Artificial Intelligence in Computer Network Technology in The Big Data Era

Priyameet Kaur Keer
Department of Management Studies.
New Horizon College Of Engg.
Bangalore, India
priyameetkeer@gmail.com

Jehan Kadhim shareef Al-safi
Department of Digital Media
University of Thi-Qar.
Iraq
jihansh2020@gmail.com

S B G Tilak Babu
Dept of ECE
Aditya Engineering College
Surampalem, Andhra Pradesh, India
thilaksayila@gmail.com

G.Ramesh
St. Martin's Engineering College,
Secunderabad, Telangana, India
grrams786@gmail.com

2022 5th International Conference on Contemporary Computing and Informatics (IC3I) | 979-8-3503-9826-7/22/$31.00 ©2022 IEEE | DOI: 10.1109/IC3I56241.2022.10073024

Abstract—**While the integration of artificial intelligence and computer technology has enriched people's daily lives, it has also become an inaccessible part of people's lives. The trend of future social development is the advancement of computer network technology, which will be the tendency of future social development. Because of the artificial intelligence technology's high level of intelligence, it has emerged as one of the most promising technologies in the realm of computer networks and is dependent on computers for its development, which led to the establishment of the technology-based development. In order to hasten the incorporation of artificial intelligence into social production and living, as well as to make production and life easier, we need to make some changes. The purpose of this study was to investigate artificial intelligence, after which the model structure of intelligent anti-spam in network security management was established, and finally, the model was evaluated. According to the findings, the intelligent anti-spam model exhibited satisfactory filtering performance.**

Keywords—Artificial, Intelligence, Computer, Network, Intelligent.

I. INTRODUCTION

The human intelligence technology realizes the simulated application of multiple human organs and limbs through machine vision, machine human body, and other technologies to make machines and equipment work more accurately and standardized; for example, driverless vehicles, mapping and surveying remote sensing technology, and so on. The field of artificial intelligence has already seen a great deal of research and implementation. The proliferation of computers and the Internet has led to the collection of massive volumes of data across a variety of sectors, which may be used to reliably forecast and assess particular outcomes. Since we now live in the era of big data, one of the most pressing problems in the discipline of computer science is figuring out how to give AI technology a more prominent place in the industry. The field of artificial intelligence has already seen extensive research and implementation. Simultaneously, with the proliferation of computer network technology and Internet technology, massive amounts of data occur in various sectors, and this data can accurately forecast and evaluate certain events. Information storage, transmission, and management are all made easier with the advent of contemporary network technology, which has spurred the rapid expansion of networks on a global scale. Economic growth and the security of this data's owner make it a valuable asset. Modern communication networks create ideal settings for exchanging data. Additionally, it serves as a development environment. People can get the data they need from the Internet if they use the right information platform and approach. However, due to technical flaws, thieves frequently steal intellectual property, such as patent copyrights and scholarly articles. The victims' interests have been severely damaged, and there have been financial repercussions as a result. As a result, the country places a premium on network information security efforts, and protecting networks is now a top priority. However, the work does not come close to satisfying information security needs through associated network management. Because of this, it's crucial to get rid of dangers from their roots. Verifying the methods, security, and authenticity of the information using conventional information processing is infeasible. The information cannot be adequately identified because it is formulated for integration [1]-[3].

II. LITERATURE REVIEW

Hao Hong Artificial intelligence and other forms of information technology have seen widespread use in the networking industry since the dawn of the information era. It is a powerful tool for enhancing the security and control of data networks. Especially with the rapid development of Internet technology, the volume of information in computer network is expanding. Whenever a computer network is in use, a massive volume of data is gathered. The usefulness of a big data information network is distinct from that of big data infrastructure and AI technologies, though. Big data and AI allow us to quickly collect massive amounts of data and then parse out the most relevant insights. This paper provides a concise overview of the qualities and uses of big data and AI in the context of a digital infrastructure[4].

