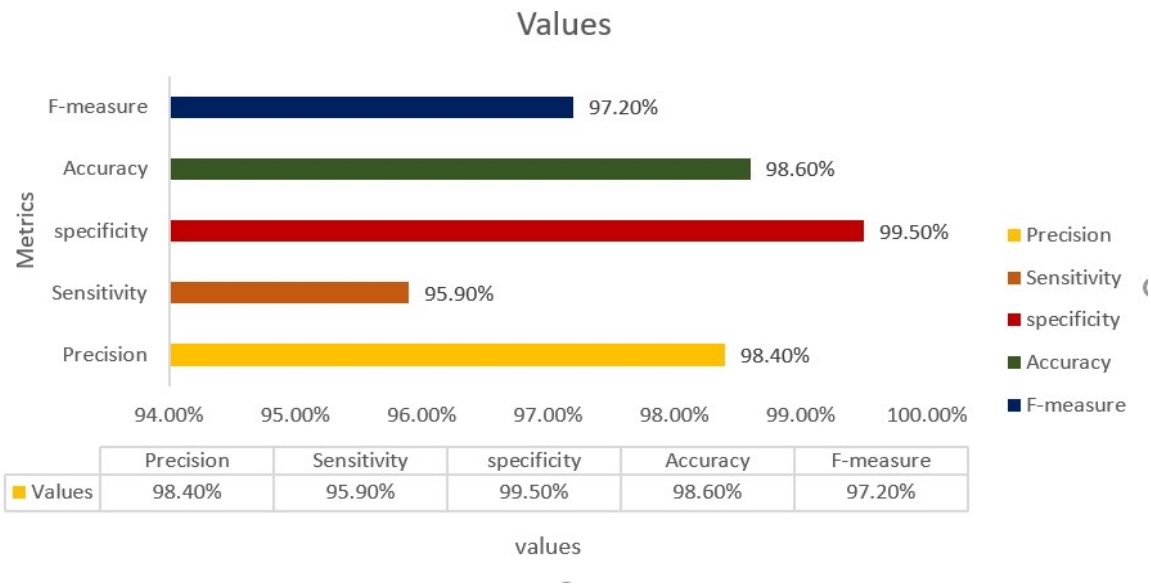

Figure 5: Results Of Our Approach For Ham Email

Table3: Comparing Between Our Work And Previous Work According Some Metrics Averages.

Methods	Avg. precision	Avg. recall	Avg.F1-score
Proposed model (PSO-LSTM)	98.5%	97.7%	98.1%
LSTM model with RMSprop Optimizer.	97%	98%	97%
LSTM model with Adams Optimizer	97.5%	98%	97%
RNN Model with Adams Optimizer.	94%	97.5%	96%
RNN model with RMSprop Optimizer	89.5%	81%	84.5%

In figure 6, The PSO LSTM model consistently performs the best, in terms of precision, recall and F1 score compared to all methods. It excels in detecting spam emails while keeping positives and false negatives to a minimum. Both LSTM models utilizing RMSprop and Adam optimizers' exhibit performance with high average precision, recall and F1 scores. They excel in categorizing spam emails with balanced outcomes. On the hand RNN models employing Adam and RMSprop optimizers show average precision, recall and F1 scores when compared to LSTM models. Their performance diminishes notably in terms of precision and F1 score. In conclusion the PSO LSTM model surpasses methods regarding precision, recall and F1 score for efficient email spam detection. The LSTM models also showcase performance whereas RNN models lag behind in scores. These results indicate that the proposed model along with LSTM based approaches are better suited for spam classification, within this domain.

