Computers, Materials & Continua

Tech Science Press

DOI: 10.32604/cmc.2023.036894

REVIEW

Survey on Deep Learning Approaches for Detection of Email Security Threat

Mozamel M. Saeed[1,*] **and Zaher Al Aghbari**[2]

[1]Department of Computer Science, Prince Sattam bin Abdulaziz University, Al Kharj, 11912, Saudi Arabia

[2]Department of Computer Science, University of Sharjah, Sharjah, 27272, United Arab Emirates

*Corresponding Author: Mozamel M. Saeed. Email: m.musa@psau.edu.sa

Received: 15 October 2022 Accepted: 06 March 2023 Published: 31 October 2023

ABSTRACT

Emailing is among the cheapest and most easily accessible platforms, and covers every idea of the present century like banking, personal login database, academic information, invitation, marketing, advertisement, social engineering, model creation on cyber-based technologies, etc. The uncontrolled development and easy access to the internet are the reasons for the increased insecurity in email communication. Therefore, this review paper aims to investigate deep learning approaches for detecting the threats associated with e-mail security. This study compiles the literature related to the deep learning methodologies, which are applicable for providing safety in the field of cyber security of email in different organizations. Relevant data were extracted from different research depositories. The paper discusses various solutions for handling these threats. Different challenges and issues are also investigated for e-mail security threats including social engineering, malware, spam, and phishing in the existing solutions to identify the core current problem and set the road for future studies. The review analysis showed that communication media is the common platform for attackers to conduct fraudulent activities via spoofed e-mails and fake websites and this research has combined the merit and demerits of the deep learning approaches adaption in email security threat by the usage of models and technologies. The study highlighted the contrasts of deep learning approaches in detecting email security threats. This review study has set criteria to include studies that deal with at least one of the six machine models in cyber security.

KEYWORDS

Attackers; deep learning methods; e-mail security threats; machine learning; phishing

1 Introduction

Cyber security plays a vital role in advancing technology, internet services, and applications. It is essential for both organizations and individuals. Cyber attackers are increasingly using malware, sometimes known as “malicious software,” such as viruses, worms, Trojan horses, and spyware, to infect businesses with a range of attacks. Research on leveraging the classification power of deep neural networks in the security of e-mails is relatively new. Deep neural networks, such as Convolutional Neural Networks, Long Short Term Memory Networks, and Recurrent Neural Networks are some important networks, which resulted in designing and improving the security of e-mails. Therefore, literature related to the methodologies of such deep learning techniques in e-mail threat detection highlights the findings of this research and finds the existing gaps in this area. Attackers can easily modify rights, access confidential data, observe user activity, and carry out other nefarious deeds [1,2].

"Business E-Mail Compromise" (BEC), is an email-borne employee impression that has become a significant security threat and is thus named "Federal Bureau of Investigation (FBI)" [3]. Almost $2.7 billion has been lost by U.S. organizations in 2018 and $12 billion collectively since 2013 [4]. Several well-known companies have witnessed such attacks, such as Ubiquiti, Facebook, and Google [5,6].

Blacklisting comprises blacklisted senders' list whose email and IP addresses are blocked and categorized as a list-based filter. Spamming and phishing can be detected through different techniques like heuristics and blacklisting [7]. The main issue concerning the procedure of blacklisting is that filters check the presence of newly arrived emails or Uniform Resource Locators (URLs) in the existing blacklisted records. If the email or URL is present, it will be classified as a malicious email. Moreover, a lot of time is taken to detect the blacklisted emails with the help of the heuristics technique [8]. The studies relating to the classification of email spam and the techniques used in the organization to control the threats related to security. The research identifies that spam threats are present in any account and can easily be transferred all around the world in the system or the network. In the study, Term frequency-inverse document frequency was a proposed method approach using a support vector machine which is one of the tools to calculate the matrices and accuracy of the algorithms in datasets [9,10]. According to one of the studies, Thermal Emission Imaging System (THEMIS) is one of the deep learning models which identify and improve the word level in spam emails. The percentage accuracy of these models on educating data sets is 99.9% and the analytical data set are 98.9% [10]. The professionals, engineers, and researchers who believe in the general area of e-mail security, and especially those designing and developing robust techniques for detecting e-mail threats would benefit from the findings of this comprehensive review. Thus, machine learning techniques are likely to offer better outcomes as compared to classical heuristic and blacklisting techniques.

Many recent studies proposed the methodologies but this research has combined the merit and demerits of the deep learning approaches adaption in email security threats. The study aims to investigate deep learning approaches for detecting the threats associated with e-mail security. This study compiles the literature related to the deep learning methodologies which are applicable for providing safety in the field of cyber email security of different organizations. Deep learning approaches are comprised of different models and their application needs more advancement in the field of technology networks which is a more complex and newer approach than the traditional machine learning approaches, even though deep learning is considered a subset of machine learning [11]. Furthermore, examples are encompassed to show how the techniques have been utilized in e-mail security.

The main contributions of this study are as follows:

- Create a theoretical base for email security using deep learning methods. Unlike previous reviews, this review investigates papers published between 2016 and 2022, from pre-defined resources, and based on pre-defined inclusion/exclusion criteria.
- Provides a comparison between challenges in detecting email security using deep learning and detection methods with their performances.
- Identify research gaps in email security and suggest future possible research directions.

The rest of the paper is organized as follows: Section 2 discusses the related works to our investigation. Section 3 presents the methodology of conducting this review including the inclusion/exclusion criteria. A review of the different types of email attacks is presented in Section 4. In Section 5, a comprehensive investigation of the different techniques used in email security is discussed. Section 6 presents a discussion of the pros and cons of the different deep learning methods used in email security.

2 Literature Review

2.1 Internet of Things

The Internet of Things (IoT) is a new emerging technology that generates much data nowadays. Today, IoT is largely a concept in which everything is interconnected via the Internet. IoT is presently and will undoubtedly be the cornerstone for future development since it opens up new avenues for unique services. The IoT market is thriving because the number of calculations that a computer can perform almost doubles biannually. In comparison, the size and quantity of electricity required over the same period are approximately half [12]. This implies that smaller and more powerful devices for connectivity and data transmission are now accessible, allowing for a broader range of applications. This component raises severe security concerns, which will be addressed immediately. Spamming difficulties are on the rise as a result of the rise of IoT. To identify and filter spam and spammers, numerous spam detection approaches are presented [13]. Existing spam detection systems are broadly classified into two categories: semantic pattern-based approaches and behavior pattern-based approaches. Every business carefully assesses the available solutions to combat spam in their environment to correctly detect spam emails and prevent escalating email spam challenges. Whitelist/Blacklist, keyword checking, mail header analysis, and other well-known procedures are employed for identifying and analyzing incoming emails for spam detection.

2.2 E-Mail as Medium of Communication

The usefulness of communication via email has pointed to the issue of large-scale spam, specifically e-mail attacks. To address the problem of phishing attacks, several measures against phishing have been proposed. Sheng et al. [14] examined the efficiency of phishing blacklists. The Blacklist majorly contains a Blacklist of senders and a Blacklist of links. This discovery method receives the sender's address and contact information in the e-mail and checks whether it has been blacklisted. Users are usually notified of updates to the Blacklist and manually detect whether it is a phishing scam. There are currently two known websites for this purpose, PhishTank, and OpenPhish. In this regard, the outstanding performance of the Blacklist shows that the method is well based on the responsive list of hardware logistics. Notably, the link between natural language processing and machine learning has immensely contributed to the discovery of online phishing. Semantic features [15], grammatical features [16], and contextual elements [17] have previously been used in this field. Vazhayil et al. [18] commenced with the fundamental techniques for net phishing analysis. Hamid et al. [19] investigated the use of a hybrid process that merges content and behavior. Email-based analytics majorly uses tagged phishing e-mails and legitimate e-mails for training and sorting to acquire a sorting model for online sorting. Bergholz et al. [20] proposed a set of actions, divided into three categories: basic features, latent topic features, and the powerful features of the Markov chain. The basic features represent extraction directly from the email without extra processing. The topic model features cannot be extracted from email while they appear similar and together. However, Dynamic Markov chain features are text features based on the bag-of-words, where the goal is to compute the probability of whether an email belongs to a specific group by modeling each type of message content.

According to the latest research, email security threats are having domains to be emphasized for the real identification of users, the content of the emails which hack the Internet integrated technologies by their exposure on the device. The simple login in the technology can absorb all the accessible data of the network. While combining machine learning, deep learning methodologies with the algorithms of the neural network have to control the traffic of the email spasm. As email is one of the cheapest and most easily accessible platforms all around the world. Natural language processors are one the efficient way to understand the nature of the email, whether the source is authenticated for the future aspect or not [21,22].

