International Journal of Scientific Research in Computer Science, Engineering and Information Technology

ISSN : 2456-3307 OPEN ACCESS

Available Online at : www.ijsrcseit.com

doi : https://doi.org/10.32628/IJSRCSEIT

An Efficient Approach : Deep Learning Based Model for Adaptive SPAM Detection in IoT Networks

Sunil Kumar[1*], Prof. Neelesh Ray[2]

[1]M Tech Scholar, Computer Science & Engineering, Millennium Institute of Technology and Science, Bhopal, India

[2]Associate Professor, Computer Science & Engineering, Millennium Institute of Technology and Science, Bhopal, India

ARTICLEINFO

Article History:

Accepted: 05 Jan 2024

Published: 30 Jan 2024

Publication Issue

Volume 10, Issue 1

January-February-2024

Page Number

175-186

ABSTRACT

The Spamming is the use of messaging systems to send multiple unsolicited messages (spam) to large numbers of recipients for the purpose of commercial advertising, for the purpose of non-commercial proselytizing, for any prohibited purpose, or simply repeatedly sending the same message to the same user. Internet of Things (IoT) enables convergence and implementations between the real-world objects irrespective of their geographical locations. Implementation of IOT network management and control makes privacy and protection strategies utmost important and challenging in such an environment.

This dissertation presents an adaptive approach based on deep learning for detecting of spam in the IOT network. The CNN-LSTM techniques is applied and optimized for better performance than others. For each topic, the existing problems are analyzed, and then, current solutions to these problems are presented and discussed. The simulation results show that the proposed sentiment analysis method has higher precision, recall and F1 score. The method is proved to be effective with high accuracy. The simulation and analysis are done using the python spider 3.7 software.

The overall accuracy achieved by the proposed work is 94.25 % while previous it is achieved 92.8 %. The error rate of proposed technique is 4.37 % while 8.2 % in existing work. Therefore, it is clear from the simulation results; the proposed work is achieved significant better results than existing work.

Keywords : SPAM, Python, Classification, DL, ML and CNN-LSTM.

I. INTRODUCTION

Internet of Things (IoT) enables convergence and implementations between the real-world objects irrespective of their geographical locations. Implementation of IOT network management and control makes privacy and protection strategies utmost

important and challenging in such an environment. IoT applications need to protect data privacy to fix security issues such as intrusions, spoofing attacks, DoS attacks, DoS attacks, jamming, eavesdropping, spam, and malware.

The safety measures of IoT devices depend upon the size and type of organization in which it is imposed. The behavior of users forces the security gateways to cooperate. In other words, we can say that the location, nature, application of IoT devices decides the security measures. For instance, the smart IoT security cameras in the smart organization can capture the different parameters for analysis and intelligent decision making. The maximum care to be taken is with web based devices as maximum number of IoT devices are web dependent.

It is common at the workplace that the IoT devices installed in an organization can be used to implement security and privacy features efficiently. For example, wearable devices collect and send user's health data to a connected smartphone should prevent leakage of information to ensure privacy. It has been found in the market that 25-30% of working employees connect their personal IoT devices with the organizational network. The expanding nature of IoT attracts both the audience, i.e., the users and the attackers.

However, with the emergence of ML in various attacks scenarios, IoT devices choose a defensive strategy and decide the key parameters in the security protocols for trade-off between security, privacy and computation. This job is challenging as it is usually difficult for an IoT system with limited resources to estimate the current network and timely attack status.

Denial of service (DDoS) attacks: The attackers can flood the target database with unwanted requests to stop IoT devices from having access to various services. These malicious requests produced by a network of IoT devices are commonly known as bots. DDoS can exhaust all the resources provided by the service provider. It can block authentic users and can make the network resource unavailable. These are the attacks imposed at the physical layer of IoT device. This attack leads to lose the integrity of the device. Attackers attempt to modify the data either at the node storage or while it is in the transmission within network. The common attacks possible at the sensor node are attacks on availability, attacks on authenticity, attacks on confidentiality, Cryptography keys brute-forcing. The countermeasures to ensure prevention of such attacks includes password protection, data encryption and restricted access control.

a. Convolutional Neural Network

A Convolutional Neural Network (CNN) with Long Short-Term Memory (LSTM) integration combines the strengths of both architectures for processing sequential and spatial data. CNNs excel at extracting hierarchical features from spatial data, such as images, through convolutional layers that learn local patterns. However, they may struggle with capturing temporal dependencies in sequential data. Integrating LSTM, a type of recurrent neural network (RNN), addresses this limitation by enabling the model to retain and learn from past information over time.

In this hybrid architecture, the CNN's convolutional layers extract spatial features, and the LSTM layers handle sequential dependencies by maintaining a memory of past inputs. This synergy is particularly powerful in tasks where understanding both spatial structures and temporal relationships is crucial, such as video analysis or time-series forecasting. The CNN-LSTM combination has proven effective in various applications, showcasing its versatility in learning complex patterns across different dimensions, making it a valuable tool in areas like computer vision and natural language processing

b. SPAM

The uninvited distribution of communications to a big audience over a variety of different communication channels is what we mean when we talk about spam. These messages might be used for a variety of objectives, including commercial advertising, non-commercial advocacy, criminal operations (particularly phishing fraud), or just delivering the same message several times to the same recipient.

Although junk email is the most widely recognized type of spam, the term also refers to similar abuses that occur in other forms of media, such as blogs, wikis, instant messaging, Usenet newsgroups, web search engines, mobile messaging, internet forums, junk fax transmissions, social media, spam mobile applications, television advertising, and file sharing.