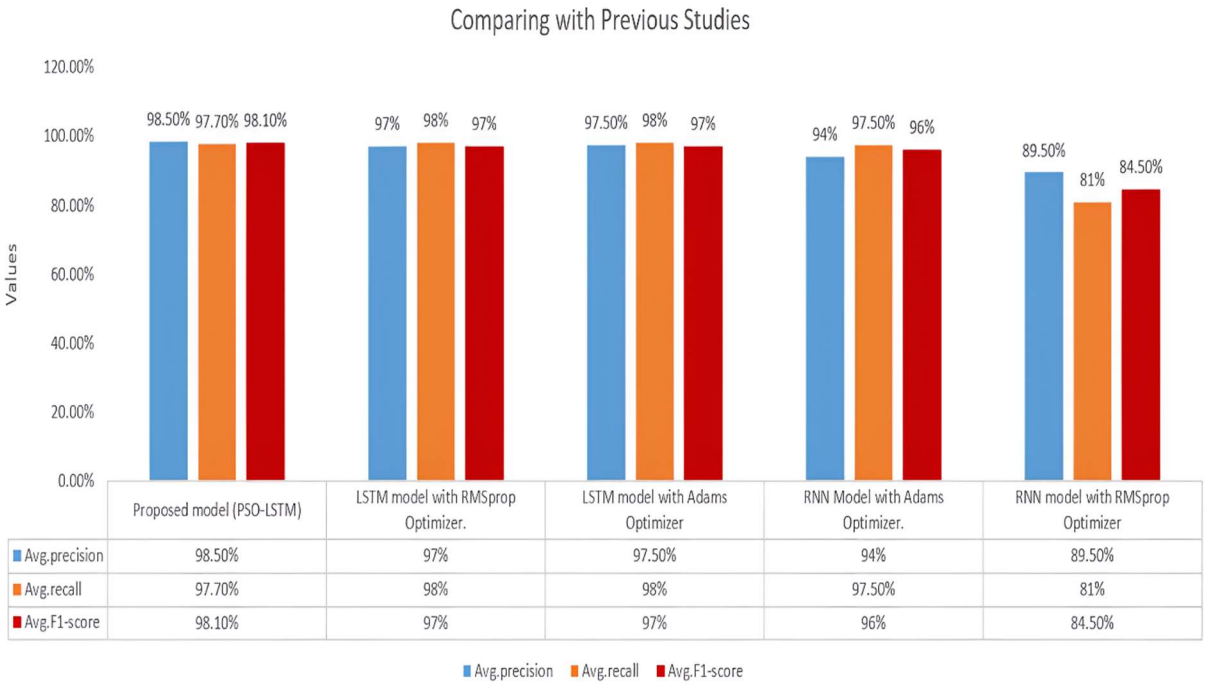

Figure 6. Comparison Analysis WITH PREVIOUS STUDIES.

5. CONCLUSION

This study aims to identify email spam, involving email service providers, individuals, businesses, network managers, ISPs, security experts, regulatory bodies, data analysts, law enforcement agencies, cybersecurity entities, and developers of spam filtering software. Through the adoption of spam detection techniques, these stakeholders can mitigate the risks associated with email spam and promote a secure and effective email environment. In our work, we begin by importing and preparing the data. We then convert words into numerical sequences through word encoding. Subsequently, we train an LSTM network with a word embedding layer. The next step involves selecting suitable solutions using the PSO algorithm, followed by categorizing data using the trained LSTM network. Our results demonstrate that our methodology enhances email spam detection and outperforms previous studies with metrics reaching up to 99.5%. We conclude that the process of identifying email spam is essential for ensuring a smooth and reliable email platform. By detecting spam, users, companies, and email providers can improve user satisfaction, safeguard against cyber threats, conserve network resources, adhere to regulations, and establish credibility with users.

AKNOWLEDGMENT

This work was supported by the Deanship of Scientific Research, Vice Presidency for Graduate Studies and Scientific Research, King Faisal University, Saudi Arabia (Grant No. KFU241248).

REFERENCES

[1] Douzi, S., AlShahwan, F. A., Lemoudden, M., & El Ouahidi, B. (2020). Hybrid email spam detection model using artificial intelligence. *International Journal of Machine Learning and Computing*, *10*(2).

[2] Kaddoura, S., Alfandi, O., & Dahmani, N. (2020, September). A spam email detection mechanism for English language text emails using deep learning approach. In 2020 IEEE 29th international conference on enabling technologies: infrastructure for collaborative enterprises (WETICE) (pp. 193-198). IEEE.

[3] Al Nafea, R., & Almaiah, M. A. (2021, July). Cyber security threats in cloud: Literature review. In *2021 international conference on information technology (ICIT)* (pp. 779-786). IEEE.

[4] Almaiah, M. A., & Al-Khasawneh, A. (2020). Investigating the main determinants of mobile cloud computing adoption in university campus. *Education and Information Technologies*, *25*(4), 3087-3107.

[5] Almaiah, M. A., Al-Rahmi, A., Alturise, F., Hassan, L., Lutfi, A., Alrawad, M., ... & Aldhyani, T. H. (2022). Investigating the effect of perceived security, perceived trust, and information quality on mobile payment usage through near-field communication (NFC) in Saudi Arabia. *Electronics*, *11*(23), 3926.