One disadvantage of Natural language processing (NLP)-based machine learning in online phishing is that it is based on the surface text of the e-mail rather than deep semantics. Therefore, with NLP based on machine learning, it is difficult to find synonyms, various sentence types, and other variants [23]. Also, machine learning methods rely primarily on attribute creation to create e-mail attributes and perform tasks through these attributes. Both blacklisting and functional engineering should be performed manually and need a large workforce and experienced specialists, which restricts the success of the analysis. On the other hand, deep learning has been successful in various NLP projects, which include text categorization [24], information extraction [25], and machine translation [26].

2.3 E-Mail Text Representation

Bag-of-word is an approach for extracting features in text data and is thus used as e-mail text representation [27]. The vocabulary of the predefined words and the extent of their occurrence are the two aspects encompassed within the model [28].

A term document matrix is an approach to represent the text based on its presence in the document [29]. The documents are expressed through the horizontal rows, while the terms that occurred in the corpus are described in the vertical columns. The term frequency-inverse document matrix determines a word's relevancy in a predefined document [30]. The inverse document frequency indicates how much data a specific comment offers, whether a rare or a common phrase [31]. Thereby, singular value decomposition can be initiated for the symmetric diagonal decomposition (SDD) [32]. A document term matrix can be developed using different terms from a pair of documents in this process [33]. Random weights initialize the embedding layer and explore embedding for all training dataset words. The first hidden layer of a network is conceptualized through the embedding layer.

2.4 Deep Learning

Here in text, scientists and researchers use machine learning (ML) and Deep learning (DL) models in several applications including agriculture [34], environment [35], text sentiment analyses [24], medicine [36], and in cyber security [37].

- Planet scope Nanosatellites Image Classification Using Machine Learning [38]
- Convolutional Neural Network-Based Automated Weed Detection System Using Unmanned Aerial Vehicle UAV Imagery [39]
- Synthetic Minority Oversampling Technique with Deep Neural Network (SMOTEDNN): A Novel Model for Air Pollution Forecasting (APF) and Air Quality Index (AQI) Classification [40]
- Climate Deep Long Short-Term Memory (CDLSTM): A Novel Model for Climate Change Forecasting [41]
- Ground water level prediction using machine learning models [42]
- Deep Learning-Based Supervised Image Classification Using UAV Images for Forest Areas Classification [43]
- Bulk Processing of Multi-Temporal Modis Data, Statistical Analyses, and Machine Learning Algorithms to Understand Climate Variables in the Indian Himalayan Region [44]

- Study of permafrost distribution in Sikkim Himalayas using Sentinel-2 satellite images and logistic regression modeling [45]
- The efficiency of artificial neural networks for glacier ice-thickness estimation: A case study in the western Himalayas, India [46]
- Sentiment analysis using machine learning: Progress in the machine intelligence for data science [47]
- Fine-tuned convolutional neural network for different cardiac view classifications [48]
- Insider Threat Detection Based on Natural Language Processing Word Embedding and Machine Learning [49]
- Classification of botnet attacks in Internet of Things Using a Convolution Neural Network [50]
- A survey of Convolution Neural Network based Network intrusion detection [51], natural language processing [48], and speech recognition [52].

Based on their architectures, deep learning models may be divided into four groups:

- Deep feed-forward neural network (DFNN), which includes several multi-layer deep learning models such as deep belief network [53], deep Boltzmann machine [54], and deep autoencoder [55]
- Convolutional neural network (CNN), which uses the convolutional and pooling layers to achieve the shift-invariant property
- Recursive neural network (RvNN), which accepts a recursive data structure of various sizes and generates hierarchical predictions
- Recurrent neural network (RNN), which has an internal hidden state to capture sequential input.

The most popular machine learning-based classifier is the support vector machine, which helps in detecting phishing and spam emails. A feature map based on the train sets and predefined transformation is built. Moreover, the phishing and spam emails are also filtered with the help of classifiers like K-nearest neighbor (KNN), in which the decisions are taken considering the K-nearest train input. A predefined similarity function is used for choosing the samples. Another classifier named Naïve Bayes considered the simple probabilistic classifier is also used. It is also possible to incorporate boosting techniques considering sequential adjustment during the process of classification. The term frequency-inverse document frequency (TF-IDF) and hand-crafted feature engineering are used for converting the email into email vectors. The reliance on classical machine learning algorithms for feature engineering is considered the major disadvantage [56]. The accuracy can be increased by selecting the best feature and for selecting the best feature there is a need for adequate knowledge about of domain. There is a decrease in the algorithm's predictive value when the feature engineering is not performed correctly. Moreover, the models can be predicted with the help of classical machine learning algorithms. Feature extraction during the classical machine learning workflow takes most of the time.

Recently, leverage has been given to the application of deep learning architectures for different cases using cyber security such as detecting phishing and malicious URL [57], intrusion detection [58], malware detection [59], detecting malicious domain names [60], and detecting phishing e-mail [61]. Deep learning architecture is can extract optimal features without any reliance on feature engineering. Therefore, deep learning architecture is considered to be robust in an adversarial environment, as compared to classifiers of classical machine learning.

2.5 Deep Learning Tools

Deep learning tools can automatically create active e-mail operations for detecting phishing e-mails. Thereby, the emphasis is on using deep learning to discover e-mail phishing in a more complete and comprehensive description of e-mail information. Repke et al. [62] returned the structure to a free-text e-mail conversation with in-depth study and word usage. Although this work is not about analyzing e-mails by e-mail, it is still illustrative for us to use deep learning and built-in word technology to use e-mails. Hiransha et al. [63] and Keras [64] suggested Word Connection and Convolutional Neural Networks (CNN) for building a phishing e-mail discovery model. There are other in-depth algorithms in use, such as Deep Fault Networks (DBN) and Recurrent Neural Networks (RNNs) [65–67]. These in-depth methods of counterfeiting e-mail analytics only apply NLP technology to fake e-mail analytics and ignore the difference between counterfeit e-mail and other goals. Contextual information is avoided to some extent.

Xu et al. [68] proposed region-based convolutional neural network (RCNN) for text classification in 2015. They investigated it on four different datasets, which include 20 Newsgroups datasets (2018), Fudan library (2018), Association for computational linguistics (ACL) corpus network (2018), and Stanford Attitude tree library (2018). They were found to be effective as compared to the standard CNN. RCNN can generate highly complex sequencing tasks. Based on why e-mail is also a problematic text, this article introduces the THEMIS model based on RCNN. Zhang et al. [65] suggested different methodologies in machine translation. Lee et al. [69] studied attention-grabbing methods of neural machine translation (NMT) and their implication on life. Attractive ways are very beneficial in several areas and can enhance image classification [70], automatic captions [71], and machine translation [72]. Pappas et al. [73] examined the hierarchical review process for document categorization and were successful in 2016.

For accurate compilation, the J48 classification algorithm deals with the extracted properties of data entered into the e-mail classification. Senturk et al. [74] treated pointless markup and new pages as feature sets and choose some features with better predictability from the initial operations. They provide O (1) complexity as an assessment method for each element set to assess its predictive power. Brites et al. [75] suggested solutions to overcome the lack of time to analyze phishing. The solution provided for phishing by analyzing the characteristics of who is Responsible for this domain name (WHOIS) and their URL information. Deep learning methods detect malicious URLs and domains [61]. Unnithan et al. [61] have used Hypertext markup language (HTML) content to analyze net phishing. Databases that contain reported phishing for this purpose, are used for many different purposes. Baykara et al. [76] used different types of classification methods, such as multi-layer perception (MLP), decision tree (D.T.), support vector machine (SVM), method of data processing like Group method of data handling (GMDH), probable neural network (PNN), genetic programming (G.P.) and logistic regression (L.R.). Mahesh [77] proposed a method for analyzing e-mails by e-mail with mixed features. It is called hybrid action because it combines URL-based, behavioral, and competitive actions. Overall calculated achievement remains 97.25% and an error rate of 2.75%. Hiransha et al. [63] suggested a weak assessment method that works through anomaly analysis, detecting a system where behavior deviates from a standard procedure. Karim et al. [78] created a machine-learning model for analyzing e-mails by e-mail. Using predictive analytics, a machine learning model was designed to use static analytics to distinguish between phishing and legitimate e-mail.