The word "spam" was first used in a Monty Python skit that depicted a restaurant where practically every meal contained Spam and where Vikings harassed diners by continuously yelling "Spam." Quite often, spam will serve as the main course during lunch.

In spite of the efforts that have been made to fight spam, it continues to be a successful business enterprise. This is due to the fact that senders are difficult to hold responsible, and marketers incur little operational expenditures while engaging in spam marketing. These expenses generally consist of the maintenance of email lists, servers, infrastructures, IP ranges, and domain names. While internet service providers have acquired the skills to meet the growing demand for their services, both the public and providers are nevertheless forced to struggle with the expenses associated with decreased productivity and fraud. Legislation to combat spam is now being drafted in several regions of the world in response to the problems described here.

c. TYPES OF SPAM

Email Spam- Email spam, also known as unsolicited bulk email (UBE) or junk mail, is the practice of sending unwanted email messages, sometimes including commercial material, in huge numbers. Other names for email spam include junk mail and spam mail. When the Internet was first opened up for business use in the middle of the 1990s, spam in email was only beginning to emerge as an issue. In the years that followed, its rate of expansion was exponential, and by 2007, a conservative estimate places its share of all emails at between 80 and 85 percent. Pressure applied to

Legislation to make it unlawful to send unsolicited email, sometimes known as spam, has been enacted in certain places, but not so much in others. It would seem that the efforts made by governing bodies, security systems, and email service providers are helping to limit the amount of spam that is sent via email. According to the "2014 Internet Security Threat Report, Volume 19" that was released by Symantec Corporation, the percentage of total email traffic that was comprised of spam decreased to 66%.

The act of collecting email addresses and then selling the resulting databases has given rise to an entire business known as email address harvesting. Some of these methods of address harvesting depend on users not reading the fine print of agreements, which results in users consenting to send messages without discrimination to their contacts since they did not read the small print.

d. Messaging spam-

Spam sent using instant messaging takes advantage of several instant messaging platforms. According to a survey by Ferris Research, even while spam instant messages are less common than their email counterparts, the number of spam IMs sent in 2003 was 500 million, which is twice as high as the level in 2002.

e. Newsgroup Spam and Forum spam-

Usenet newsgroups are the targets of the sort of spam known as "newsgroup spam," which is sometimes known simply as "spam." In point of fact, spamming of Usenet newsgroups occurred long before spamming of email. The conventions of Usenet describe spamming as excessive multiple posting, which refers to the practice of repeatedly publishing the same message or ones that are substantially identical. The pervasiveness of spam on Usenet was the impetus for the creation of the Breitbart Index, which is an objective measurement of the "sameness" of a message.

The practice of posting unsolicited advertisements within discussion forums on the internet is known as "forum spam." Spam is typically generated by automated programs known as spambots. The vast majority of forum spam consists of links to third-party websites. The purpose of these connections is twofold: first, gambling, pornography, real estate, or loans; second, to increase the amount of traffic that goes to

these commercial websites. Some of these links have tracking code that may identify the spambot; if a purchase is made using one of these links, the spammer who is responsible for the spambot will receive a commission.

f. Mobile Phone Spam

The text messaging service of a mobile phone is the target of spam that is sent via mobile phones. Customers may find this particularly aggravating not just because to the annoyance it causes, but also due to the possibility that they will be charged a price for each text message they receive in some regions. SMS messages are now required to give the alternatives of HELP and STOP in order to comply with the CAN-SPAM legislation in the United States. The latter option allows the recipient to terminate any connection with the advertiser via SMS.

Because there is a fee associated with sending an SMS, there has not been as much phone spam as one might expect given the widespread usage of mobile phones. In recent times, there have been reports of spam being sent to mobile phones using push notifications received from browsers. These can occur when users are given the option to receive notifications from harmful websites or websites that serve malicious advertisements.

g. Social Networking Spam-

Even social networking sites like Facebook and Twitter can get messages that include spam links. Hackers get into user accounts and transmit fraudulent links by impersonating the user's trusted connections, such as friends and family. When it comes to Twitter, spammers build their reputation by following verified accounts like Lady Gaga's; when the owner of the verified account follows the spammer back, it legitimizes the spammer. Despite the fact that Twitter uses the broadcast model, in which all tweets from a user are broadcast to all of the person's followers, the company has conducted research to determine what interest structures enable users to get relevant tweets while minimizing their exposure to spam. On social media sites, spammers transmit either undesirable content (or material that is irrelevant to the platform) or false information out of malevolent intent.

h. Spam in blogs

Spamming done on weblogs is referred to as blog spam. This sort of spam took advantage of the open nature of comments in the blogging software Movable sort in 2003. It did this by continually submitting comments to various blog articles that gave nothing more than a link to the spammer's commercial web site. In 2003, this type of spam was very common. Wikis and guestbooks, both of which allow users to contribute content, are frequently the targets of assaults that are quite similar to these. The spamming of a certain tag on websites such as Tumblr is an additional method of spam that may be used in blog comments.

VoIP spam- Voice over Internet Protocol (VoIP) spam is a type of spam that often uses SIP, which stands for the Session Initiation Protocol. This is quite comparable to calls made by telemarketers using standard telephone lines. When the consumer opts to take the spam call, they are often subjected to listening to a prerecorded message or advertising that is part of the spam. This is often easier for the spammer to accomplish due to the fact that VoIP services are inexpensive and simple to anonymize over the internet, and there are several methods for delivering a large number of calls from a single place. It is typically possible to identify accounts or IP addresses that are being used for VoIP spam by seeing a high number of outbound calls, a poor call completion rate, and a short conversation length.