[6] Almaiah, M. A., Dawahdeh, Z., Almomani, O., Alsaaidah, A., Al-Khasawneh, A., & Khawatreh, S. (2020). A new hybrid text encryption approach over mobile ad hoc network. *Int. J. Electr. Comput. Eng.(IJECE)*, *10*(6), 6461-6471.

[7] Almaiah, M. A., Ali, A., Hajjej, F., Pasha, M. F., & Alohali, M. A. (2022). A lightweight hybrid deep learning privacy preserving model for FC-based industrial internet of medical things. *Sensors*, *22*(6), 2112.

[8] Almaiah, M. A., Hajjej, F., Ali, A., Pasha, M. F., & Almomani, O. (2022). A novel hybrid trustworthy decentralized authentication and data preservation model for digital healthcare IoT based CPS. *Sensors*, *22*(4), 1448.

[9] Al Hwaitat, A. K., Almaiah, M. A., Almomani, O., Al-Zahrani, M., Al-Sayed, R. M., Asaifi, R. M., ... & Alsaaidah, A. (2020). Improved security particle swarm optimization (PSO) algorithm to detect radio jamming attacks in mobile networks. *International Journal of Advanced Computer Science and Applications*, *11*(4).

[10] Adil, M., Almaiah, M. A., Omar Alsayed, A., & Almomani, O. (2020). An anonymous channel categorization scheme of edge nodes to detect jamming attacks in wireless sensor networks. *Sensors*, *20*(8), 2311.

[11] Almaiah, M. A. (2021). A new scheme for detecting malicious attacks in wireless sensor networks based on blockchain technology. In *Artificial intelligence and blockchain for future cybersecurity applications* (pp. 217-234). Cham: Springer International Publishing.

[12] Al Hwaitat, A. K., Almaiah, M. A., Ali, A., Al-Otaibi, S., Shishakly, R., Lutfi, A., & Alrawad, M. (2023). A new blockchain-based authentication framework for secure IoT networks. *Electronics*, *12*(17), 3618.

[13] Ali, A., Almaiah, M. A., Hajjej, F., Pasha, M. F., Fang, O. H., Khan, R., ... & Zakarya, M. (2022). An industrial IoT-based blockchain-enabled secure searchable encryption approach for healthcare systems using neural network. *Sensors*, *22*(2), 572.

[14] Siam, A. I., Almaiah, M. A., Al-Zahrani, A., Elazm, A. A., El Banby, G. M., El-Shafai, W., ... & El-Bahnasawy, N. A. (2021). Secure health monitoring communication systems based on IoT and cloud computing for medical emergency applications. *Computational Intelligence and Neuroscience*, *2021*(1), 8016525.

[15] Alrawad, M., Lutfi, A., Almaiah, M. A., & Elshaer, I. A. (2023). Examining the influence of trust and perceived risk on customers intention to use NFC mobile payment system. *Journal of Open Innovation: Technology, Market, and Complexity*, *9*(2), 100070.

[16] Almaiah, M. A., Yelisetti, S., Arya, L., Babu Christopher, N. K., Kaliappan, K., Vellaisamy, P., ... & Alkdour, T. (2023). A Novel Approach for Improving the Security of IoT–Medical Data Systems Using an Enhanced Dynamic Bayesian Network. *Electronics*, *12*(20), 4316.

[17] Altulaihan, E., Almaiah, M. A., & Aljughaiman, A. (2022). Cybersecurity threats, countermeasures and mitigation techniques on the IoT: Future research directions. *Electronics*, *11*(20), 3330.

[18] Almomani, O., Almaiah, M. A., Alsaaidah, A., Smadi, S., Mohammad, A. H., & Althunibat, A. (2021, July). Machine learning classifiers for network intrusion detection system: comparative study. In *2021 International Conference on Information Technology (ICIT)* (pp. 440-445). IEEE.

[19] Adil, M., Khan, R., Ali, J., Roh, B. H., Ta, Q. T. H., & Almaiah, M. A. (2020). An energy proficient load balancing routing scheme for wireless sensor networks to maximize their lifespan in an operational environment. *IEEE Access*, *8*, 163209-163224.