2.6 Architecture of Deep Learning

Classification of URLs as malicious or benign is represented in deep learning architecture in Fig. 1. The three national sections present in this architecture are:

- URL's character coding—convert characters into a format to be transmitted over the Internet
- Representing features via deep layers—arranging high-dimensional vectors in a compact image form conducible for deep learning
- Classification—non-linear activation function to assign scores

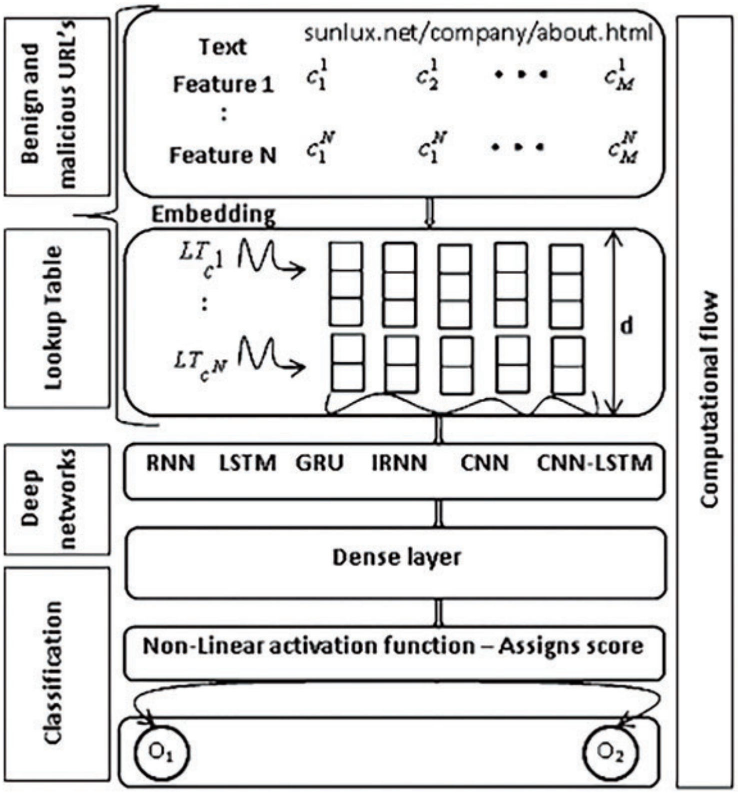
Benign and malicious URL's
Text
sunlux.net/company/about.html
Feature 1
Feature N
Embedding
Lookup Table
d
RNN LSTM GRU IRNN CNN CNN-LSTM
Deep networks
Dense layer
Non-Linear activation function – Assigns score
Classification
O1
O2
Computational flow

Figure 1: Architecture of deep learning [79]

2.7 Deep Neural Network

Artificial neural network (ANN), a computational model, is affected by features of biological neural networks. The family of ANN includes a convolutional neural network, recurrent neural network (RNN), and feed-forward neural network (FFN). A graph comprising neurons known as mathematical units is formed by FFN. The continuous cycle is formed as information is passed on by FFN from one side of the node to another. Therefore, past values are not highly valued. As shown in Fig. 2, the MLP is a kind of FFN comprising 3 or more layers:

- Input layer—receives the input signal to be processed
- Hidden layers (may be more than 1)—the true computational engine of the MLP
- Output layer (comprises of neurons known as units in mathematical notation)—performs tasks such as prediction and classification

The choice of the hidden layer is made considering the hyper-parameter tuning method. The sigmoid non-linear activation function is used by the classical multi-layer perceptron.

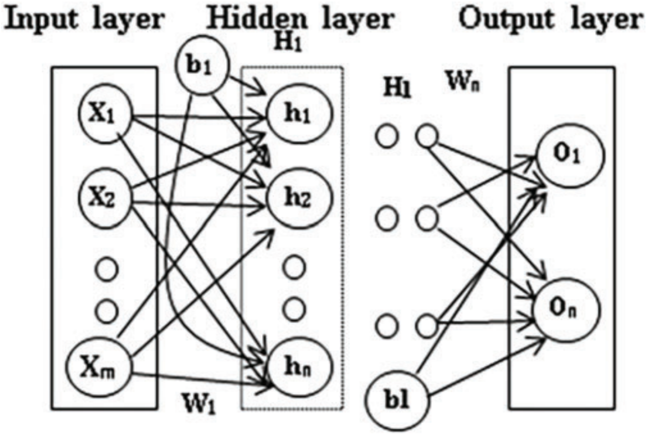

Figure 2: Hidden layers in the deep neural network [8]

3 Methods

3.1 Threats to Validity

This review study has set criteria to include studies that deal with at least one of the six machine models in cyber security. The target cyber threats include spam, detection, intrusion, and malware detection. For searching different string combinations were used for instance: ‘machine learning and cyber security and ‘deep learning and cyber security. Moreover, relevant data was taken from the Association for Computing Machinery (ACM) Digital Library, Science Direct, Web of Science, Scopus, IEEE Xplorer, and SpringerLink. Google Scholar. In addition to the papers provided, the prior survey and review articles were used to offer a thorough performance rating.

3.2 Paper Filtering

After downloading the paper results from the search using the search terms discussed above, the study analyses articles that are available in Open access. Irrelevant and duplicate documents were removed by applying the exclusion criteria (shown below). The following inclusion/exclusion rules are used in these papers. After screening studies through inclusion and exclusion the study includes 101 studies in this review article. The inclusion criteria of the study are:

- Papers published within the last decade.
- Papers in the area of detecting e-mail threats using deep learning techniques.
- Papers are written in the English language.
- Papers that are available in Open access.

The exclusion criteria of the study are:

- Papers on deep learning but not on e-mail threat detection.
- Papers with unclear citation information include year, authors, publisher, etc.
- Papers with unclearly written methodology.
- Papers with that are not available on Open access.

4 Review Analysis

4.1 E-Mail Security Threats

E-mail is frequently the target of attacks since it is widely deployed, used, and well-understood for communicating with untrusted external organizations. Attackers can exploit e-mails to gain control over an organization, disrupt Information Technology. Access to resources, and access confidential information [80]. The following are the common threats to e-mail systems:

4.1.1 Malware

Progressively, attackers benefit from e-mails for delivering a myriad of attacks to corporations through malicious software or malware that encompass viruses, spyware, worms, and Trojan horses [81]. If successful, such attacks may offer negative entity control over servers and workstations, which can be exploited for transforming advantages, gaining access to sensitive information, monitoring users' activities, and performing other malicious activities [82]. Deep learning techniques are also used in post-production. In other words, after the malware's analysis (training) of the available signaling data, the analysis tool (detection system) can be tested based on new real-time data for performance evaluation.

4.1.2 Spam and Phishing

Spam messages disturb consumer productivity, use information technology resources excessively, and are used as a dissemination platform for malware [83]. Phishing is related to spam and refers to deceptive computer-based ways to trick individuals into reacting to the e-mail and disclosing sensitive information. Spam messages are delivered through compromised e-mail systems using an alternate e-mail address [84].

4.1.3 Social Engineering

E-mail can be used by an attacker instead of hacking into a system to collect sensitive information from consumers of an organization or getting users for performing activities. E-mail spoofing is a typical social engineering attack. One individual or program successfully pretenses as another by fabricating sender information in e-mails to hide the true origin [85].

Table 1 presents a review of e-mail security using deep learning, discussing various concerned topics and studies conducted by different authors over the years. It highlights the threats related to e-mail security, such as e-mail-based attacks aimed at seizing control of companies and accessing private information. It also covers malware, spam, phishing, and social engineering issues in e-mail security, as well as the use of deep learning for managing bulk e-mails and controlling security on smart devices.

Table 1: Reviewing e-mail security using deep learning

Concerned topic	Study/Author	Year	Concluding remarks
E-mail security threats	Fowler	2017	Attackers may use e-mail to seize control of a company, disrupt Information Technology access to resources, and get access to private information.

(Continued)

Table 1 (continued)

Concerned topic	Study/Author	Year	Concluding remarks
	Cidon et al.	2019	The most common cyber threat to the email security system is business emailing compromise (BEC) and impersonation of employees. There was for the attacker to with the private credential of the users. The security of data collection needs to be strong by using malicious payload with alerts.
	Sheng et al.	2009	Threatening email security is known as a crime of the ecosystem by enforcing the policies and countermeasures to shut the money trails and misalignment of new policies development.
	Unnithan et al.	2014	MitM-attack (Man in the Middle) is a recent advancement and one of the common programs used by non-mobile systems. It has a low ratio and probability of a false positive attitude in the users. The packet of transmission control protocol (TCP) has successfully installed the time stamps which can delay all the sequential delays of the reference data for its authentication.
Malware	Zeng	2017	Attackers utilize e-mail to transmit a variety of attacks on companies using malicious software or malware, including viruses, spyware, worms, and Trojan horses.
	Om	2017	Attacks may provide an evil entity with authority over servers and workstations, which may subsequently be utilized to change benefits, access sensitive information, monitor users' actions, and engage in other harmful acts.
	Roberts	2017	Criminal knows the trick to collect the information of information from users and then commit illegal robberies and thefts, transferring the money illegally. The organization has to provide, more protection to the hardware and the software of the system and demonstrate to the users the psychology of the cybercriminals.

