International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 10 Issue: 11
DOI: https://doi.org/10.17762/ijritcc.v10i11.5781
***Article Received**: 28 August 2022 **Revised**: 07 October 2022 **Accepted**: 21 October 2022*

Stability and Effective Process Control for Secure Email Filtering

Yashaswini A R[1], Shruthi N[2], Nandini S R[3], Santhosh B J[4], Namitha A R[5], K. R. Swetha[6]
[1]Assistant Professor, Dept. of CSE
Maharaja Institute of Technology, Mysore, Karntaka, India.
e-mail: yashugowdaar@gmail.com
[2]Assistant Professor, Dept. of ISE
JSS Science and Technology, Mysur, Karntaka, India.
e-mail: shruthin@jssstuniv.in
[3]Assistant Professor, Dept of CSE
BGS institute of technology, Adichunchanagiri university, B G Nagar, Karnataka, India.
e-mail: nandu.may25@gmail.com
[4]Assistant Professor, Dept of CSE
BGS institute of technology, Adichunchanagiri university, B G Nagar, Karnataka, India.
e-mail: santhoshbj221@gmail.com
[5]Assistant Professor, Dept of CSE
BGS institute of technology, Adichunchanagiri university, B G Nagar, Karnataka, India.
e-mail: namigowdaar@gmail.com
[6]Assistant Professor, Dept of CSE
BGS institute of technology, Adichunchanagiri university, B G Nagar, Karnataka, India.
e-mail: swethagowdha@gmail.com
Corresponding Author: K. R. Swetha, *e-mail:* swethagowdha@gmail.com

Abstract— A fantastic tool for both commercial and personal communication is electronic mail. It has increasingly become a necessary component of our working life since it is straightforward, available, and simple to use. Spam emails have started to tarnish internet experiences and threaten the integrity of email. Due to the exponential growth of spam, both people and organisations are under a great deal of financial and other strain. In order to prevent the future of email itself from being in jeopardy, a solution to the spam problem must be discovered. There is an urgent need to solve the Email spam issue since spam volume has been rising over the last several decades. As part of this effort, many effects of spam emails on businesses and people were noted and thoroughly examined. In order to properly assess current technologies, solutions, and methods, a comprehensive literature review was conducted throughout the procedures. The goals of this work is to develop new methodologies for the implementation of new strategies for the efficient management of email spam and to construct a proof-of-concept software system for the Process controlled assessment of such strategies.

Keywords- Process control, Spamdoop, Stability, Big-Data, Email, Filter, Virus, Web, File system.

I. INTRODUCTION

New and emerging information sources such as web-based media, location data generated by mobile phones and other roaming devices as well as public data available on the web, and information from sensors implanted in cars, buildings, and other objects are all part of the "Big Data" movement. Data volume and size determine the possible insights and value of big data, which may be expressed in the overall amount of data stored [1]. The bulk of contemporary company now runs on electronic mail (E-mail), which has also become a popular means of inter-personal contact for linked individuals. Due to its ease of use, low cost, and support for only immediate transmission, email is very popular. Additionally, it enables users to maintain a conversation log. Over time, email has completely changed how people interact. The Radicati Group predicts that by the end of 2016, there will be more than 4.3 billion email accounts globally, up from the estimated 3.3 billion accounts in 2012. The amount of undesired email messages (mainly spam email) that are received each year is rising dramatically as a result of the increased usage of electronic mail for communication, according to Sara Radicati. The spam issue, which initially emerged in the first decade of the twenty-first century, is still a concern today. According to the Symantec research, 63.7 percent of spam was sent globally