[20] Almaiah, M. A., Al-Zahrani, A., Almomani, O., & Alhwaitat, A. K. (2021). Classification of cyber security threats on mobile devices and applications. In *Artificial Intelligence and Blockchain for Future Cybersecurity Applications* (pp. 107-123). Cham: Springer International Publishing.

[21] Alamer, M., & Almaiah, M. A. (2021, July). Cybersecurity in Smart City: A systematic

mapping study. In *2021 international conference on information technology (ICIT)* (pp. 719-724). IEEE.

[22] Khan, M. N., Rahman, H. U., Almaiah, M. A., Khan, M. Z., Khan, A., Raza, M., ... & Khan, R. (2020). Improving energy efficiency with content-based adaptive and dynamic scheduling in wireless sensor networks. *IEEE Access*, *8*, 176495-176520.

[23] Bubukayr, M. A. S., & Almaiah, M. A. (2021, July). Cybersecurity concerns in smart-phones and applications: A survey. In *2021 international conference on information technology (ICIT)* (pp. 725-731). IEEE.

[24] Adil, M., Khan, R., Almaiah, M. A., Binsawad, M., Ali, J., Al Saaidah, A., & Ta, Q. T. H. (2020). An efficient load balancing scheme of energy gauge nodes to maximize the lifespan of constraint oriented networks. *IEEE Access*, *8*, 148510-148527.

[25] Adil, M., Khan, R., Almaiah, M. A., Al-Zahrani, M., Zakarya, M., Amjad, M. S., & Ahmed, R. (2020). MAC-AODV based mutual authentication scheme for constraint oriented networks. *IEEE Access*, *8*, 44459-44469.

[26] Albalawi, A. M., & Almaiah, M. A. (2022). Assessing and reviewing of cyber-security threats, attacks, mitigation techniques in IoT environment. *J. Theor. Appl. Inf. Technol*, *100*, 2988-3011.

[27] Aldhyani, T. H., Khan, M. A., Almaiah, M. A., Alnazzawi, N., Hwaitat, A. K. A., Elhag, A., ... & Alshebami, A. S. (2023). A secure internet of medical things framework for breast cancer detection in sustainable smart cities. *Electronics*, *12*(4), 858.

[28] AlMedires, M., & AlMaiah, M. (2021, July). Cybersecurity in industrial control system (ICS). In *2021 International Conference on Information Technology (ICIT)* (pp. 640-647). IEEE.

[29] Almudaires, F., & Almaiah, M. (2021, July). Data an overview of cybersecurity threats on credit card companies and credit card risk mitigation. In *2021 International Conference on Information Technology (ICIT)* (pp. 732-738). IEEE.

[30] AlSalem, T. S., Almaiah, M. A., & Lutfi, A. (2023). Cybersecurity Risk Analysis in the IoT: A Systematic Review. *Electronics*, *12*(18), 3958.

[31] Alrawad, M., Lutfi, A., Almaiah, M. A., Alsyouf, A., Arafa, H. M., Soliman, Y., & Elshaer, I. A. (2023). A Novel Framework of Public Risk Assessment Using an Integrated Approach Based on AHP and Psychometric Paradigm. *Sustainability*, *15*(13), 9965.

[32] Altulaihan, E., Almaiah, M. A., & Aljughaiman, A. (2024). Anomaly Detection IDS for Detecting DoS Attacks in IoT Networks Based on Machine Learning Algorithms. *Sensors*, *24*(2), 713.

[33] Ali, A., Pasha, M. F., Fang, O. H., Khan, R., Almaiah, M. A., & K. Al Hwaitat, A. (2022). Big data based smart blockchain for information retrieval in privacy-preserving healthcare system. In *Big Data Intelligence for Smart Applications* (pp. 279-296). Cham: Springer International Publishing.

[34] Almaiah, M. A. (2020). An Efficient Smart Weighted and Neighborhood-enabled Load Balancing Scheme for Constraint Oriented Networks. *International Journal of Advanced Computer Science and Applications*, *11*(12).

[35] DAWAHDEH, Z. E., ALMAIAH, M. A., ALKHDOUR, T., LUTFI, A., ALDHYANI, T. H., & BSOUL, Q. (2024). A NEW MODIFIED GRAYSCALE IMAGE ENCRYPTION TECHNIQUE USING ELLIPTIC CURVE CRYPTOSYSTEM. *Journal of Theoretical and Applied Information Technology*, *102*(7).