(Continued)

Table 1 (continued)

Concerned topic	Study/Author	Year	Concluding remarks
	Chiramdasu et al.	2021	The framework to control the malicious content of the URLs by implementing Logistic regression. The sources of Phish tank, kaggle.com, etc., have been used to test the model. And it resulted in positive feedback.
Spam and phishing	Vergelis et al.	2019	Spam communications can disrupt customer productivity, use an excessive amount of I.T. resources, and serve as a platform for virus distribution.
	Patel et al.	2019	Spam communications are sent via hacked e-mail systems using a different e-mail address.
	FBI	2018	In this case study, students have identified the techniques of phishing and email scams by controlling the lens of internal and external audits. The issues related to BEC have the remediate ways and controls the implement to minimize the effect of risk of cyber security.
	Mohan et al.	2018	Online cybercrimes and the scams of technology will mitigate the issues of high demand. Detection of Domain Generation Algorithm (DGA) and URL malicious detection has been studied. The positive outcome discovered was the proposed syntactic patterns for identification of ominous online factors S.P.O.O.F net model which has 99% control of cybersecurity.
Social engineering	Albladi et al.	2018	E-mail spoofing is a common social engineering assault in which one person or program successfully impersonates another by forging sender information in e-mails to conceal the genuine origin.
	Yuan et al.	2018	Industrial and academic organizations have many users and their usage behavior is countable. Insider threat detection has been actively controlled by Long Short Term Memory (LSTM) and Convolutional Neural Networks (CNN).

(Continued)

Table 1 (continued)

Concerned topic	Study/Author	Year	Concluding remarks
	He et al.	2016	The visualization of the recognized task for deep neural networking has been very difficult to train. The foundation of the common object in context (COCO) object detection dataset has provided improvement. Image, not detection localization is considered to be the most successful advancement.
	Park et al.	2015	The object of the verbs in the legitimate emails and the phishing emails have syntactic similarity in their content more technological advancement need to be added in controlling the email content.
	LeCun et al.	2015	To induce the model of the deep learning discoveries, internal parameters of propagating back algorithm have to use the control on images, video, and audio data.
Management of bulk email	Kong et al	2021	To scrutinize the content of Bulk emailing related to the advertisement of different organizations and media is considered one the biggest to control time waste and the easy access of spam into the used devices. Many management strategies are discussed to handle this revolutionary problem technically [86].
	Stringhini et al.	2015	For most companies, spear phishing is considered to be more sophisticated which causes them many major losses. The model of controlling the advance subsequent emailing is the most important step and needs more advancement in it.
	Bhowmick et al.	2016	The filtered email spam technique is needed to mere focus. The development in the programming of email has been required for exploring the benchmark for evaluation and the prior examination of basic email filtering by using engineering tools.

(Continued)

Table 1 (continued)

Concerned topic	Study/Author	Year	Concluding remarks
	Verma et al.	2014	The email system which is integrated into different has about 95% accuracy data of the users and it has a robust adaptive method to control the problem and protect sensitive information.
	Vinayakumar et al.	2018	Domain name System (DNA) logs and the system proxy logs have been the successful platform to control the big data of the internet security. The detection of fraud and activities of malicious networking needs a proper approach to analyze packets of the network.
Controlled security on smart devices	Al-Garadi et al.	2020	Modern short-hand techniques for safety development related to deep learning and machine learning handling are suggested to save the privacy of the individual's personal smart devices [87].
	Yuan et al.	2021	Deep learning is considered the tool to detect insider threats. There is a very less ratio that the employee of the company understand the sensitivity of malware and uses the infected universal serial bus (USB) drive on a different platform and their workstation. It is one of the biggest challenges to control.
	Vinayakumar et al.	2019	To control the use the external devices, the proposed high-scale framework has been used like (SHIA) Sale Hybrid IDS Alert Net, which has the capability to monitor the 24-hour networking and is able to generate alerts to stop cyber-attacks.
	Berman et al.	2019	The deep learning method and its cyber security applications have provided the proper restricted machines of Boltzmann and the auto deep generated encoders, it has generated many adversarial networks. A broad array of Botnets to control the malicious domain attack and false data injection has been administered in different organizations.

(Continued)

Table 1 (continued)

Concerned topic	Study/Author	Year	Concluding remarks
	Vinayakumar et al.	2018	The efficacy of the deep learning network has detected the issue of the executable of portable files in the system. The experiment of the 1000 epochs has a very effective topologies network and it has very positive results in the trial experiments.
	Rao et al.	2019	Automation of security defense has the assistance to integrate the application of security and infrastructure. This study included the predictive analysis of 89.7% which provide full security to the upcoming attack and the policies which are implemented for defense.

4.2 Deep Learning Methods for Handling Email Security Threats

4.2.1 Content-Based Filtering Technique

In the content-based recommender system, the explanations related to the target item play an essential role in making predictions. These explanations are termed Content. In the content-based recommender system, the past purchasing designs and the senior ratings of the users, along with the item's content, are collectively utilized, keeping in mind the end goal to arrive at predictions. The primary thought behind the content-based recommender system is that user interests can be determined based on features or properties of the items they have graded or used previously. Content-based systems suggest items because of a close examination between the description of the items and a client's profile. The component of items is mapped with the highlight of clients keeping in mind the end goal to get a client–item similarity. The best-coordinated pairs will be recommended as suggestions. In the recommendations of documents to the users such as articles, papers, weblogs, web pages, publications, and so on, the content-based recommender systems are regarded as the most successful filtering technique. Content based filtering (CBF) used many different models, such as the vector space model, neural networks, decision trees, etc., to find or measure document similarity.

4.2.2 Case-Based Spam Filtering Method

It is one of the well-known spam filtering methods. In particular, pre-processing steps transform the e-mail via client interface, selection, process assessment, feature extraction, and e-mail data grouping. Initially, extraction for both spam and non-spam e-mails is made using the collection model. Afterward, the data is categorized into two vector sets. Finally, the deep learning algorithm is utilized for training datasets and testing them for deciding whether the prospective mails are spam or non-spam [88].

4.2.3 Recommender System

The first important point or approach in the recommendation system is predicting the rating value for the compound of the user item. In this case, the assumption is to predict data through the user's preferences for specific items. An M × N matrix is created to record the M user, and N items were recorded values used for the training model. The problem has occurred in the system due to a lack of accuracy as the system is based on an assumption. This problem is often known as the matrix completion problem because the matrix of values is recorded incomplete, and all other values are forecasted by learning algorithms. The other common problem in the recommendation system is the ranking problem. In the real scenario, it is not necessary that predicted items must be based on the user's past preferences because a user may not like any item again, which was considered in the past. The requirement for new item recommendations is not only based on ratings of user-specific preferences. So, the merchant should present something new to the user which may attract him more than past.

4.2.4 Likeness-Based Spam Filtering Technique

The likeness-based recommender system requires related data about various accessible things as the content alongside the client's profile, which must follow the client's preferences. In the content-based recommender system, the past purchasing designs and the senior ratings of the users, along with the item's content, are collectively utilized, keeping in mind the end goal to arrive at predictions. This technique is recommended the ideas to the users by comparing the user preferences and the content related to the items. Afterward, the current circumstances are assigned to the most well-known class of its K-closest training cases [89]. The K-nearest neighbor is used in this approach to filter spam e-mails. The newest form of likeness-based spam filtering technique is the support vector machine, the art classification technique to experience unwanted mail [90].

4.2.5 Adaptive Spam Filtering Technique

The primary thought behind the content-based recommender system is that user interests can be determined based on features or properties of the items they have graded or used previously. The explanations related to the target item play an essential role in making predictions. These explanations are termed Content. Content-based systems suggest items because of a close examination between the description of the items and a client's profile. The component of items is mapped with the highlight of clients keeping in mind the end goal to get a client–item similarity. The best-coordinated pairs will be recommended [91]. Previously, Seth et al. [92] applied multimodal spam classification using deep learning techniques. Similarly, Long Short-Term Memory (LSTM) and Bidirectional-LSTM (Bi-LSTM) were used in a previous paper conducted by Sethi et al. [93].

Table 2 reviews different deep learning methods for handling email security threats, specifically focusing on spam filtering techniques. The first study proposes a Case-Based Spam Filtering Method using deep learning to identify and classify spam emails based on training and evaluating datasets. The Likeness-Based Spam Filtering Technique, as described in the second study, suggests ideas to users by comparing user preferences and related email content. The third study presents an Adaptive Spam Filtering Technique that utilizes deep learning algorithms to map item components with user highlights, recommending the best-coordinated pairs as suggestions to users. Additionally, the third study mentions the use of Bi-LSTM and LSTM in classifying multimodal spam.