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 10 Issue: 11
DOI: https://doi.org/10.17762/ijritcc.v10i11.5781
***Article Received**: 28 August 2022 **Revised**: 07 October 2022 **Accepted**: 21 October 2022*

in July 2014. Spam emails often come as rapid, time-varying, high-volume data streams that silently adapt to any countermeasures. In a dynamic context with rapid changes, accurate categorization of these data streams is a significant difficulty. Here, it's crucial to emphasise that not every unsolicited email is offensive. In truth, these emails often have very legitimate uses, including invitations to begin new collaborations, to attend conferences or seminars, to volunteer as referees or reviewers, to get permitted alerts or restraints from one's own company or other chosen agencies. Similar scenarios might arise if a university uses moderated list services to communicate with the students enrolled in certain courses and programmes [2]. These uses of email technology, even when uninvited, are entirely legal. Therefore, emails that do not fit into the categories of solicited emails and unsolicited but appropriate emails of the sort indicated above are the main source of the issue. Spam is what we refer to as these unwanted emails, therefore a fair Process control over spam is what we want to accomplish with the suggested study. This study focuses on the investigation and creation of dependable, trustworthy, and user-friendly computer systems and methods. People who examine the data's usefulness might benefit from a wide range of data types and characteristics. Data fusion is a common technique used by Big Data to cover up missing parts of information, such as photos, text, audio, and video files. To meet the difficulties and demands of the growth route and also the development, the speed with which the data is created and managed is critical. Big data is usually present in real time[3]. Big data's inconsistency might obstruct the path to effective management. The accuracy of a research may be affected by the quality of the data gathered. In [4], a new, universal approach for email message protection is shown and labelled. In comparison to the prior work, the revolutionary model architecture is more nave and casual to use. In addition, they chose a model that is readily assailable, preventing users from designing and executing several complex processes in order to achieve email security. Unauthorized access to email may be prevented and users' internal privacy protected by using the new strategies shown in this study. Because of this, inventors may identify structural design more freely without interoperability. The cloud is becoming equipped with secure methods for analysing large amounts of data. Secure Distributed File System (SDFS) is used to read a safe record in a cloud specialised co-op. Using a hash of the safe document's name, a hashed record name is obtained, metadata for the protected document is discovered using the hashed record name, a sharing strategy identification is recovered from the metadata, and consent to decode the safe record is obtained from an external substance[5]. Using the sharing strategy identifier, we can extract a security key and encoded record names from the metadata, as well as mention at least one scrambled information document that forms the safe document from a public cloud specialist organization's hub. We can also recover plaintext data for the safe document by decrypting and reassembling the at least one encoded data document.

II. LITERATURE SURVEY

Gary Thuerk, a marketer for Digital Equipment Corporation (DEC), directly delivered the first spam mail. On May 1, 1978, he sent a message to around 400 people on the ARPANET in an effort to draw attention to their product presentation of the DECSYSTEM 2060, and 2060T systems. E-mail chains were first established in 1982, and a new kind of spam for multi-user interactive environments (MUDs) started in 1989. Up until 1993, these spam emails were bearable. Spammers first began utilising computers to send spam in 1994 rather than doing it by hand [6]. In 1994, Canter and Siegel were the first significant spammers. They had published what was known as "Green Card Spam," a message on US immigration law and the Green Card lottery. The incident involving the unintentional usage of USENet for mass email on March 31, 1993, was the first occurrence that was scientifically verified. Unknowingly, Richard Depew had submitted close to 200 duplicate posts to a newsgroup. The first significant spam was USENet-based bulk mail, which was introduced on January 18, 1994. Many newsgroups have received it as religious messages announcing the imminent return of Jesus. It had generated a lot of discussion and contention. Clarence Thomas, the person who submitted it, was subjected to a barrage of inquiries but escaped with just a light penalty. Nigerian spam was the other significant kind [7]. The Nigerian government was irritated by it since it began about 2000 and caused a lot of unwanted press. Later years saw the ongoing emergence of several variations of these schemes. Email fraud refers to mails that lure us into sending big sums of money and thereafter seek for our bank account information as well as frauds that force us to give over our various credit card or bank account information. One of the most well-known and well-known money laundering schemes is the Nigerian scam [20]. Here, a government official receives an email from an unknown sender who identifies himself as a government official, a recipient's family, or a representative of a rich dead person. They may ask for money under false pretences in certain circumstances and promise to pay it back soon. Using a sharable document level key, systems and approaches are able to access information records [21]. Workgroup keys and the exceptional data associated with the information document are both used to construct the sharable record level key. Using a Secure Parser, the sharable record level key may be used to encode and split data. It is also possible to share information in frameworks and strategies without having to duplicate it on the end-system [22]. user's Information is encoded and split across