II. RELATED WORK

The Internet of Things (IoT) is a gathering of millions of gadgets having sensors and actuators connected over wired or remote channel for information transmission. IoT has developed quickly over the course of the last 10 years with in excess of 25 billion gadgets expected to be associated by 2020. The volume of information let out of these gadgets will increment many-overlap in the years to come. Notwithstanding an expanded

volume, the IoT gadgets creates a lot of information with various modalities having shifting information quality characterized by its speed regarding time and position reliance. In such a climate, machine learning (ML) calculations can assume a significant part in guaranteeing security and approval in light of biotechnology, strange location to work on the ease of use, and security of IoT frameworks. Then again, attackers frequently view learning calculations to take advantage of the weaknesses in shrewd IoT-based frameworks. Persuaded from these, in this article, we propose the security of the IoT gadgets by distinguishing spam utilizing ML. To accomplish this goal, Spam Recognition in IoT utilizing Machine Learning system is proposed. In this structure, five ML models are assessed utilizing different measurements with a huge assortment of data sources highlights sets. Each model figures a spam score by thinking about the refined information highlights. This score portrays the reliability of IoT gadget under different boundaries. REFIT Shrewd Home informational collection is utilized for the approval of proposed method. The outcomes acquired demonstrate the viability of the proposed plot in contrast with the other existing plans. Spam and non-spam email recognizable proof are one of the most difficult assignments for both email specialist co-ops and customers. The spammers attempt to spread deceiving realities through aggravating messages by standing out for client. A few spam recognizable proof models have recently been proposed and tried however the recorded precision has shown that further work toward this path is expected to accomplish further developed exactness, low preparation time, and less blunder rate. In this examination work, we have proposed a model that groups the email into spam and ham. DBSCAN and Seclusion Backwoods are utilized to distinguish the outrageous qualities beyond the particular reach. Heatmap, Recursive Element Disposal, and Chi-Square component determination procedures are utilized to choose the compelling highlights. The proposed model is carried out in both machine learning and deep learning to lay out a relative examination. Multinomial Gullible Bayes (MNB), Arbitrary Woodland (RF), K-Closest Neighbor (KNN), Slope Supporting (GB) are utilized to present troupe technique in machine learning execution. Repetitive Brain Organization (RNN), Angle Plunge (GD), Counterfeit Brain Organization (ANN) for deep learning execution. An outfit technique is developed to consolidate different classifiers' result. The troupe techniques permit creating better forecast exactness contrasted with a solitary classifier. Our proposed model acquired a precision of 100 percent, AUC=100, MSE mistake = 0 and RMSE blunder = 0 for machine learning execution and exactness of close to 100%, misfortune value= 0.0165 for deep learning execution in view of an email spam base dataset gathered from the UCI machine learning archive.

In present day time, Mental Internet of Things (CIoT) related to IoT develops which gives the knowledge force of detecting and calculation for cutting edge IoT (Nx-IoT) organizations. The information researchers have found a lot of strategies for information revelation from handled information in CIoT. This assignment is achieved effectively and information continues for additional handling. The significant reason for the disappointment of IoT gadgets is because of the attacks, where web spam is more noticeable. There appears to be a necessity of a method which can distinguish the web spam before it goes into a gadget. Propelled from these issues, in this work, Mental spammer system (CSF) for web spam identification is proposed. CSF distinguishes the web spam by fluffy rule based classifiers alongside machine learning classifiers. Every classifier creates the quality score of the website page. These quality scores are then ensembled to produce a solitary score, which
predicts the spamicity of the site page. For ensembling, fluffy democratic methodology is utilized in CSF. The trials were performed utilizing standard dataset WEBSPAM-UK 2007 as for exactness and above created. From the outcomes got, it has been exhibited

that CSF works on the precision by 97.3%, which is relatively high in contrast with the other existing methodologies in writing.

The motivation behind the following internet of things (IoT) is that of making accessible heap of administrations to individuals by high detecting smart gadgets equipped for thinking and continuous acting. The combination of IoT and multi-specialist frameworks (MAS) gives the chance to profit from the social disposition of specialists to perform machine-to-machine (M2M) collaboration among shrewd substances. Notwithstanding, the determination of dependable accomplices for participation addresses a hard errand in a portable and united setting, particularly in light of the fact that the dependability of gadgets is generally unreferenced. The issues examined above can be blended by reviewing the notable idea of social strength in IoT frameworks, i.e., the capacity of an IoT organization to oppose to potential attacks by noxious specialist that possibly could taint huge region of the organization, spamming untrustworthy data and/or accepting out of line ways of behaving. In this sense, social flexibility is given to confront pernicious exercises of programming specialists in their social collaborations, and don't manage the right working of the sensors and other data gadgets. Here, the utilization of a standing model can be a practicable and successful answer for structure neighborhood networks of specialists based on their social capacities. In this work, we propose a system for specialists working in an IoT climate, called ResIoT, where the development of networks for cooperative designs is performed based on specialist notoriety. To approve our methodology, we played out an exploratory mission through a recreated system, which permitted us to check that, by our methodology, gadgets have no financial comfort to performs deluding ways of behaving. Besides, further exploratory outcomes have shown that our methodology can recognize the idea of the dynamic specialists in the frameworks (i.e., legitimate and malevolent) , with an exactness of at the very least 11 % contrasted with the best contender tried and featuring a high flexibility concerning a few noxious exercises.