Table 2: Reviewing deep learning methods for handling email security threats

Concerned topic	Study/Author	Year	Concluding remarks
Case-based spam filtering method	Christina et al.	2010	The deep learning method is used to train and evaluate datasets to determine if upcoming e-mails are spam or not.
Likeness-based spam filtering technique	Sakkis et al.	2001	The Likeness-Based Spam Filtering Technique recommends ideas to users by comparing user preferences and material linked to the items.
	Chavez	2020	The K-nearest neighbor is employed to filter spam e-mails. The most recent type of likeness-based spam filtering approach is the support vector machine, a state-of-the-art classification tool for dealing with undesired e-mails.
Adaptive spam filtering technique	Pelletier et al.	2004	The component of items is mapped with the highlight of clients with the ultimate objective of achieving client–item similarity. As ideas, the best-coordinated pairs will be suggested.
	Seth et al.	2017	Deep learning algorithms were used to classify multimodal spam.
	Sethi et al.	2017	Bi-LSTM and LSTM were employed.

5 Discussion

Email is commonly used for official communication between people. Therefore, attackers frequently attack emails to access confidential information. Emails are attacks by malware which is also reported by Zeng [81] who stated that attackers benefit from e-mail for delivering a myriad of attacks to corporations through malicious software or malware. The spam is sent using a different email address and delivered through infected email systems as also stated by Patel et al. [84].

The cyber realm has massive amounts of data from many sources, to which deep learning may be applied. However, a study in this area is complicated by the scarcity of publicly available datasets, which are either tiny, outdated, or developed internally and not shared among researchers. Large, frequently updated benchmark datasets will be essential to improve cyber security solutions to build genuine confidence in deep learning algorithms. Furthermore, the ability to evaluate detection rates, speed, memory utilization, and other performance parameters require the capacity to test suggested deep learning algorithms in real-world operating settings. The cyber security sector has just recently begun to recognize the usefulness of Deep Learning, and new datasets are appearing.

Email security is among the most common issue encountered in recent times; therefore, several solutions are provided for controlling email security threats. However, the attackers usually modify their attack strategy by exploiting the existing solution’s susceptibilities. The email security threat can occur through the most common ways are malware, social engineering, and using fake e-mail or web pages which is in line with studies [94].

The DNS protocol is deployed through a DNS-based Blacklist for controlling phishing e-mails. However, a server experiences constraints concerning performance and resources because of many blacklisted e-mails. The term frequency and the inverse document frequency are essential concepts in an information retrieval system. The term frequency, denoted as term-frequency (TF), is the frequency of the specific terms in a particular document. It simply tells how many times the specific term appears in a document. At the same time, the inverse of the document is denoted by the inverse document frequency (IDF), which considers the terms with the lowest frequency. Suppose a user makes a search on Google for "the rise of technology", it is undoubtedly the term "the" will must have a high frequency than the term "technology". Still, the importance of the term technology cannot be denied as well from the query point of view. In such situations, the tf-idf discredits the impact of highly repeated words in a document to decide the significance.

According to the study, the smart devices which are integrated with the internet of things have many issues related to network access control, email, bank account, identity address authentication, and verification. The methods are introduced to control easy access by the hacker or the bad internet organization. Many advantages and shorthand techniques for safety development related to deep learning and machine learning handling are suggested to save the privacy of the individual on its own [87].

The service provider ensures authentication at the domain level [95]. E-mail based on domain name and hash password is used for authenticating e-mail level authentication as a digital signature [96]. It has been witnessed that most consumers ignored e-mail authentication, which became one of the significant barriers. Spoofed hyperlinks are a prevalent attribute in phishing e-mails. For instance, Chen et al. [97] examined the actual and visual associations for any variations. So, if the specific term appears many times in a document, it will reduce its weight automatically. Similarly, if a term appears a few times in documents, it is evident that the term has a higher weight. The IDF uses the log to dampen the impact of high-frequency terms [98]. In the review study by Kong et al. [86] enclosed are the management strategies to control the trafficking of the bulk email related to the promotion and advertisement of the organization or the media. The uncontrolled feedback on the product makes the user tired and wastes the time the user goes through every email. The most difficult part that user faces is the deletion of thousands of emails all at once. This traffic diverts the focus of the relevant communications [99].

It is recommended that the future of e-mail security systems lies in deep learning for deep adversarial learning and content-based classification techniques. Deep understanding enables computers to learn from knowledge and experience irrespective of comprehensive programming and significant patterns from primitive data [100]. In recent studies, the user who is using electronic email faces many fake email trafficking which disturbs the storage capacity and several cloud tool systems are invented for the protection of the systems [101].

6 Study Limitation

The conventional machine learning algorithms were very complicated for mining appropriately-represented attributes due to the restrictions that classified such algorithms. The limitations of the traditional machine learning algorithms encompass high computational costs, the need for knowledge from professionals in a specific field, and the curse of dimensionality. Deep learning techniques are deployed to solve representation issues by constructing several Naïve attributes to represent a multifaceted concept. Deep learning will be more influential in solving the problem of spam e-mails. Since the number of available training data is rising, the efficiency and effectiveness of deep understanding have become more considerable. Papers that are available in Open access are easy to access for extraction of the relevant studies but all the papers relevant to this study are not as open access. This is one of the main study limitations that every relevant study was not available to collect more information or for comparison.

7 Conclusion

The present study has investigated deep learning approaches for detecting the threats associated with e-mail security. This survey aims to present a relevant body of work to encourage academics to enhance the state of deep learning for cyber security systems. This study classified e-mail security threats, including social engineering, malware, spam, phishing, uncontrolled traffic of advertisement emails, and spam are aligned with discussion through various solutions for handling these threats. The compilation of different studies in this paper identifies many platforms for the organization to observe the internet system's security in the form of email trafficking. E-mail security can be detected easily by the coding method and spam email can be easily filtered by many computer software and the network by different learning models of deep learning and machine learning. This highlighted many visionary modules which are part of our daily life that require the safety development by cyber security to protect their dataset of the smart devices and the organization. LSTM and Bi-LSTM, the THEMIS model based on RCNN, and many models are integrating and designing the best platform to provide deep learning approaches for the detection of email security. Various solutions were classified as fake page detection or spoofed e-mail filtering. Identifying malicious actions can be improved by including these two sub-modules in the current framework. Although, many recent studies proposed the methodologies but this research have combined the merit and demerits of the deep learning approaches adaption to the email security threat. Future studies need to investigate technologies based on protected software or strategies or network to differentiate between useful email and spam email. Moreover, future studies also need to develop the strategy of deleting the bulk email at a more organized and organizational level as it is a time-consuming process.

Acknowledgement: The authors would like to express their deep thankful and grateful to all the associated personnel in any reference that contributed in/for the purpose of this research.

Funding Statement: This study is supported via funding from Prince Sattam bin Abdulaziz University Project Number (PSAU/2023/R/1444).

Author Contributions: M. M. Saeed: conceived and designed the experiments, analyzed the data, prepared figures and tables, authored and reviewed drafts of the manuscript, and approved the final manuscript. Z. Aghbari: analyzed the data, prepared figures and tables, authored and reviewed drafts of the manuscript, and approved the final manuscript.

Availability of Data and Materials: The data that support the findings of this study are available from the corresponding author M. M. Saeed, upon reasonable request.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] S. Yuan and X. Wu, "Deep learning for insider threat detection: Review, challenges, and opportunities," *Computers and Security*, vol. 104, pp. 102221, 2021.

[2] F. Yuan, Y. Cao, Y. Shang, Y. Liu, J. Tan *et al.,* "Insider threat detection with a deep neural network," in *Int. Conf. on Computational Science*, Wuxi, China, Lecture Notes in Computer Science, vol. 10860, pp. 43–54, 2018. https://doi.org/10.1007/978-3-319-93698-7_4

[3] A. Cidon, L. Gavish, I. Bleier, N. Korshun, M. Schweighauser *et al.,* "High precision detection of business e-mail compromise," in *28th USENIX Security Symp. (USENIX Security 19)*, University of South Carolina, Washington, USA, pp. 1291–1307, 2019. https://doi.org/10.1109/ms.2011.67

[4] FBI. "Business e-mail compromise," The 12-billion-dollar scam, 2018. [Online]. Available: https://www.ic3.gov/media/2018/180712.aspx

[5] J. J. Roberts, "Facebook and google were victims of $100m payment scam," 2017. [Online]. Available: http://fortune.com/2017/04/27/facebook-google-rimasauskas/

[6] G. Stringhini and O. Thonnard, "That ain't you: Blocking spearphishing through behavioral modeling," in *Int. Conf. on Detection of Intrusions and Malware, and Vulnerability Assessment*, Cham, Milan, Italy, Springer, pp. 78–97, 2015. https://doi.org/10.1007/978-3-319-20550-2_5

[7] A. Bhowmick and S. M. Hazarika, "Machine learning for e-mail spam filtering: Review, techniques and trends," 2016. [Online]. Available: http://arXiv:1606.01042. https://doi.org/10.1007/978-981-10-4765-7_61

[8] R. Vinayakumar, M. Alazab, K. P. Soman, P. Poornachandran, A. Al-Nemrat *et al.,* "Deep learning approach for intelligent intrusion detection system," *IEEE Access*, vol. 7, pp. 41525–41550, 2019. https://doi.org/10.1109/access.2019.2895334

[9] R. Singh, "Analysis of spam email filtering through naïve bayes algorithm across different datasets," *International Journal of Innovative Science and Research Technology*, vol. 6, no. 5, pp. 644–647, 2021.