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 10 Issue: 11
DOI: https://doi.org/10.17762/ijritcc.v10i11.5781
***Article Received**: 28 August 2022 **Revised**: 07 October 2022 **Accepted**: 21 October 2022*

an outside/purchaser organisation and an undertaking/maker organisation. In order to offer the end customers of the outside/purchaser organisation access to the information, a figurative image was generated by a worker in the endeavor/maker organisation and sent out to them. It's possible that these preloaded records will reveal clues about the data encoded and divided [8]. A client of the external/customer organisation does not have to enter or replicate information on the endeavor/maker network in order to access the information. A system and technique for dealing with network metadata are shown. The personality of an organization's metadata and how it is shown to clients of the data it conveys may be managed by gradually starting up executable programming modules that decide on strategy-based choices. The information for an organisation may be sorted by type, and each subclass within a type can be defined by a unique mark esteem [9]. The unique fingerprint value might be used to coordinate with the organization's metadata subclasses against essential strategies and change rules.. One of NetFlow's epitome innovations for layout-based organisation metadata is its ability to monitor network traffic for obscure formats and catch format definitions, as well as to provide recommendations to chairmen about layouts for which custom approaches and transformation rules are not yet available. Shift modules are able to successfully change over selected kinds or subclasses of organisation metadata into elective metadata designs[6]. Exemplifications of the present advancement may the authenticity of approaching bundles of organisation information and dispose of twisted or improper communications. Exemplifications are also capable of continuously analysing and channelling approaching bundles of organisation metadata to identify relevant parts of their data content and divide or course various floods of approaching organisation metadata for different preparation in the current creation's handling motor. Be aware of the possibility to reduce yield metadata traffic by deleting particular messages or selecting surges of message based measures that can be developed by an administrator and determined during the early evaluation of coming messages. There are two ways to approach this: either on a long-term basis or for a short period of time due to special circumstances in the business. An organisation leader, for example, may focus on network metadata in the framework that is created by the edge devices in the company to investigate possible interruptions. For the most part, an information investigation framework obtains all of the limits associated with an assembly office. Memory-inhabitant stockpiling based on the majority of assembling limits is the initial continuous knowledge that the framework identifies from numerous information sources. The vast bulk of sources of knowledge are concerned with the assembly line. Data from a wide range of sources is collected and stored in a distributed capacity based on the majority of assembler boundaries in a massive information investigation framework. Building up a collection of sensitive information, sorting information, and separating and separating the sensitive information from the rest of the information is the method for obtaining information [10]. The sorted data is stored in a separate location (locally on a PC or on another PC in a LAN or WAN or on the Internet.) Perhaps a manual will be written. Both the channel and the guide are subject to destruction or storage. The information entered, deleted, and the remaining part of the data may be wiped from the PC when it is first started. The use of encryption to improve security is conceivable (counting moves of information, channel and guide). It is permitted to recreate the information in the context of a predetermined exceptional status. To enable a majority of comparing, recreated thoughts on the plaintext with a majority of uncommon status (discarding higher security words). A PC-readable media holding programming rules and a data-handling framework is encasing it. Fridrich demonstrates a method for encrypting images to hide data and messages. It is revealed in Fridrich '483 that it is possible to insert an advanced square image with an unknown number of dark levels into a picture transporter. Scrambled using a chaotic Baker map, this enigmatic image initially appears [11]. The resulting image is a random jumble of pixels with randomly dispersed dark levels and no apparent spatial relationships. Two-fold in dimension (height and breadth, or 2n2m), this enigmatic image has 256 layers of darkness. A numerical equation alters the depiction of the transporter. outlines a strategy for disseminating and repurposing data. Components of a field or a computational architecture are used to describe the data to be delivered or stored. Using these N characters of data, each of these n-piece chunks has m characters of information. Lines 37–46 in column one. It is used to adjust non-critical failure stockpiling in a split or appropriated memory framework to the use of this framework Remaking data is done by dispersing data into n pieces with the purpose that any m pieces will do. Different parts of the memory accumulating media are used to store the various bits[12]. The data is recreated using at least m components in a complex numerical procedure. An apparatus for handling records, such as those containing singular and plural words, is disclosed by Masuichi and coworkers. The apparatus also includes means for removing words from books and storing word extraction programmes, as well as a capacity vehicle for transporting the word extraction programmes [13]. Calculations are used to connect the meanings of words that have been deleted. The document's task list is based on the extricated terms and related words. According to Humes, the Internet may be used to filter out offending websites by using a PC structure and method that separates text content from Web pages that have