The developing interest in the different interpersonal organization stages prompts gigantic number of connections between various clients from one side of the planet to the other. These limitless connections give a reasonable climate to spammers to spread as the intricacy of the informal communities increments. Programmed identification of such noxious clients inside this horde of perplexing cooperation's is perhaps the most troublesome exploration issue. Various methodologies have been taken on to battle against pernicious exercises. Among the different promising methodologies is the one depending on utilizing diagram investigation procedures. In this work, we recommend two portrayal models for social collaboration's chart based datasets. The portrayal models are basically evolved in light of breaking down connections and relations between clients. The primary model is created in view of diagram based examination, while the other one is created in light of successive handling of client cooperations. In view of the led tests, we reason that the two portrayal models show high spam recognition precision. In any case, chart based examination models produce higher precision levels contrasted with those delivered by cooperation arrangements handling models.

lately, insider dangers inside PCs have been congesting in light of the fact that a high amount of malware and its variations have been spread greatly by spam mail, advertising attack, and clients' lack of regard. Besides, a portion of the lethargic malware wouldn't be investigated by insect infection programming, and the gamble exists constantly until at last turning into a grievous monetary misfortune. A few examinations created signature-based techniques to recognize insider dangers, yet we are more inspired by how to improve on the organization conduct from refined traffic stream. Without reviewing network payload and parcel with tedious, we center around the traffic conduct that we just think about the highlights of source IP, objective IP, timestamp of association, and

amount of association. To vanquish the black box of convoluted network traffic, this work applies the deep learning worldview and proposes the variation form of VGG16 to look at the elements inside traffic stream. At last, this work proposes a strategy to help more clarification on traffic conduct with learning model.

III.PROPOSED METHODOLOGY

To collect SPAM dataset from kaggle website. To implement proposed approach based on deep learning technique. To improve the performance of Spam Detection in IoT using proposed technique. To simulate proposed method on spyder python 3.7 software. To enhance the performance of overall prediction result. Steps

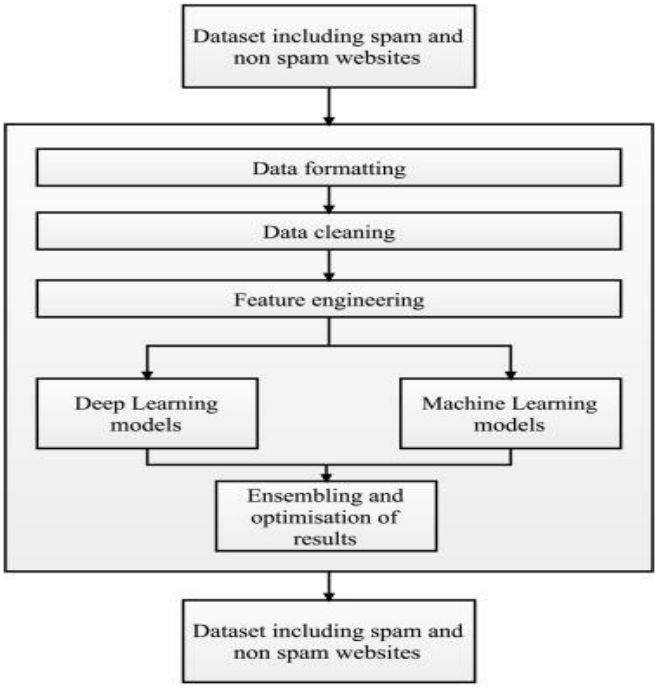


Figure 1. Flow Chart

Steps-

- Firstly, download the SPAM dataset from kaggle website, which is a large dataset provider and machine learning repository Provider Company for research.
- Now apply the preprocessing of the data, here handing the missing data, removal nullvalues.
- Now extract the data features and evaluate in dependent and independent variable.
- Now apply the classification method based on the deep learning recurrent neural network and long term short memory (CNN-LSTM).
- Now generate confusion matrix and show all predicted class like true positive, false positive, true negative and false negative.
- Now calculate the performance parameters by using the standard formulas in terms of the precision, recall, F_measure, accuracy and error rate.

IV.RESULT AND ANALYSIS

It is an interpreter, raised level, comprehensively helpful programming language. Made by Guido van Rossum and first delivered in 1991, Python's plan reasoning stresses code clarity with its famous utilization of critical whitespace. Its language builds and article organized philosophy hope to help developers with forming clear, genuine code for little and colossal scale projects.

Python is continuously made and garbage accumulated. It upholds various programming ideal models, including procedural, object-organized, and utilitarian programming. Python is frequently depicted as a "batteries included" language on account of its exhaustive standard library.

Python was considered in the last part of the 1980s as a replacement to the ABC language. Python 2.0, delivered in 2000, introduced highlights like rundown perceptions and a junk arrangement framework prepared for social event reference cycles. Python 3.0, delivered in 2008, was a critical correction of the language that isn't absolutely in reverse great, and much Python 2 code doesn't run unmodified on Python 3.

The Python 2 language, for instance Python 2.7.x, was authoritatively suspended on 1 January 2020 (first prepared for 2015) after which security patches and various upgrades will not be delivered for it. With

Python 2's completion of-life, just Python 3.5.x and later are upheld.

Python translators are open for some working frameworks. An overall organization of software engineers creates and keeps up with CPython, an open source reference execution. A non-benefit affiliation, the Python Programming Foundation, oversees and coordinates assets for Python and CPython improvement.