[36] Vijayalakshmi, K., Al-Otaibi, S., Arya, L., Almaiah, M. A., Anithaashri, T. P., Karthik, S. S., & Shishakly, R. (2023). Smart Agricultural–Industrial Crop-Monitoring System Using Unmanned Aerial Vehicle–Internet of Things Classification Techniques. *Sustainability*, *15*(14), 11242.

[37] Almaiah, M. A., & Alkdour, T. (2023). Securing Fog Computing Through Consortium Blockchain Integration: The Proof of Enhanced Concept (PoEC) Approach. In *Recent Advancements in Multimedia Data Processing and Security: Issues, Challenges, and Techniques* (pp. 107-140). IGI Global.

[38] Alkhdour, T. A. Y. S. E. E. R., Almaiah, M. A., Ali, A. I. T. I. Z. A. Z., Lutfi, A. B. D. A. L. W. A. L. I., Alrawad, M. A. H. M. A. O. D., & Tin, T. T. (2024). Revolutionizing Healthcare: Unleashing Blockchain Brilliance Through Fuzzy Logic Authentication. *Journal Of Theoretical And Applied Information Technology*, *102*(4).

[39] ALMAIAH, M. A., ALI, A., SHISHAKLY, R., ALKHDOUR, T., LUTFI, A., & ALRAWAD, M. (2024). BUILDING TRUST IN IOT: LEVERAGING CONSORTIUM BLOCKCHAIN FOR SECURE COMMUNICATIONS. *Journal of Theoretical and Applied Information Technology*, *102*(3).

[40] Almomani, O., Almaiah, M. A., Madi, M., Alsaaidah, A., Almomani, M. A., & Smadi, S. (2023, October). Reconnaissance attack detection via boosting machine learning classifiers. In *AIP Conference Proceedings* (Vol. 2979, No. 1). AIP Publishing.

[41] Alkdour, T., Almaiah, M. A., Shishakly, R., Lutfi, A., & Alrawad, M. (2023). Exploring the Success Factors of Smart City Adoption via Structural Equation Modeling. *Sustainability*, *15*(22), 15915.

[42] ALMAIAH, M. A., ALI, A., SHISHAKLY, R., ALKHDOUR, T., LUTFI, A., & ALRAWAD, M. (2024). A NOVEL FEDERATED-LEARNING BASED ADVERSARIAL FRAMEWORK FOR AUDIO-VISUAL SPEECH ENHANCEMENT. *Journal of Theoretical and Applied Information Technology*, *102*(4).

[43] ALMAIAH, M. A., ALI, A., TIN, T. T., ALKHDOUR, T., LUTFI, A., & ALRAWAD, M. (2024). UNLOCKING USER PRIVACY: A PRIVACY-FOCUSED CRYPTOCURRENCIES FRAMEWORK FOR CONCEALING TRANSACTIONS USING ZERO-KNOWLEDGE PROOFS (ZKPS). *Journal of Theoretical and Applied Information Technology*, *102*(8).

[44] Mohamed, M. A., Shawai, Y. G., Almaiah, M. A., Derahman, M. N., Lutfi, A., & Bakar, K. A. A. (2024). Challenges in data representation for efficient execution of encryption operation. *Bulletin of Electrical Engineering and Informatics*, *13*(2), 1207-1216.

[45] Ahmad, W., Almaiah, M. A., Ali, A., & Al-Shareeda, M. A. (2024, April). Deep Learning Based Network intrusion detection for unmanned aerial vehicle (UAV). In *2024 7th World Conference on Computing and Communication Technologies (WCCCT)* (pp. 31-36). IEEE.

[46] ALKHDOUR, T., ALI, A., ALMAIAH, M., TIN, T. T., AL-SHAREEDA, M. A., ALALI, R., ... & LUTFI, A. (2024). TRANSFORMING HEALTHCARE WITH FEDERATED LEARNING: SECURING FOG SYSTEMS FOR THE NEXT GENERATION. *Journal of Theoretical and Applied Information Technology*, *102*(9).

[47] ALTARAWNEH, K., OSHOUSH, A., ALTARAWNI, I., ALMAIAH, M. A., ALKDOUR, T., LUTFI, A., ... & SHEHAB, R. (2024). VALIDATION OF SECURE E-VOTING SYSTEM BASED BLOCKCHAIN IMMUTABILITY: THE JORDANIAN PARLIAMENTARY ELECTIONS. *Journal of Theoretical and Applied Information Technology*, *102*(6).