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 10 Issue: 11
DOI: https://doi.org/10.17762/ijritcc.v10i11.5781
***Article Received**: 28 August 2022 **Revised**: 07 October 2022 **Accepted**: 21 October 2022*

been downloaded over the Internet. reveals a strategy for managing sensitive data. When sensitive information is stored on many PC frameworks, a framework chairman is unable to access it. Questions from a client's terminal are encrypted using two codes one for an identity data set and the other for a data set for accessing specific information[14]. Identifier data is sent from the source terminal of the client to the main PC. Data from a client's ID and trusted status is checked by the main PC/identifier data set before a second inner ID is added to the information bundle/question. The information access data set (the following PC) is then introduced to the altered inquiry and, if the client's source terminal is trusted, the response to the information query is delivered back to the client.

III. LANGUAGE DESIGN

Java programming was created by Sun Microsystems Limited, under the direction of James Gosling, and introduced as a key element of Sun Microsystems' Java platform in 1995. (Java 1.0 [J2SE]). Newest Java Standard Edition "SE 8" version. Because of Java's growth and widespread acclaim, several configurations have been put together to adorn various kinds of networking systems. Figure.1 shows the JVM architecture. For example, J2EE is used for enterprise applications, whereas J2ME is used for mobile ones. Java SE, Java ME, and Java EE are the new names for the revolutionary J2 versions, which are guaranteed to be Mark Once, Run Anywhere.

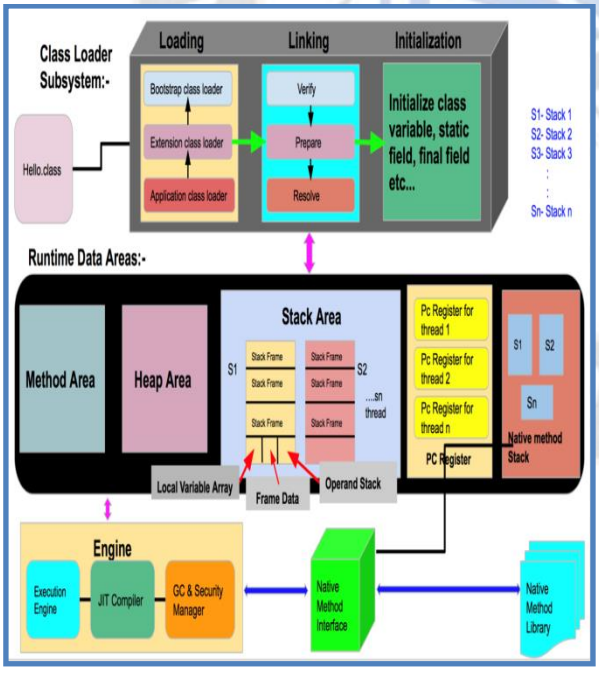

Figure 1: JVM architecture.

When describing the virtual machine, it's said to be an instance of software that runs on the actual machine system. WORA (Write Once, Executed Anywhere) is the general concept for Java, which is often run on a virtual machine [15]. The compiler assembles the files of Java into a Java.class file, and then the class file is loaded and executed by the JVM. In the figure above, you can see the JVM's overall schematic architecture.

IV. BIG DATA SYSTEM DESIGN

A set of Actors and Use Cases participating in the process are shown in Use Case diagrams, which show the relationships and desires that exist between them. It is also important to note that Use Case Diagrams are designed to facilitate the statement with the system's future users and customers as well as to assist establish the system's requirements[16]. Use Case Diagrams depict how well a system performs as well as any functional blocks that aren't being used.