Deyong Jiang, in the age of big data networks, advances in computing and information technology are happening at a breakneck pace. The country and certain significant corporations have increased their research on artificial intelligence technology in response to the rapid development of big data network technology. The paper begins with a brief introduction to both big data and AI, and then proceeds to an examination of AI's defining features and technological benefits. Moreover, this study analyses the use of AI in computer networks from the perspectives of network security, system evaluation, and network security management, with the goal of proposing a reference method for the enhanced implementation of AI in this field. As a byproduct of its findings, this research can help advance both AI and CN as fields of study and application [5].

Xiujuan Xian with the advancement of science and innovation, the underlying capacities of computer network innovation, for example, information activity and word meaning understanding, have been not able to satisfy the genuine requirements of current clients. The advancement of computer network innovation into something more sympathetic and intelligent appears to be undeniable as of now. Artificial intelligence permits computers to accomplish more modern work recently held for people, saving additional time and expanding efficiency. At the same time, it may help individuals take advantage of smarter services, advance scientific and technological progress, and foster social progress over the long haul. Consequently, this paper elaborates on the use of AI in computer network technology, educating readers and laying the groundwork for future advances in AI.

Donnie Sheng Cheng China's artificial intelligence research and development has taken a giant leap forward thanks to the country's booming economy and cutting-edge scientific and technological advancements. The reasonable application of AI technology is a crucial part of the management and operation of today's computer networks; it contributes to the security and reliability of the networks themselves, achieves the goal of scientific and efficient processing of the massive amounts of data generated by the networks themselves, and helps the information society as a whole grow steadily and sustainably. Against the backdrop of big data, this article will examine and debate the use of AI in computer networks in further detail.

Yang Lin Recent years have seen tremendous progress in science and technology, leading to an explosion in the volume and variety of data available online and ushering in the era of big data for modern civilization. The vast economic, social, and scientific potential of big data has captured the interest of professionals from every industry. The study of big data has attracted the attention of many academics. Changed lifestyles, improved quality of life, and progress toward AI are all results of advances in computer network technology. When used to computer network technology, artificial intelligence increases its efficiency and effectiveness. This article uses AI in the context of the big data era as its study object, delving into the field's potential applications to computer network technology. It should serve as a useful point of reference for future work in this area.

III. Design Of An Intelligent E-Mail Anti-Spam System

- *Anti-spam email system flow*

The Linux platform firewall formed the foundation of the anti-spam email system used in this research. The intelligent firewall can be used to block unwanted messages like spam e-mails, web pages, and even texts. In this research, we focused solely on spam email screening. The system took an email's data package as it travelled through the network, evaluated it, and then determined what the email was about. Discarding an email is necessary when its contents contain debauchery. Figure 1 depicts the full procedure[6]-[10].

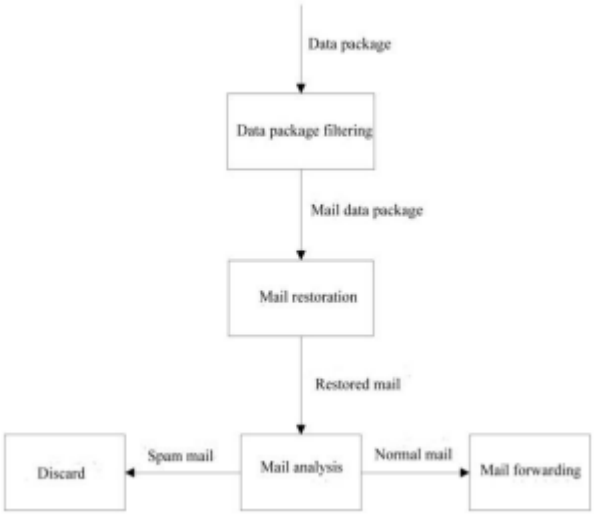

Figure 1: The anti-spam email system's workflow

- *Email protocol examination*

The two modes of operation for the Simple Mail Transfer Protocol (SMTP) [14] are sending and receiving. The detailed procedure looked like this. When the client used TCP port 25 on the SMTP server, the connection was established (TCP). The client first sent HELO to the server, revealing its location, and then followed it up with MAIL, revealing its intended recipient's identity. After the server received the command, it responded with an OK and got ready to receive. RCPT was sent by the client. If the server can accept email, it should indicate so. After some back and forth, DATA was used to send out an email. The ending QUIT was chosen in the end. Table 1 displays the detailed results of executing some commands[11]-[12].