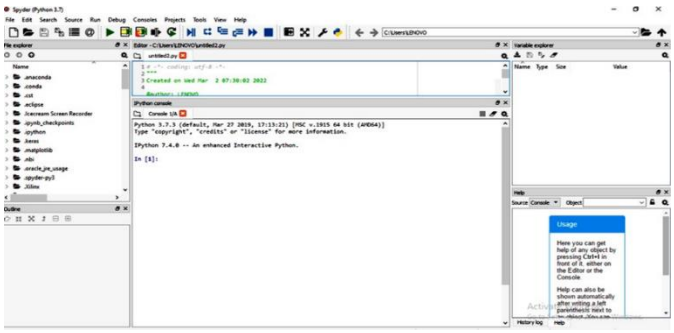


Figure 1: IDE on Python

Figure 5.17 is presenting various IOT devices total count with the month format. The month consider from the jan to dec.

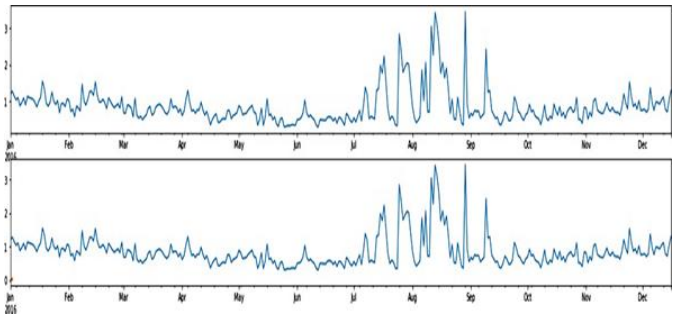


Figure 2: Training

Figure 2 is presenting the training of the IOT devices. It consider from the month of jan to end of the dec.

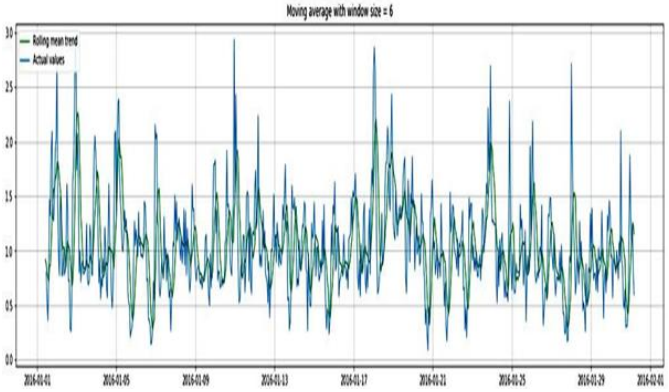


Figure 3: Moving size 6

Figure is 3 is showing actual and the average value the moving average window size 6.

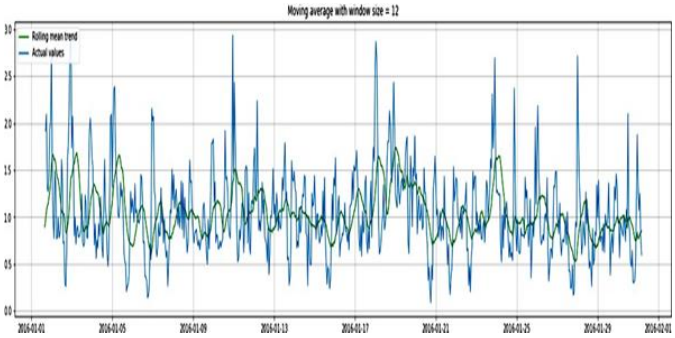


Figure 4: Moving size 12

Figure is 4 is showing actual and the average value during the moving average window size 12.

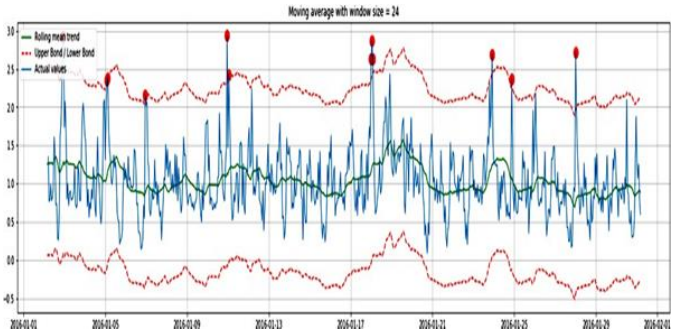
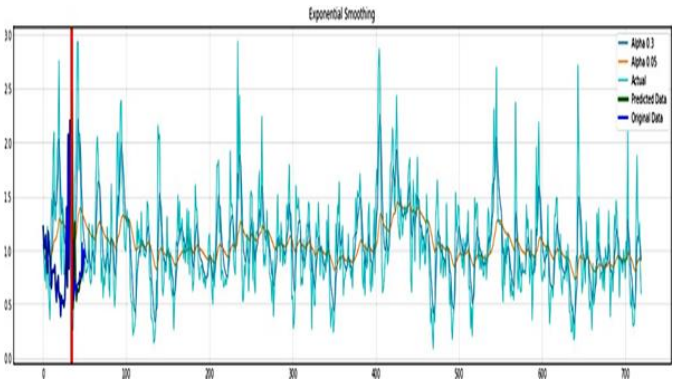


Figure 5 : Moving size 24

Figure is 5 is showing actual and the average value during the moving average window size 24. The upper and lower bond range is also mentioned.



6: Exponential Smoothing

Figure is 6 is showing exponential smoothing. The various values like original data, actual data and the predicated data values are shown.