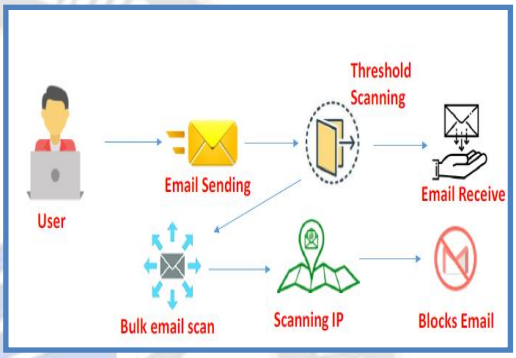

Figure 2: System Design

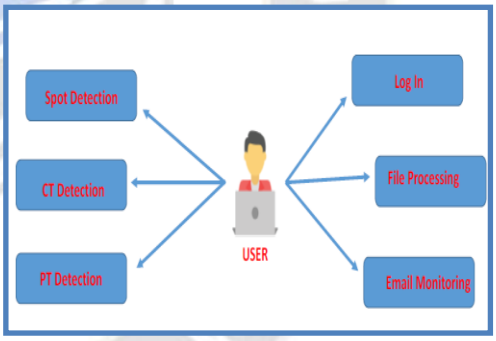

Figure 3: Usecase Flow Diagram

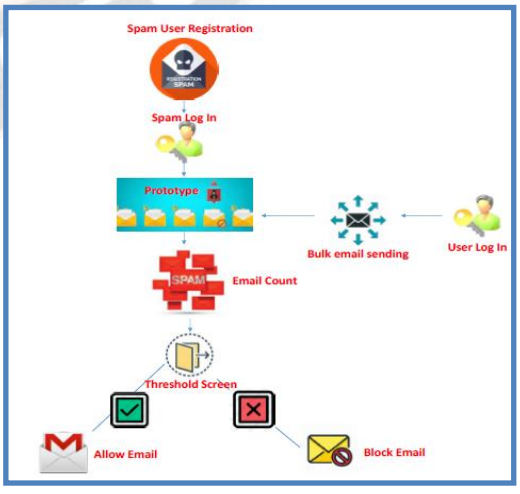

Figure 4: Activity Diagram.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 10 Issue: 11
DOI: https://doi.org/10.17762/ijritcc.v10i11.5781
***Article Received**: 28 August 2022 **Revised**: 07 October 2022 **Accepted**: 21 October 2022*

An Action Diagram is a visual representation of how exercises are arranged in a framework using Activities. System design and Usecase Flow diagram is depicted in Figure.2 and 3 respectively. A single step forward in a conversation is what we call an Activity [17]. It is a condition of being in which there is internal action and a certain amount of active progress. In the case that an exercise has a variety of circumstances, it may also have many active progresses. In terms of visual representation, the Class Diagram serves as the foundational building block. In addition to illustrating the application's purpose theoretically, it is also used to demonstrate how the models are translated into computer code[18]. In addition, class outlines may be used to present information. One of the primary purposes of class overview diagrams is to help students see how various components of their applications work together to create the final product[19]. These classes are discussed in situations with three parts in the class diagrams. The name of the class is shown in the top portion. The characteristics of the class may be found in the middle of the page. The activity diagram is presented in Figure.4. Students may use the class's approaches and exercises as a starting point in this section. Schematic representation of Class Diagram is shown in Figure.5.

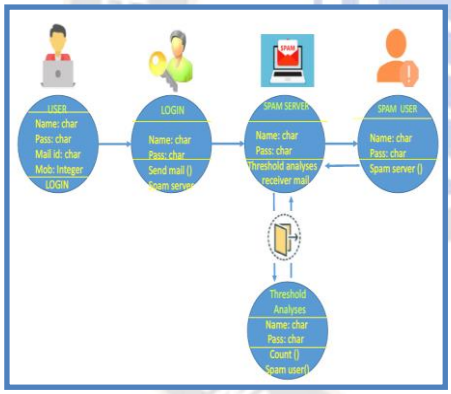

Figure5: Schematic representation of Class Diagram.