[10] R. Chiramdasu, G. Srivastava, S. Bhattacharya, P. K. Reddy and T. R. Gadekallu, "Malicious URL detection using logistic regression," in *2021 IEEE Int. Conf. on Omni-Layer Intelligent Systems (COINS)*, Barcelona, Spain, pp. 1–6, 2021. https://doi.org/10.1109/coins51742.2021.9524269

[11] D. S. Berman, A. L. Buczak, J. S. Chavis and C. L. Corbett, "A survey of deep learning methods for cyber security," *Information*, vol. 10, no. 4, pp. 122, 2019.

[12] K. Shaukat, T. M. Alam, I. A. Hameed, W. A. Khan, N. Abbas *et al.,* "A review on security challenges in internet of things (IoT)," in *2021 26th Int. Conf. on Automation and Computing (ICAC) IEEE*, Portsmouth, UK, pp. 1–6, 2021. https://doi.org/10.23919/icac50006.2021.9594183

[13] N. Ahmed, R. Amin, H. Aldabbas, D. Koundal, B. Alouffi *et al.,* "Machine learning techniques for spam detection in email and IoT platforms: Analysis and research challenges," *Security and Communication Networks*, vol. 2022, pp. 1–19, 2022.

[14] S. Sheng, B. Wardman, G. Warner, L. Cranor, J. Hong *et al.,* "An empirical analysis of phishing blacklists," 2009. https://doi.org/10.1109/ecrime.2009.5342608

[15] R. Verma and N. Hossain, "Semantic feature selection for text with application to phishing email detection," in *Lecture Notes in Computer Science*, pp. 455–468, 2014. https://doi.org/10.1007/978-3-319-12160-4_27

[16] G. Park and J. M. Taylor, "Using syntactic features for phishing detection," 2015. [Online]. Available: http://arXiv:1506.00037. https://doi.org/10.1063/pt.5.028530

[17] R. Verma, N. Shashidhar and N. Hossain, "Detecting phishing emails the natural language way," *Lecture Notes in Computer Science*, pp. 824–841, 2012. https://doi.org/10.1007/978-3-642-33167-1_47

[18] A. Vazhayil, N. B. Harikrishnan, R. Vinayakumar, K. P. Soman and A. D. R. Verma, "PED-ML: Phishing e-mail detection using classical machine learning techniques," in *Proc. of 1st AntiPhishing Shared Pilot 4th ACM Int. Workshop Secure, Privacy Anal (IWSPA)*, Tempe, AZ, USA, pp. 1–8, 2018. https://doi.org/10.1109/icccnt.2018.8494159

[19] I. R. A. Hamid and J. Abawajy, "Hybrid feature selection for phishing e-mail detection," in *Int. Conf. on Algorithms and Architectures for Parallel Processing*, Berlin, Germany, Springer, pp. 266–275, 2011. https://doi.org/10.1007/978-3-642-24669-2_26

[20] A. Bergholz, J. De Beer, S. Glahn, M. F. Moens, G. Paaß *et al.,* "New filtering approaches for phishing email," *Journal of Computer Security*, vol. 18, no. 1, pp. 7–35, 2010.

[21] T. Mehrotra, G. K. Rajput, M. Verma, B. Lakhani and N. Singh, "Email spam filtering technique from various perspectives using machine learning algorithms, in data driven approach towards disruptive technologies," in *Proc. of MIDAS 2020*, Singapore, Springer, pp. 423–432, 2021. https://doi.org/10.1007/978-981-15-9873-9_33

[22] S. P. Shyry and Y. B. Jinila, "Detection and prevention of spam mail with semantics-based text classification of collaborative and content filtering, in journal of physics," in *Int. Conf. on Mathematical Sciences (ICMS 2020)*, Chennai, India, pp. 1770–12031, 2021. https://doi.org/10.1088/1742-6596/1770/1/012031

[23] C. N. Gutierrez, T. Kim, R. Della Corte, J. Avery, D. Goldwasser *et al.,* "Learning from the ones that Got away: Detecting new forms of phishing attacks," *IEEE Transactions on Dependable and Secure Computing*, vol. 15, no. 6, pp. 988–1001, 2018.

[24] J. Barnes, R. Klinger and S. S. I. Walde, "Projecting embeddings for domain adaptation: Joint modeling of sentiment analysis in diverse domains," 2018. [Online]. Available: http://arXiv:1806.04381. https://doi.org/10.18653/v1/p18-1231

[25] P. Li and K. Mao, "Knowledge-oriented convolutional neural network for causal relation extraction from natural language texts," *Expert Systems with Applications*, vol. 115, pp. 512–523, 2019. https://doi.org/10.1016/j.eswa.2018.08.009

[26] Y. Kim, C. Denton, L. Hoang and A. M. Rush, "Neural machine translation by jointly learning to align and translate," in *Proc. of ICLR*, 2017. https://doi.org/10.18653/v1/w18-2703

[27] S. Douzi, F. A. AlShahwan, M. Lemoudden and B. E. Ouahidi, "Hybrid email spam detection model using artificial intelligence," *International Journal of Machine Learning and Computing*, vol. 10, no. 2, pp. 316–322, 2020.

[28] W. Etaiwi and A. Awajan, "The effects of features selection methods on spam review detection performance," in *Int. Conf. on New Trends in Computing Sciences (ICTCS)*, Amman, Jordan, IEEE, pp. 116–120, 2017. https://doi.org/10.1109/ictcs.2017.50

[29] N. B. Harikrishnan, R. Vinayakumar and K. P. Soman, "A machine learning approach towards phishing e-mail detection," in *Proc. of the Anti-Phishing Pilot at ACM Int. Workshop on Security and Privacy Analytics (IWSPA AP)*, Amrita School of Engineering, India, vol. 2013, pp. 455–468, 2018. https://doi.org/10.3233/jcs-2010-0371

[30] M. Diale, T. Celik and C. van der Walt, "Unsupervised feature learning for spam email filtering," *Computers & Electrical Engineering*, vol. 74, pp. 89–104, 2019.

[31] S. Srinivasan, V. Ravi, M. Alazab, S. Ketha, A. M. Al-Zoubi *et al.,* "Spam emails detection based on distributed word embedding with deep learning," in *Title of Machine Intelligence and Big Data Analytics for Cybersecurity Applications*, Switzerland: Springer, Cham, vol. 919, pp. 161–189, 2020.

[32] M. Goswami and B. S. Purkayastha, "Discovering patterns using feature selection techniques and correlation," in *Lecture Notes on Data Engineering and Communications Technologies*, pp. 824–831, 2020. https://doi.org/10.1007/978-3-030-38040-3_94

[33] V. Ra, B. G. HBa, A. K. Ma, S. KPa, P. Poornachandran *et al.,* "Deepti-PhishNet: Applying deep neural networks for phishing e-mail detection," in *Proc. of 1st AntiPhishing Shared Pilot 4th ACM Int. Workshop Security Privacy Anal (IWSPA)*, Tempe, AZ, USA, pp. 1–11, 2018. https://doi.org/10.1109/eurosp.2018.00040

[34] K. Liakos, P. Busato, D. Moshou, S. Pearson and D. Bochtis, "Machine learning in agriculture: A review," *Sensors*, vol. 18, no. 8, pp. 2674, 2018.

[35] Q. Yuan, H. Shen, T. Li, Z. Li, S. Li *et al.,* "Deep learning in environmental remote sensing: Achievements and challenges," *Remote Sensing of Environment*, vol. 241, pp. 111716, 2020.

[36] A. Rajkomar, J. Dean and I. Kohane, "Machine learning in medicine," *New England Journal of Medicine*, vol. 380, no. 14, pp. 1347–1358, 2019.