[48] ALTARAWNEH, K., ALTARAWNI, I., ALMAIAH, M., HAMMAD, M., ALKHDOUR, T., ALALI, R., & LUTFI, A. (2024). A HYBRID MODEL OF RSA AND NTRU FOR SECURING OF CLOUD COMPUTING. *Journal of Theoretical and Applied Information Technology*, *102*(7).

[49] ALKHDOUR, T., ALMAIAH, M., ALMUWAIL, K. I., AL-SHAREEDA, M. A., ALDAHYANI, T., & ALRAWASHDEH, R. (2024). OVERVIEW OF CYBERSECURITY RISK ASSESSMENT FOR MEDICAL INFORMATION SYSTEMS. *Journal of Theoretical and Applied Information Technology*, *102*(7).

[50] Al-Na'amneh, Q., Nasayreh, A. N., Al Mamlook, R., Gharaibeh, H., Alsheyab, A. M., & Almaiah, M. (2024). Improving Memory Malware Detection in Machine Learning With Random Forest-Based Feature Selection. In *Risk Assessment and Countermeasures for Cybersecurity* (pp. 96-114). IGI Global.

[51] Kontsewaya, Y., Antonov, E., & Artamonov, A. (2021). Evaluating the effectiveness of machine learning methods for spam detection. Procedia Computer Science, 190, 479-486.

[52] Gangavarapu, T., Jaidhar, C. D., & Chanduka, B. (2020). Applicability of machine learning in spam and phishing email filtering: review and approaches. Artificial Intelligence Review, 53(7), 5019-5081.

[53] Guo, Y., Mustafaoglu, Z., & Koundal, D. (2023). Spam detection using bidirectional transformers and machine learning classifier algorithms. Journal of Computational and Cognitive Engineering, 2(1), 5-9.

[54] Sun, N., Lin, G., Qiu, J., & Rimba, P. (2022). Near real-time twitter spam detection with

machine learning techniques. International Journal of Computers and Applications, 44(4), 338-348.

[55] Mohsin, A. H., Zaidan, A. A., Zaidan, B. B., Mohammed, K. I., Albahri, O. S., Albahri, A. S., & Alsalem, M. A. (2021). PSO–Blockchain-based image steganography: towards a new method to secure updating and sharing COVID-19 data in decentralised hospitals intelligence architecture. *Multimedia tools and applications*, *80*, 14137-14161.

[56] Ray, S., Mishra, K. N., & Dutta, S. (2022). Detection and prevention of DDoS attacks on M-healthcare sensitive data: a novel approach. *International Journal of Information Technology*, *14*(3), 1333-1341.

[57] Trab, S., Bajic, E., Zouinkhi, A., Abdelkrim, M. N., & Chekir, H. (2018). RFID IoT-enabled warehouse for safety management using product class-based storage and potential fields methods. *International Journal of Embedded Systems*, *10*(1), 71-88.

[58] Anirudh, M., Thileeban, S. A., & Nallathambi, D. J. (2017, January). Use of honeypots for mitigating DoS attacks targeted on IoT networks. In *2017 International conference on computer, communication and signal processing (ICCCSP)* (pp. 1-4). IEEE.

[59] Lee, S. H., Shiue, Y. L., Cheng, C. H., Li, Y. H., & Huang, Y. F. (2022). Detection and prevention of DDoS attacks on the IoT. *Applied Sciences*, *12*(23), 12407.

[60] Alahmadi, A. A., Aljabri, M., Alhaidari, F., Alharthi, D. J., Rayani, G. E., Marghalani, L. A., ... & Bajandouh, S. A. (2023). DDoS Attack Detection in IoT-Based Networks Using Machine Learning Models: A Survey and Research Directions. *Electronics*, *12*(14), 3103.

[61] Aljuhani, A. (2021). Machine learning approaches for combating distributed denial of service attacks in modern networking environments. *IEEE Access*, *9*, 42236-42264.

[62] Iftikhar, S., Al-Madani, D., Abdullah, S., Saeed, A., & Fatima, K. (2023). A supervised feature selection method for malicious intrusions detection in IoT based on genetic algorithm. *International Journal of Computer Science & Network Security*, *23*(3), 49-56.