V. RESULTS AND DISCUSSION

Spamdoop uses this section to send and receive messages, scan the sender's email address, and then permanently ban the spammer's email address. As a result, any additional messages that fall under the user's threshold will be allowed into the user's email account. The goal of testing is to uncover errors. The only way to ensure that a piece of work has no flaws or shortcomings is to put it through rigorous testing. However, it isn't a method for testing the utility of various segments, sub congregations, gathers and even a finished product. It's a method for putting programming skills into practise in order to make certain that the Software framework meets its requirements and meets the needs of its customers without failing. Different types of tests exist. Each sort of exam has a certain goal in mind. Unit testing is the process of conducting experiments to ensure that the program's internal logic is operating properly and that the program's inputs are resulting in a valid output. Branches of choice and the internal code stream should all be accepted. It is a test of the application's component programming units. When an individual unit is completed, it is mixed with other units. Underlying testing that relies on and is intrusive is what we're dealing with here. Testing at the segment level, unit tests look for flaws in a specific business transaction, application, or even framework architecture. It is the responsibility of unit tests to ensure that every unusual method of business contact functions according to the documented details and comprises clearly defined inputs and expected consequences. The purpose of doing integration tests is to determine whether or not the various pieces of code that make up a programme really work together as a single unit. Testing is more concerned with the outcome of screens or fields than it is with the process itself. Unit testing shows that even if parts were separately fulfilled, coordination tests show that the combination of segments is correct and dependable. Finding the problems that result from combining segments is the aim of incorporation testing. The majority of functional tests provide a methodical proof that the tested capabilities were there, which is supported by technical and organisational requirements such system documentation and user guides. Functional tests are organised and prepared around essentials, vital capabilities, or one-of-a-kind experiments. In addition, testing should take into account systematic inclusion pertaining to recognising Business measure streams; information fields, specified measurements, and progressive cycles. Utilitarian testing must be completed before any more tests are discovered or the value of present tests is determined. It is essential to ensure that the whole coordinated programming architecture fits the requirements of the test. It's everything but a set-up that ensures predictable results. The Spam Detection and Identification is depicted in Figure.6. The framework reconciliation test is an example of framework testing. System testing also relies on depictions and streams of data, highlighting pre-driven cycles and integration points.

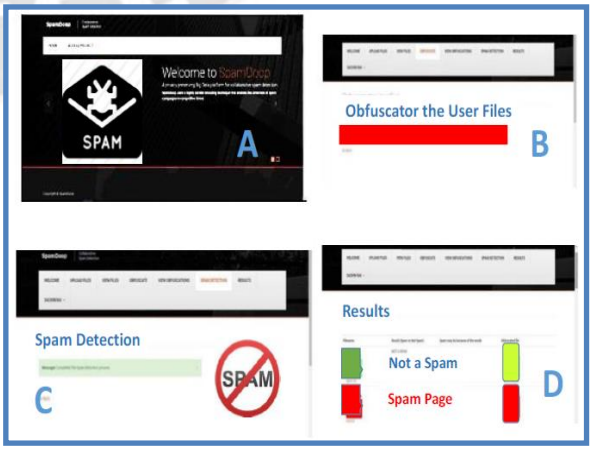

Figure 6: Spam Detection and Identification

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 10 Issue: 11
DOI: https://doi.org/10.17762/ijritcc.v10i11.5781
***Article Received**: 28 August 2022 **Revised**: 07 October 2022 **Accepted**: 21 October 2022*