[37] S. Velliangiri and K. K. Kasaraneni, "Machine learning and deep learning in cyber security for IoT," in *ICDSMLA 2019*, pp. 975–981, 2020. https://doi.org/10.1007/978-981-15-1420-3_107

[38] M. A. Haq, "Planetscope nanosatellites image classification using machine learning," *Computer Systems Science and Engineering*, vol. 42, no. 3, pp. 1031–1046, 2022.

[39] M. A. Haq, "CNN based automated weed detection system using UAV imagery," *Computer Systems Science and Engineering*, vol. 42, no. 2, pp. 837–849, 2022.

[40] M. A. Haq, "SMOTEDNN: A novel model for air pollution forecasting and AQI classification," *Computers, Materials & Continua*, vol. 71, no. 1, pp. 1403–1425, 2022.

[41] T. Chakraborty and I. Ghosh, "Real-time forecasts and risk assessment of novel coronavirus (COVID-19) cases: A data-driven analysis," *Chaos, Solitons & Fractals*, vol. 135, pp. 109850, 2020.

[42] T. Hai, M. M. Hameed, H. A. Marhoon, M. Z. Kermani, H. Salim *et al.,* "Groundwater level prediction using machine learning models: A comprehensive review," *Neurocomputing*, vol. 489, pp. 271–308, 2022. https://doi.org/10.1016/j.neucom.2022.03.014

[43] J. Chen, M. Yang and J. Ling, "Attention-based label consistency for semi-supervised deep learning based image classification," *Neurocomputing*, vol. 453, pp. 731–741, 2021.

[44] X. Li, G. Jiang, X. Tang, Y. Zuo, S. Hu *et al.,* "Detecting geothermal anomalies using multi-temporal thermal infrared remote sensing data in the Damxung–Yangbajain Basin, Qinghai–Tibet Plateau," *Remote Sensing*, vol. 15, no. 18, pp. 4473, 2023.

[45] S. Mudi, S. Paramanik, M. D. Behera, A. J. Prakash, N. R. Deep *et al.,* "Moderate resolution LAI prediction using Sentinel-2 satellite data and indirect field measurements in Sikkim Himalaya," *Environmental Monitoring and Assessment*, vol. 194, no. 12, pp. 897, 2022.

[46] P. Gantayat, A. V. Kulkarni and J. Srinivasan, "Estimation of ice thickness using surface velocities and slope: case study at Gangotri Glacier, India," *Journal of Glaciology*, vol. 60, no. 220, pp. 277–282, 2014.

[47] A. Yadav and D. K. Vishwakarma, "Sentiment analysis using deep learning architectures: A review," *Artificial Intelligence Review*, vol. 53, no. 6, pp. 4335–4385, 2020.

[48] A. Kumar, J. Kim, D. Lyndon, M. Fulham and D. Feng, "An ensemble of fine-tuned convolutional neural networks for medical image classification," *IEEE Journal of Biomedical and Health Informatics*, vol. 21, no. 1, pp. 31–40, 2016.

[49] K. Paxton-Fear, D. Hodges and O. Buckley, "Understanding insider threat attacks using natural language processing: Automatically mapping organic narrative reports to existing insider threat frameworks," in *Int. Conf. on Human-Computer Interaction*, pp. 619–636, 2020.

[50] A. A. Cunha, J. B. Borges and A. A. F. Loureiro, "Classification of botnet attacks in IoT using a convolutional neural network," in *Proc. of MSWiM*, Montreal Quebec, Canada, pp. 63–70, 2022.

[51] L. Mohammadpour, T. C. Ling, C. S. Liew and A. Aryanfar, "A survey of CNN-based network intrusion detection," *Applied Sciences*, vol. 12, no. 16, pp. 1–34, 2022.

[52] L. Deng, G. Hinton and B. Kingsbury, "New types of deep neural network learning for speech recognition and related applications: An overview," in *IEEE Int. Conf. on Acoustics, Speech and Signal Processing*, BC, Canada, pp. 8599–8603, 2013. https://doi.org/10.1109/icassp.2013.6639344

[53] G. E. Hinton, S. Osindero and Y. W. Teh, "A fast learning algorithm for deep belief nets," *Neural Computation*, vol. 18, no. 7, pp. 1527–1554, 2006.

[54] R. Salakhutdinov, A. Mnih and G. Hinton, "Restricted boltzmann machines for collaborative filtering," in *Proc. of the 24th Int. Conf. on Machine Learning—ICML '07*, University of Toronto, Canada, pp. 791–798, 2007. https://doi.org/10.1145/1273496.1273596

[55] P. Vincent, H. Larochelle, Y. Bengio and P. A. Manzagol, "Extracting and composing robust features with denoising auto encoders," in *Proc. of the 25th Int. Conf. on Machine Learning—ICML '08, Association for Computing Machinery*, New York NY, United States, Helsinki, Finland, pp. 1096–1003, 2008. https://doi.org/10.1145/1390156.1390294

[56] H. Rao, X. Shi, A. K. Rodrigue, J. Feng, Y. Xia *et al.,* "Feature selection based on artificial bee colony and gradient boosting decision tree," *Applied Soft Computing*, vol. 74, pp. 634–642, 2019.

[57] R. Vinayakumar, K. P. Soman and P. Poornachandran, "Detecting malicious domain names using deep learning approaches at scale," *Journal of Intelligent & Fuzzy Systems*, vol. 34, no. 3, pp. 1355–1367, 2018.

[58] R. Vinayakumar, K. P. Soman and P. Poornachandran, “Evaluating effectiveness of shallow and deep networks to intrusion detection system,” in *Int. Conf. on Advances in Computing, Communications and Informatics (ICACCI)*, Udupi, India, pp. 1282–1289, 2017. https://doi.org/10.1109/icacci.2017.8126018

[59] R. Vinayakumar and K. P. Soman, “DeepMalNet: Evaluating shallow and deep networks for static PE malware detection,” *ICT Express*, vol. 4, no. 4, pp. 255–258, 2018.

[60] V. S. Mohan, R. Vinayakumar, K. P. Soman and P. Poornachandran, “S.P.O.O.F Net: Syntactic patterns for identification of ominous online factors,” in *IEEE Security and Privacy Workshops (SPW)*, San Francisco, CA, USA, pp. 258–263, 2018. https://doi.org/10.1109/spw.2018.00041

[61] N. A. Unnithan, N. B. Harikrishnan, R. Vinayakumar, K. P. Soman and S. Sundarakrishna, “Detecting phishing e-mail using machine learning techniques,” in *Proc. of 1st Anti-Phishing Shared Task Pilot 4th ACM IWSPA Co-Located 8th ACM Conf. on Data Application Security and Privacy (CODASPY)*, Bangalore, India, pp. 51–54, 2018. https://doi.org/10.1145/2557547.2557579

[62] T. Repke and R. Krestel, “Bringing back structure to free text email conversations with recurrent neural networks,” In: G. Pasi, B. Piwowarski, L. Azzopardi and A. Hanbury (Eds.), *Advances in Information Retrieval*, Advances in Information Retrieval. ECIR 2018, vol. 10772, pp. 114–126, Cham: Springer, 2018.

[63] M. Hiransha, N. A. Unnithan, R. Vinayakumar, K. Soman and A. D. R. Verma, “Deep learning-based phishing e-mail detection,” in *Proc. of 1st AntiPhishing Shared Pilot 4th ACM Int. Workshop Secure, Privacy Anal. (IWSPA)*, Tempe, AZ, USA, India, vol. 2124, pp. 16, 2018.

[64] Á. Peris and F. Casacuberta, “NMT-Keras: A very flexible toolkit with a focus on interactive NMT and online learning,” *The Prague Bulletin of Mathematical Linguistics*, vol. 111, no. 1, pp. 113–124, 2018. https://doi.org/10.2478/pralin-2018-0010

[65] J. Zhang and X. Li, “Phishing detection method based on borderline-smote deep belief network,” in *Proc. SpaCCS*, Guangzhou, China, pp. 45–53, 2017.

[66] A. C. Bahnsen, E. C. Bohorquez, S. Villegas, J. Vargas and F. A. Gonzalez, “Classifying phishing URLs using recurrent neural networks,” in *APWG Symp. on Electronic Crime Research (eCrime)*, Scottsdale, AZ, USA, pp. 1–8, 2017. https://doi.org/10.1109/ecrime.2017.7945048

[67] S. Smadi, N. Aslam and L. Zhang, “Detection of online phishing email using dynamic evolving neural network based on reinforcement learning,” *Decision Support Systems*, vol. 107, pp. 88–102, 2018.