[63] Fauzi, M. A., Hanuranto, A. T., & Setianingsih, C. (2020, October). Intrusion detection system using genetic algorithm and K-NN algorithm on dos attack. In *2020 2nd International Conference on Cybernetics and Intelligent System (ICORIS)* (pp. 1-6). IEEE.

[64] Liu, X., & Du, Y. (2023). Towards effective feature selection for iot botnet attack detection using a genetic algorithm. *Electronics*, *12*(5), 1260.

[65] Ahmad, R., Wazirali, R., Bsoul, Q., Abu-Ain, T., & Abu-Ain, W. (2021). Feature-selection and mutual-clustering approaches to improve DoS detection and maintain WSNs' lifetime. *Sensors*, *21*(14), 4821.

[66] Onah, J. O., Abdullahi, M., Hassan, I. H., & Al-Ghusham, A. (2021). Genetic Algorithm based feature selection and Naïve Bayes for anomaly detection in fog computing environment. *Machine Learning with applications*, *6*, 100156.

[67] Ullah, S., Mahmood, Z., Ali, N., Ahmad, T., & Buriro, A. (2023). Machine learning-based dynamic attribute selection technique for ddos attack classification in iot networks. *Computers*, *12*(6), 115.

[68] Alzahrani, R. J., & Alzahrani, A. (2021). Security analysis of DDoS attacks using machine learning algorithms in networks traffic. *Electronics*, *10*(23), 2919.

[69] Zhao, J., Xu, M., Chen, Y., & Xu, G. (2023). A DNN architecture generation method for DDoS detection via genetic alogrithm. *Future Internet*, *15*(4), 122.

[70] Marvi, M., Arfeen, A., & Uddin, R. (2021). A generalized machine learning-based model for the detection of DDoS attacks. *International Journal of Network Management*, *31*(6), e2152.

[71] Norouzi, M., Gürkaş-Aydın, Z., Turna, Ö. C., Yağci, M. Y., Aydin, M. A., & Souri, A. (2023). A Hybrid Genetic Algorithm-Based Random Forest Model for Intrusion Detection Approach in Internet of Medical Things. *Applied Sciences*, *13*(20), 11145.

[72] Seifousadati, A., Ghasemshirazi, S., & Fathian, M. (2021). A Machine Learning approach for DDoS detection on IoT devices. *arXiv preprint arXiv:2110.14911*.

[73] Mohmand, M. I., Hussain, H., Khan, A. A., Ullah, U., Zakarya, M., Ahmed, A., ... & Haleem, M. (2022). A machine learning-based classification and prediction technique for DDoS attacks. *IEEE Access*, *10*, 21443-21454.

[74] DeBarr, D., & Wechsler, H. (2010). Using social network analysis for spam detection.

In *Advances in Social Computing: Third International Conference on Social Computing, Behavioral Modeling, and Prediction, SBP 2010, Bethesda, MD, USA, March 30-31, 2010. Proceedings 3* (pp. 62-69). Springer Berlin Heidelberg.

[75] Rusland, N. F., Wahid, N., Kasim, S., & Hafit, H. (2017, August). Analysis of Naïve Bayes algorithm for email spam filtering across multiple datasets. In *IOP conference series: materials science and engineering* (Vol. 226, No. 1, p. 012091). IOP Publishing.

[76] Xu, H., Sun, W., & Javaid, A. (2016, March). Efficient spam detection across online social networks. In *2016 IEEE International Conference on Big Data Analysis (ICBDA)* (pp. 1-6). IEEE.

[77] Jiang, S., Pang, G., Wu, M., & Kuang, L. (2012). An improved K-nearest-neighbor algorithm for text categorization. *Expert Systems with Applications*, *39*(1), 1503-1509.

[78] Verma, M., & Sofat, S. (2014). Techniques to detect spammers in twitter-a survey. *International Journal of Computer Applications*, *85*(10).

[79] Subasi, A., Alzahrani, S., Aljuhani, A., & Aljedani, M. (2018, April). Comparison of decision tree algorithms for spam e-mail filtering. In *2018 1st International Conference on Computer Applications & Information Security (ICCAIS)* (pp. 1-5). IEEE.

[80] Jamil, F., Kahng, H. K., Kim, S., & Kim, D. H. (2021). Towards secure fitness framework based on IoT-enabled blockchain network integrated with machine learning algorithms. Sensors, 21(5), 1640.