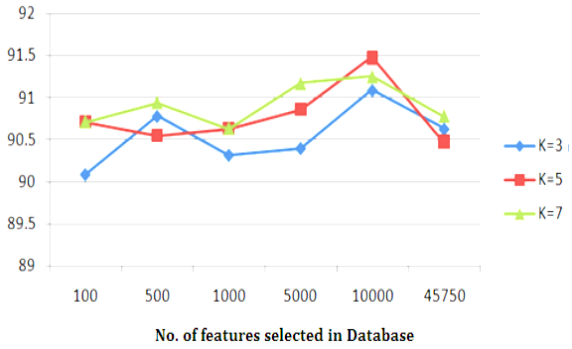

Figure 7: Number of Features with Corresponding Accuracy

Here is a look at the spamdoop: (A) depicts the homepage (B) displays the Obfuscator Screen and its results (C) displays the snapshot of spam detection page (D) demonstrates the snapshot of the results page with comprehensive documentation of spam and no spam messages. The study utilized the Enron dataset. The 5172 email entries in this dataset are all either considered spam or junk mail. The supplied Enron dataset was divided into two independent datasets, one for training and one for testing, using a self-developed tool. For every three records selected for the training dataset, this software selects one record for the test dataset. The quantity of false positives generated by the findings is also reported by this software. Figure 7 displays accuracy information for different k values. Utilizing boosting by giving the global model greater weight and the local models equal weight might be an effective modification. In this study, both a parallel and a sequential version were used. Comparing the MapReduce version to the centralised (one huge machine) version, the training model time is drastically reduced. The accuracy of LibSVM was discovered to be on the lower side (in relation to the default value). All datasets, local models, and their related accuracy are shown in Figure 8.

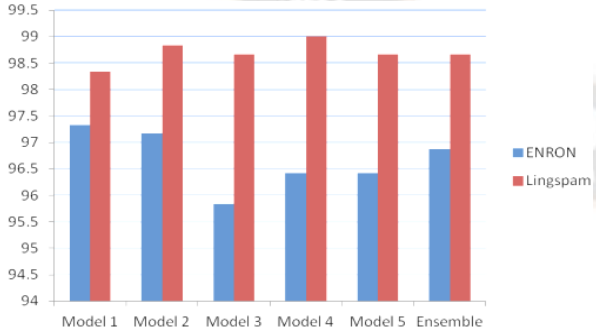

Figure 8: Accuracy and Local Models for All Datasets

The suggested work is a hybrid technique of SVM and Decision tree to categories emails into various categories Spam, valid, and likelihood in an effort to build an effective spam filter. Reducing the amount of false positive instances is the goal of utilizing the Likelihood class. In the backdrop, it is explained why employing a hybrid technique is preferable than utilizing an effective classifier that currently exists. Enron's first data set is split into a training and testing set with a ratio of 7:3. After that, the records are put into a decision tree classifier to build a model and categories the data. It is evident from the decision tree's output that many records were correctly categorized by the decision tree with a high degree of confidence value, while others of them were categorised with a lower level. To properly forecast the class, data whose estimated confidence is less than 70% should be taken into consideration for further processing. Due to this, records with low confidence values that the SVM classifier divided into several classes were filtered and kept separately. The decision tree divides the remaining data into two categories: spam and non-spam. The outcome shows that it outperformed what would have occurred if SVM or decision tree were employed alone. Along with improved prediction accuracy, the DT-SVM technique cut down on the total amount of time needed to categorise the data. Different algorithms, including KNN and Bayesian, were categorised using the same test data in addition to basic SVM and decision trees. Figures 9 and 10 are graphs that compare the accuracy and training times. kNN, which uses a lazy learner approach, classifies the test records based on how similar the attributes of the training and test records are.

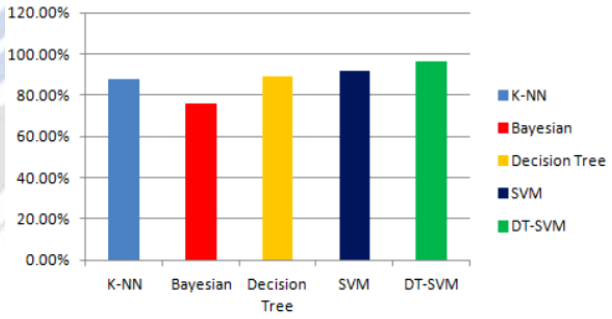

Figure 9: Comparison of Accuracy Using Different Algorithms

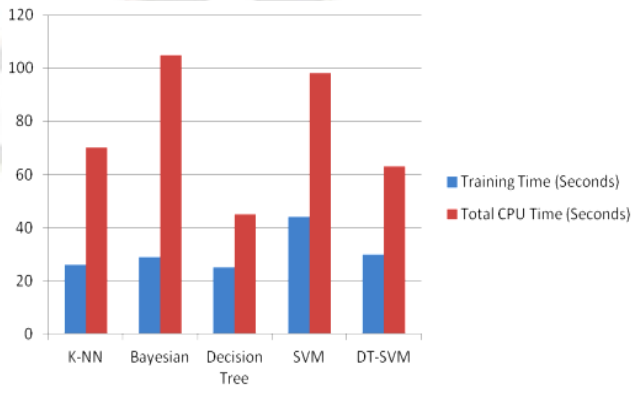

Figure 10: Comparison of Time using Various Algorithms

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 10 Issue: 11
DOI: https://doi.org/10.17762/ijritcc.v10i11.5781
***Article Received**: 28 August 2022 **Revised**: 07 October 2022 **Accepted**: 21 October 2022*