[68] C. Xu, P. Zhao, Y. Liu, J. Xu, V. S. S. Sheng *et al.,* “Recurrent convolutional neural network for sequential recommendation,” in *The World Wide Web Conf.*, China, pp. 3398–3404, 2019. https://doi.org/10.1145/3308558.3313408

[69] J. Lee, J. H. Shin and J. S. Kim, “Interactive visualization and manipulation of attention-based neural machine translation,” in *Proc. of the 2017 Conf. on Empirical Methods in Natural Language Processing: System Demonstrations, Association for Computational Linguistics*, Copenhagen, Denmark, pp. 121–126, 2017. https://doi.org/10.18653/v1/d17-2021

[70] Y. Yang, Z. Zhong, T. Shen and Z. Lin, “Convolutional neural networks with alternately updated clique,” in *IEEE/CVF Conf. on Computer Vision and Pattern Recognition, Proc. of the IEEE Conf. on Computer Vision and Pattern Recognition (CVPR)*, Utah, USA, pp. 2413–2422, 2018. https://doi.org/10.1109/cvpr.2018.00256

[71] S. Ding, S. Qu, Y. Xi, A. K. Sangaiah and S. Wan, “Image caption generation with high-level image features,” *Pattern Recognition Letters*, vol. 123, pp. 89–95, 2019. https://doi.org/10.1016/j.patrec.2019.03.021

[72] K. Cho, B. van Merriënboer, C. Gulcehre, D. Bahdanau, F. Bougares *et al.,* “Learning phrase representations using RNN encoder–Decoder for statistical machine translation,” in *Proc. of the 2014 Conf. on Empirical Methods in Natural Language Processing (EMNLP)*, NY, US, vol. 1406, pp. 1078, 2014.

[73] N. Pappas and A. Popescu-Belis, “Human versus machine attention in document classification: A dataset with crowdsourced annotations,” in *Proc. of NLPSM*, Austin, TX, USA, pp. 94–100, 2016.

[74] S. Şentürk, E. Yerli and I. Sogukpinar, “Email phishing detection and prevention by using data mining techniques,” in *Int. Conf. on Computer Science and Engineering (UBMK)*, Antalya, Turkey, pp. 707–712, 2017. https://doi.org/10.1109/ubmk.2017.8093510

[75] D. Brites and M. Wei, "PhishFry—A proactive approach to classify phishing sites using SCIKIT learn," in *Proc. of IEEE GC Workshop*, Waikoloa, HI, USA, pp. 1–6, 2019.

[76] M. Baykara and Z. Z. Gurel, "Detection of phishing attacks," in *6th Int. Symp. on Digital Forensic and Security (ISDFS)*, Menoufia University, Menouf, Egypt, vol. 12, no. 1, pp. 42, 2018.

[77] H. V. Mahesh, "E-mail classification tool to detect phishing using hybrid features," Ph.D. dissertation, University of Moratuwa, Sri Lanka, 2019.

[78] A. Karim, S. Azam, B. Shanmugam, K. Kannoorpatti and M. Alazab, "A comprehensive survey for intelligent spam email detection," *IEEE Access*, vol. 7, pp. 168261–168295, 2019.

[79] R. Vinayakumar, K. P. Soman, P. Poornachandran and S. Sachin Kumar, "Evaluating deep learning approaches to characterize and classify the DGAs at scale," *Journal of Intelligent & Fuzzy Systems*, vol. 34, no. 3, pp. 1265–1276, 2018.

[80] J. Fowler, "Modern e-mail security concerns: Threats to e-mail privacy and privacy solutions," Ph.D. dissertation, Kalamazoo College, USA, 2017.

[81] Y. G. Zeng, "Identifying email threats using predictive analysis," in *Int. Conf. on Cyber Security and Protection of Digital Services (Cyber Security)*, London, UK, pp. 1–2, 2017. https://doi.org/10.1109/cybersecpods.2017.8074848

[82] K. Om, "Secure email gateway," in *IEEE Int. Conf. on Smart Technologies and Management for Computing, Communication, Controls, Energy and Materials (ICSTM)*, Chennai, India, pp. 49–53, 2017. https://doi.org/10.1109/icstm.2017.8089126

[83] M. Vergelis, T. Shcherbakova, T. Sidorina and T. Kulikova, "Spam and phishing in 2018," *Russ*, 2019. [Online]. Available: https://securelist.Ru/spam-and-phishing-in-2018/93453

[84] P. Patel, D. M. Sarno, J. E. Lewis, M. Shoss, M. B. Neider *et al.,* "Perceptual representation of spam and phishing e-mails," *Applied Cognitive Psychology*, vol. 33, no. 6, pp. 1296–1304, 2019.

[85] S. M. Albladi and G. R. S. Weir, "User characteristics that influence judgment of social engineering attacks in social networks," *Human-Centric Computing and Information Sciences*, vol. 8, no. 1, 2018. https://doi.org/10.1186/s13673-018-0128-7

[86] R. Kong, H. Zhu and J. A. Konstan, "Learning to ignore: A case study of organization-wide bulk email effectiveness," in *Proc. of the ACM on Human-Computer Interaction (CSCW1)*, Twin Cities, USA, vol. 5, no. 80, pp. 1–23, 2021.

[87] M. A. Al-Garadi, A. Mohamed, A. K. Al-Ali, X. Du, I. Ali *et al.,* "A survey of machine and deep learning methods for internet of things (IoT) security," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 3, pp. 1646–1685, 2020.

[88] V. Christina, S. Karpagavalli and G. Suganya, "A study on email spam filtering techniques," *International Journal of Computer Applications*, vol. 12, no. 1, pp. 7–9, 2010.

[89] G. Sakkis, I. Androutsopoulos, G. Paliouras, V. Karkaletsis, C. D. Spyropoulos *et al.,* "Stacking classifiers for anti-spam filtering of e-mail," *Information Retrieval*, vol. 6, no. 1, pp. 49–73, 2003.

[90] A. Chavez, "TF-IDF classification based multinomial naïve bayes model for spam filtering," M.S. dissertation, National College of Ireland, Ireland, 2020.

[91] L. Pelletier, J. Almhana and V. Choulaklain, "Adaptive filtering of spam," in *Proc. of Second Annual Conf. on Communication Networks and Services Research*, Frederiction, NB, Canada, pp. 346–345, 2004. https://doi.org/10.1109/dnsr.2004.1344731

[92] S. Seth and S. Biswas, "Multimodal spam classification using deep learning techniques," in *Proc. of SITIS*, Jaipur, India, pp. 346–349, 2017.

[93] P. Sethi, V. Bhandari and B. Kohli, "SMS spam detection and comparison of various machine learning algorithms," in *Proc. of IC3TSN*, Gurgaon, India, pp. 28–31, 2017.

[94] N. A. G. Arachchilage and S. Love, "Security awareness of computer users: A phishing threat avoidance perspective," *Computers in Human Behavior*, vol. 38, pp. 304–312, 2014.

[95] M. Delany, "Domain-based email authentication using public keys advertised in the DNS (DomainKeys)," RFC 4870, 2007. https://doi.org/10.17487/RFC4870

[96] B. Adida, S. Hohenberger and R. L. Rivest, "Fighting phishing attacks: A lightweight trust architecture for detecting spoofed e-mails," In: R. de Prisco and M. Yung (Eds.), *DIMACS Wkshp on Theft in E-Commerce, Lightweight Email Signatures (Extended Abstract)*, vol. 4116, pp. 288–302, Security and Cryptography for Networks. SCN 2005, Berlin, Heidelberg: Springer, 2005.

[97] J. Chen and C. Guo, "Online detection and prevention of phishing attacks," in *First Int. Conf. on Communications and Networking in China*, Beijing, China, pp. 1–7, 2006. https://doi.org/10.1109/chinacom.2006.344718

[98] M. Chandrasekaran, K. Narayanan and S. Upadhyaya, "Phishing e-mail detection based on structural properties," in *NYS Cyber Security Conf., the Handbook of Research on Social and Organizational Liabilities in Information Security*, State University of New York, USA, vol. 3, 2006. https://doi.org/10.4018/978-1-61350-323-2.ch203

[99] A. Azari, J. M. Namayanja, N. Kaur, V. Misal and S. Shukla, "Imbalanced learning in massive phishing datasets," in *Proc. of IEEE HPSC and IEEE IDS*, Baltimore, MD, USA, pp. 127–132, 2020.

[100] X. Yuan, P. He, Q. Zhu and X. Li, "Adversarial examples: Attacks and defenses for deep learning," *IEEE Transactions on Neural Networks and Learning Systems*, vol. 30, no. 9, pp. 2805–2824, 2019.

[101] F. Ubaid, R. Amin, F. B. Ubaid and M. M. Iqbal, "Mitigating address spoofing attacks in hybrid SDN," *International Journal of Advanced Computer Science and Applications*, vol. 8, no. 4, pp. 562–570, 2017.