Table 1. List Of Pertinent SMTP Commands

SMTP command	Implicationsofcommands
HELO	Client sends the command toestablish connection with SMTPserverandsendsE-mailaddressto SMTPserver
MAIL	ClientsendsthenameofaddressertoSMTPserver
RCPT	ClientsendsthenameofreceivertoSMTPserver

DATA	ClientsendsmailcontenttoSMTPserver
QUIT	Terminating the connectionbetweenclientandSMTPserver afterreceivingtheresponseofOKreplied bySMTP.

Mail center Convention Adaptation 3 (POP3) is principally used to work with client-side controller of server-side email stockpiling and recovery. Coming up next is the itemized working idea. The client laid out a TCP association with the server at port 110, and afterward conveyed the client's mail client name and secret phrase (Client and PASS) to the POP3 server for validation. Then, at that point, it requested that the server send a few measurements (utilizing Detail), showed the quantity of messages put away on the server (utilizing Rundown), and received some mail (utilizing RETR). After that DELE was utilized to check erased messages via the post office server. The QUIT order was then conveyed to for all time eradicate the "erased" organizer's items[13].

TABLE II. LIST OF PERTINENT POP3 COMMANDS

POP3 command	Implicationsofcommands
USER	Processingusername
PASS	Processinguserpassword
STAT	Requestservertosendstatistical dataaboutmailboxsuchasnumberofmailsand totalnumberofbytes
LIST	Sendingbackthenumberofmailsandthesizeof eachmail.
RETR	Sending back all the texts of e-mailswith parameteridentifier
DELE	Labelingmailswithparameteridentifierasdeleted
QUIT	Deletemailswithlabelsinserver andquit.

- *Plan of capturing, redirection and reclamation of email*

Prior to endeavoring to capture spam messages, it is critical to accumulate the substance of the actual messages. Port 25 of SMTP or port 110 of POP3 was observed to get information bundle and pertinent orders were broke down to get significant data, for example, shipper, collector, text content, and connection as messages in view of SMTP and POP3 were laid out on TCP association and imparted utilizing important convention port. Different handling rules were applied to the recovered spaces to refine them.

The framework executed a Snare capability to deal with mail information bundles in the Forward hub, with the handling activity designed as NF-Line, considering redirection of these messages. To change from bit mode to client mode, IP information bundles with matching source and objective port numbers were embedded into Netfilter line. To sweeten the deal even further, all information bundles, barring the letter information bundle, were sent with next to no limitations. While the matching measures were met interestingly, the data set matching strategy ended. After information handling, the right bundles were shipped off the network, while the erroneous ones were abandoned.

Preceding reestablishing IP-based email messages, it is important to reassemble any IP information bundle sections that might have been lost during reinforcement or move. The part mark field recovered from the header and the degenerate was at first used to lay out in the event that an IP information bundle had been divided. IP information bundles were put away utilizing the sk buff configuration in the event that fracture was demonstrated. Arranged after the sk buff information structure, this is where we conceived our information being put away. The data pointer was situated toward the start of the text. The current part's area comparative with any remaining information bundle pieces not entirely set in stone. The information bundle was checked to check whether the pieces showed up together. Every one of the pieces were assembled back to recuperate the email in the event that it wasn't, or monitored. Email and different types of intelligent substance were at last re-established through convention and the information stream among source and beneficiary[14].