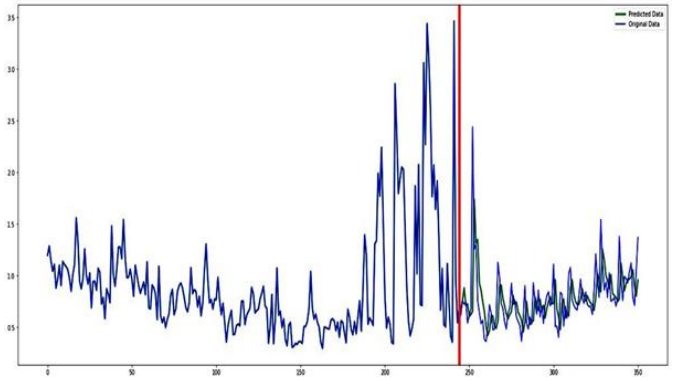


Figure 7 : Predicted and actual data

Figure is 7 is showing predicted and actual data from the given dataset. It is clear from the result graph; the most of the data is predicted.

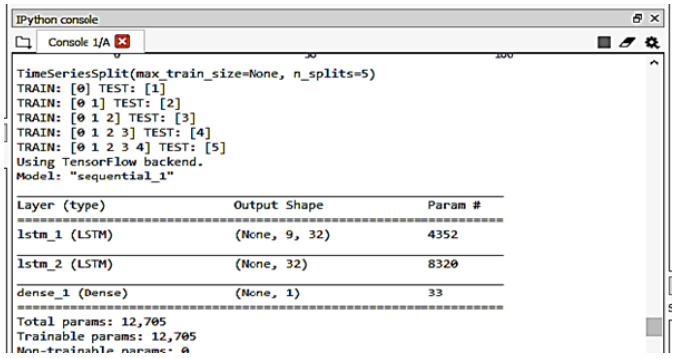


Figure 8 : Process in python

Figure is 8 is showing internal process, which shows in the python console. The long term short memory (LSTM) method applied for the classification of this dataset.

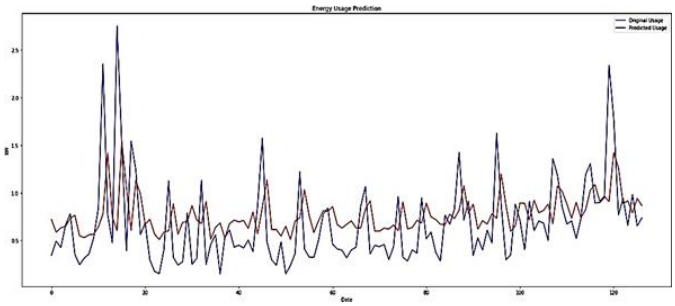


Figure 9: Energy Prediction

Figure is 9 is showing energy prediction. The original and predicted energy is shown in the graphical form.

Table 1 : Simulation Results

Sr. No.	Parameter Name	Value
1	Method	Deep Learning (CNN-LSTM)
2	Accuracy	94.25 %
3	Classification error	4.37 %
4	MSE	0.076%
5	Memory	100 MB

Table 1 is showing the simulation results of the proposed technique. The overall accuracy is 94.25% with 4.28% error rate.

Table 2: Result Comparison

Sr. No.	Parameters	Previous Work [1]	Proposed Work
1	Technique	Machine Learning (Linear Model)	Deep Learning (CNN-LSTM)
2	Accuracy	92.8%	94.25 %
3	Classification Error	8.2 %	4.37 %

Figure 2 is showing the result comparison of the previous and proposed work. The overall accuracy

achieved by the proposed work is 94.25 % while previous it is achieved 92.8 %. The error rate of proposed technique is 4.37 % while 8.2 % in existing work. Therefore it is clear from the simulation results; the proposed work is achieved significant better results thanexisting work.

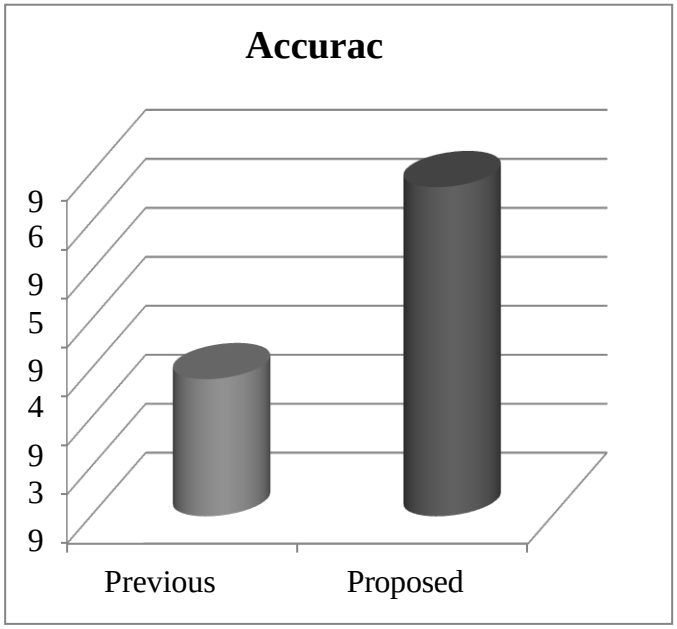


Figure 5.26 : Accuracy Result graph

Figure 5.26 is presenting the simulation results graph of the accuracy. The proposed work achieved better accuracy then existing work.

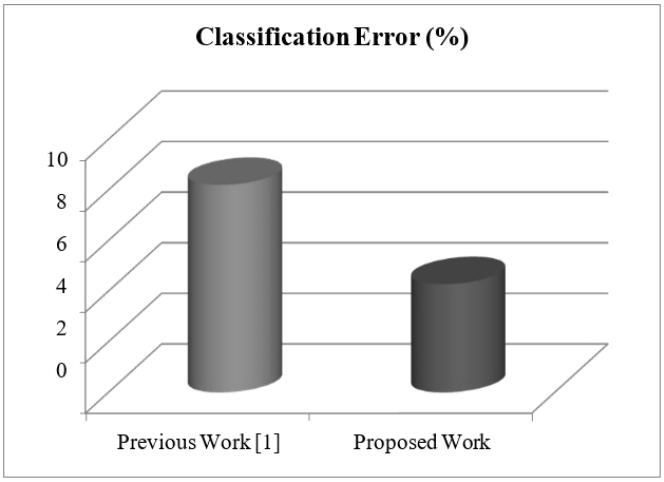


Figure 5.27: Classification Error

Figure 5.27 is presenting the simulation results graph of the classification error. The proposed work achieved better accuracy then existing work.

V. CONCLUSION AND FUTURE WORK

Anything that has a sensor attached to it and can transmit data from one object to another or to people with the help of internet is known as an IoT device. The IoT devices include wireless sensors, software, actuators, computer devices and more. There are several top devices in the market. Smart Mobiles, smart refrigerators, smart watches, smart fire alarms, smart door locks, smart bicycles, medical sensors, fitness trackers, smart security system, etc., are few examples of IoT products. Security in IoT is the act of securing Internet devices and the networks they're connected to from threats and breaches by protecting, identifying, and monitoring risks all while helping fix vulnerabilities from a range of devices that can pose security risks to your business. Hardware, software and connectivity will all need to be secure for IoT objects to work effectively. Without security for IoT, any connected object, from refrigerators to manufacturing bots, can be hacked. Once hackers gain control, they can usurp the object's functionality and steal the user's digital data.

The proposed framework, detects the spam parameters of IoT devices using deep learning models. The IoT dataset used for simulation is pre-processed by using feature engineering procedure. By simulation the framework with deep learning models, each IoT appliance is awarded with a spam score. This refines the conditions to be taken for successful working of IoT devices in a smart home.

This dissertation presents an adaptive spam detection technique for IOT devices using deep learning technique. The simulation is performed using Python spyder environment, simulated results shows that the overall accuracy achieved by the proposed work is 94.25 % while previous it is achieved 92.8 %. The error rate of proposed technique is 4.37 % while 8.2 % in existing work. Therefore it is clear from the simulation results; the proposed work is achieved significant better results than existing work.

In future, according to Mordor Intelligence, the IoT technology market value is expected to rise to $1.39 trillion by 2026. This incredible growth is likely due to a number of factors: The COVID-19 pandemic accelerated the advancement of remote monitoring, smart home devices, and data analysis solutions. IoT allows businesses and people to be more connected to the world around them, and to do more meaningful, higher-level work.

VI. REFERENCES

[1]. A. Makkar, S. Garg, N. Kumar, M. S. Hossain, A. Ghoneim and M. Alrashoud, "An Efficient Spam Detection Technique for IoT Devices Using Machine Learning," in IEEE Transactions on Industrial Informatics, vol. 17, no. 2, pp. 903-912, Feb. 2021, doi: 10.1109/TII.2020.2968927.

[2]. F. Hossain, M. N. Uddin and R. K. Halder, "Analysis of Optimized Machine Learning and Deep Learning Techniques for Spam Detection," 2021 IEEE International IOT, Electronics and Mechatronics Conference (IEMTRONICS), 2021, pp. 1-7, doi: 10.1109/IEMTRONICS52119.2021.9422508.

[3]. A. Makkar, U. Ghosh, P. K. Sharma and A. Javed, "A Fuzzy-based approach to Enhance Cyber Defence Security for Next-generation IoT," in IEEE Internet of Things Journal, doi: 10.1109/JIOT.2021.3053326.

[4]. G. Fortino, F. Messina, D. Rosaci and G. M. L. Sarne, "ResIoT: An IoT social framework resilient to malicious activities," in IEEE/CAA Journal of Automatica Sinica, vol. 7, no. 5, pp. 1263-1278, September 2020, doi: 10.1109/JAS.2020.1003330.

[5]. K. A. Al-Thelaya, T. S. Al-Nethary and E. Y. Ramadan, "Social Networks Spam Detection Using Graph-Based Features Analysis and Sequence of Interactions Between Users," 2020 IEEE International Conference on Informatics, IoT, and Enabling Technologies (ICIoT), 2020, pp. 206-211, doi: 10.1109/ICIoT48696.2020.9089509.

[6]. T. Y. Ho, W. Chen, M. Sun and C. Huang, "Visualizing the Malicious of Your Network Traffic by Explained Deep Learning," 2020 International Conference on Artificial Intelligence in Information and Communication (ICAIIC), 2020, pp. 687- 692, doi: 10.1109/ICAIIC48513.2020.9065247.

[7]. J. Zhang, Q. Yan and M. Wang, "Evasion Attacks Based on Wasserstein Generative Adversarial Network," 2019 Computing, Communications and IoT Applications (ComComAp), 2019, pp. 454-459, doi: 10.1109/ComComAp46287.2019.9018647.

[8]. A. Makkar, N. Kumar and M. Guizani, "The Power of AI in IoT : Cognitive IoT- based Scheme for Web Spam Detection," 2019 IEEE Symposium Series on

[9]. Computational Intelligence (SSCI), 2019, pp. 3132-3138, doi: 10.1109/SSCI44817.2019.9002885.