- *Bayesian classification algorithm*

From what should be visible in Figure 2, apparently a Bayesian characterization framework was utilized to settle on the choice on spam email. One of the most remarkable enemy of spam email arrangements accessible today is a factual calculation in view of Bayesian guidelines. The consolidation of the brain network procedure likewise gives it the possibility to learn all alone. By looking at the recurrence of similar expressions in the recently gotten spam messages and substantial messages, we had the option to lay out whether there were spam words and whether an email was spam.

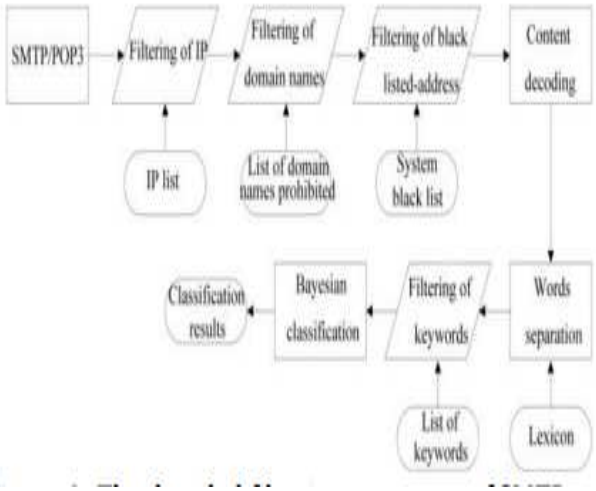

Figure 2: The specific filters used by SMTP and POP3

$$a(w) = \frac{\text{Number of spam e - mails containing word } w}{\text{Number of all spam e – mails}} \quad (1)$$

$$b(w)=\frac{\text{Number of non-spam e-mails containing word } w}{\text{Number of all spam e-mails}} \quad (2)$$

This leads us to the formula for determining the likelihood that an e-mail containing a given word is spam:

$$c(w)=\frac{a(w)}{a(w)+b(w)} \quad (3)$$

In the new, superior algorithm,

$$S=C^{-1}(-2\ln\prod_{\omega} d(w),2z) \quad (4)$$

where C-1() stands for the inverse chi-squared function. To determine the likelihood that an e-mail was not spam, (1-f(w)) might be substituted for f(w). Consequently, the likelihood that an e-mail was spam was:

$$Q=\frac{1+S-P}{2} \quad (5)$$

As a result of all the calculations, a conclusion has been reached. The email was classified as spam if the score was very near to 0. Assuming the final tally was somewhat close to 1, the message was classified as not spam. If the final tally was about 0.5, then the verdict was ambiguous.

IV. RESULTS

In order to simulate a real-world scenario for testing purposes, a system acting as a gateway was linked to a mail server, a mail sender, and a mail receiver via an interaction machine.

A total of 500, 1000, 1500, and 2000 spam emails were sent to the recipient in the first round of testing, and a similar number of non-spam emails were sent in the second.

Test Outcomes Table 3 displays the results of identifying spam and non-spam emails.

Table 3 shows that the rate at which genuine messages were recognized was a lot higher than the rate at which spam messages were distinguished; the rate at which genuine messages were recognized rose consistently, while the rate at which spam messages were distinguished rose and fell couple with the quantity of spam messages got. The more limited the ID season of the two kinds of messages, the quicker the ID speed is probably going to be; the recognizable proof speed of spam messages is high when the quantity of messages is little, and the ID speed of non-spam messages is high when the quantity of messages is enormous[15].

TABLE III. RESULTS OF THE IDENTIFICATION

Identification results		Number of e-mails			
		500	1000	1500	2000
Identification degree(%)	Spame-mail	93.0	92.1	94.0	93.3
	Non-spame-mail	97.9	98.1	99.0	99.4
Identification time(ms)	Spame-mail	540.9	532.4	529.9	528.3
	Non-spame-mail	541.8	533.0	529.0	520.9