[10]. A. K. Singh, S. Bhushan and S. Vij, "Filtering spam messages and mails using fuzzy C means algorithm," 2019 4th International Conference on Internet of Things: Smart Innovation and Usages (IoT-SIU), 2019, pp. 1-5, doi: 10.1109/IoT-SIU.2019.8777483.

[11]. T. Lange and H. Kettani, "On Security Threats of Botnets to Cyber Systems," 2019 6th International Conference on Signal Processing and Integrated Networks (SPIN), 2019, pp. 176-183, doi: 10.1109/SPIN.2019.8711780.

[12]. T. Qiu, H. Wang, K. Li, H. Ning, A. K. Sangaiah and B. Chen, "SIGMM: A Novel Machine Learning Algorithm for Spammer Identification in Industrial Mobile Cloud Computing," in IEEE Transactions on Industrial Informatics, vol. 15, no. 4, pp. 2349-2359, April 2019, doi: 10.1109/TII.2018.2799907.

[13]. G. Kumar and V. Rishiwal, "Statistical Analysis of Tweeter Data Using Language Model With KLD," 2018 3rd International Conference On Internet of Things: Smart Innovation and Usages (IoT-SIU), 2018, pp. 1-6, doi: 10.1109/IoT- SIU.2018.8519938.

[14]. E. Anthi, L. Williams and P. Burnap, "Pulse: An adaptive intrusion detection for the Internet of Things," Living in the Internet of Things: Cybersecurity of the IoT - 2018, 2018, pp. 1-4, doi: 10.1049/cp.2018.0035.

[15]. A. Kaushik and S. Talati, "Securing IoT using layer characterstics," 2017 3rd International Conference on Applied and Theoretical Computing and Communication Technology (iCATccT), 2017, pp. 290-298, doi: 10.1109/ICATCCT.2017.8389150.

[16]. İ. Ü. Oğul, C. Özcan and Ö. Hakdağlı, "Fast text classification with Naive Bayes method on Apache Spark," 2017 25th Signal Processing and Communications Applications Conference (SIU), 2017, pp. 1-4, doi: 10.1109/SIU.2017.7960721.

[17]. Z. Lv, J. Lloret, H. Song, J. Shen and W. Mazurczyk, "Guest Editorial: Secure Communications Over the Internet of Artificially Intelligent Things," in IEEE Internet of Things Magazine, vol. 5, no. 1, pp. 58-60, March 2022, doi: 10.1109/MIOT.2022.9773087.

[18]. B. W. Khoueiry and M. R. Soleymani, "A Novel Machine-to-Machine Communication Strategy Using Rateless Coding for the Internet of Things," in IEEE

[19]. Internet of Things Journal, vol. 3, no. 6, pp. 937-950, Dec. 2016, doi: 10.1109/JIOT.2016.2518925.

[20]. J. S. Jang, Y. L. Kim and J. H. Park, "A study on the optimization of the uplink period using machine learning in the future IoT network," 2016 IEEE International Conference on Pervasive Computing and Communication Workshops (PerCom Workshops), 2016, pp. 1-3, doi: 10.1109/PERCOMW.2016.7457131.

[21]. M. Condoluci, G. Araniti, T. Mahmoodi and M. Dohler, "Enabling the IoT Machine Age With 5G: Machine-Type Multicast Services for Innovative Real-Time Applications," in IEEE Access, vol. 4, pp. 5555-5569, 2016, doi: 10.1109/ACCESS.2016.2573678.

[22]. R. K. Deore, V. R. Sonawane and P. H. Satpute, "Internet of Thing Based Home Appliances Control," 2015 International Conference on Computational Intelligence and Communication Networks (CICN), 2015, pp. 898-902, doi: 10.1109/CICN.2015.177.

[23]. V. Selis and A. Marshall, "MEDA: A machine emulation detection algorithm," 2015 12th International Joint Conference on e-Business and Telecommunications (ICETE), 2015, pp. 228-235.

[24]. D. Singh, G. Tripathi and A. Jara, "Secure layers based architecture for Internet of Things," 2015 IEEE 2nd World Forum on Internet of Things (WF-IoT), 2015, pp. 321-326, doi: 10.1109/WF-IoT.2015.7389074.

[25]. R. Parada, J. Melià-Seguí, A. Carreras, M. Morenza-Cinos and R. Pous, "Measuring user-object interactions in IoT spaces," 2015 IEEE International Conference on RFID Technology and Applications (RFID-TA), 2015, pp. 52-58, doi: 10.1109/RFID- TA.2015.7379797.

[26]. V. P. Kafle, Y. Fukushima and H. Harai, "ID-based communication for realizing IoT and M2M in future heterogeneous mobile networks," 2015 International Conference on Recent Advances in Internet of Things (RIoT), 2015, pp. 1-6, doi: 10.1109/RIOT.2015.7104908.

[27]. S. Cirani, M. Picone, P. Gonizzi, L. Veltri and G. Ferrari, "IoT-OAS: An OAuth- Based Authorization Service Architecture for Secure Services in IoT Scenarios," in IEEE Sensors Journal, vol. 15, no. 2, pp. 1224-1234, Feb. 2015, doi: 10.1109/JSEN.2014.2361406.

Cite this article as :

Sunil Kumar, Prof. Neelesh Ray, "An Efficient Approach : Deep Learning Based Model for Adaptive SPAM Detection in IoT Networks", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 10, Issue 1, pp.175-186, January-February-2024.