V. CONCLUSION

We owe the development of AI to advances in computing, networking, and information theory. In the context of today's big data era, when data growth is exponential, approaches that can handle massive amounts of data efficiently and effectively are essential. The introduction of AI provides a viable solution to the issue of limited information processing capacity at the present time. Information security is a prerequisite for the quick processing of information by artificial intelligence. The anti-spam e-mail system was developed in this research after a thorough examination of important theories in artificial intelligence. The Bayesian method was used to filter the emails once they were gathered from the mail server by intercepting, rerouting, and recovering data packages from the SMTP and POP3 ports. Based on the test findings, it appears that the system can successfully identify spam emails and block them from reaching their intended recipients. It is clear that incorporating AI into computer network technology has the potential to not only address issues like security and data response times plaguing today's networks, but also to further societal progress.

REFERENCES

[1] Hao Hong (2021),” Analyze the Application of Big Data and Artificial Intelligence Technology in Computer Network”, Atlantis Highlights in Intelligent System

[2] Deyong Jiang (2021),” Application of Artificial Intelligence in Computer Network Technology in big data era”,

[3] Xiujuan Tian (2019),” Application of Artificial Intelligence in Computer Network Technology”, Francis Academic Press

[4] DongSheng Cheng (2019),” Application of Ai Technology in Computer Network under Big Data Environment”, Frontiers in Educational Research

[5] Lin Yang (2018),” Research on Application of Artificial Intelligence Based on Big Data Background in Computer Network Technology”, IOP Conf. Series: Materials Science and Engineering

[6] S B G Tilak Babu and Ch Srinivasa Rao, "An optimized technique for copy–move forgery localization using statistical features", ICT Express, Volume 8, Issue 2, Pages 244-249, 2022.

[7] S B G Tilak Babu and Ch Srinivasa Rao, "Efficient detection of copy-move forgery using polar complex exponential transform and gradient direction pattern" , Multimed Tools Appl (2022). https://doi.org/10.1007/s11042-022-12311-6

[8] Kumar, S., Yadav, R., Kaushik, P., Babu, S. T., Dubey, R. K., & Subramanian, "Effective Cyber Security Using IoT to Prevent E-Threats and Hacking During Covid-19." International Journal of Electrical and Electronics Research, pp 111-116, 2022.

[9] S. Demigha, “Big Data Technologies: A Practical Application for Higher Education,” icickm, proceedings of the 17th International Conference on Intellectual Capital, Knowledge Management and

Organsational Learning, pp. 151-157, 2020, DOI: 10.34190/EKM.20.005.

[10] A Dhiraj, M. Minelli, and M. Chambers, “Big Data, Big Analytics: Emerging Business Intelligence and Analytic Trends for Today's Businesses Paperback,” – 1 January 2013, Wiley series.

[11] Han H , Terzenidis N , Syrivelis D , et al. Energy-Proportional Data Center Network Architecture Through OS, Switch and Laser Co-design. arXiveprints, 2021.

[12] Papa panagiotou, Vasileios, Diou C , Delopoulos A . Self-Supervised Feature Learning of 1D Convolutional Neural Networks with Contrastive Loss Using In-Ear Microphone Audio for Eating Detection. 2021.

[13] Kunwar, V., Agarwal, N., Rana, A., Pandey, J.P. (2018). Load Balancing in Cloud—A Systematic Review. In: Aggarwal, V., Bhatnagar, V., Mishra, D. (eds) Big Data Analytics. Advances in Intelligent Systems and Computing, vol 654. Springer, Singapore. https://doi.org/10.1007/978-981-10-6620-7_56.

[14] H. Walia, A. Rana and V. Kansal, "A Naïve Bayes Approach for working on Gurmukhi Word Sense Disambiguation," 2017 6th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO), Noida, India, 2017, pp. 432-435, doi: 10.1109/ICRITO.2017.8342465.

[15] Priyanka Chawla, Inderveer Chana, Ajay Rana, Cloud-based automatic test data generation framework, Journal of Computer and System Sciences, Volume 82, Issue 5, 2016, Pages 712-738, ISSN 0022-0000, https://doi.org/10.1016/j.jcss.2015.12.001.