VI. CONCLUSION

According to this research work, one of the primary purposes of Spamdoop is to aid in collective spam detection by safeguarding all users' privacy while simultaneously collecting large amounts of data on a wide variety of spam types. Currently, spam detection algorithms only allow the email's body to be used for analysis. The first level of complexity is still useful, since it allows the use of trigram techniques for binary data grouping, such as figures. If the spammer doesn't notice the unlikely trigrams in the main output step, it's a good idea to cut them out of the final product. According on the size of the channels in question, multiple approaches for determining how big the channel should be might be used.

REFERENCES

[1] E.M. Bahgat, S. Rady, W. Gad An e-mail filtering approach using classification techniques The 1st International Conference on Advanced Intelligent System and Informatics (AISI2015), November 28-30, 2018, Springer International Publishing, BeniSuef, Egypt (2018), pp. 321-331.

[2] A. P, A. Sharma, S. B. M, P. Pavankumar, N. K. Darwante, "Performance Monitoring and Dynamic Scaling Algorithm for Queue Based Internet of Things," *2022 International Conference on Innovative Computing, Intelligent Communication and Smart Electrical Systems (ICSES)*, pp. 1-7, (2022) doi: 10.1109/ICSES55317.2022.9914108.

[3] AlMahmoud, Abdelrahman, et al. "Spamdoop: A privacy-preserving Big Data platform for collaborative spam detection." IEEE Transactions on Big Data (2019).

[4] Puneeth Kumar, B.S., Ramesh Naidu, P., Sridhara, S.B. (2023). Internet of Things and Cognitive Radio Networks: Applications, Challenges and Future. In: Yadav, S., Chaudhary, K., Gahlot, A., Arya, Y., Dahiya, A., Garg, N. (eds) Recent Advances in Metrology . Lecture Notes in Electrical Engineering, vol 906. Springer, Singapore. https://doi.org/10.1007/978-981-19-2468-2_3.

[5] S. B. Sridhara, M. Ramesha, "Recent advances in graph theory and its applications," Advances in Mathematics:Scientific Journal, vol. 10, no. 3, pp. 1407–1412, 2021, doi: 10.37418/amsj.10.3.29.

[6] Avinash Sharma, B. Kameswara Rao, Ravi Shankar, Parismita Sarma, Abhay Chaturvedi, Naziya Hussain, Industrial quality healthcare services using Internet of Things and fog computing approach, Measurement: Sensors, Volume 24, 2022, 100517, ISSN 2665-9174, https://doi.org/10.1016/j.measen.2022.100517 .

[7] K. Thomas, C. Grier, J. Ma, V. Paxson, and D. Song, ''Design and evaluation of a real-time URL spam filtering service,'' in Proc. IEEE Symp. Secur. Privacy, Jun. 2011, pp. 447–462.

[8] A. P, A. Sharma, A. Singla, N. Sharma, "IoT Group Key Management using Incremental Gaussian Mixture Model," *2022 3rd International Conference on Electronics and Sustainable Communication Systems (ICESC)*, 2022, pp. 469-474, doi: 10.1109/ICESC54411.2022.9885644.

[9] C. Yang, R. C. Harkreader, and G. Gu, ''Die free or live hard? Empirical evaluation and new design for fighting evolving Twitter spammers,'' in Proc. Int. Workshop Recent Adv. Intrusion Detection, 2019, pp. 318–337.

[10] Kishore, D. V. Gowda, Shivashankar, and S. Mehta, "MANET topology for disaster management using wireless sensor network," in International Conference on Communication and Signal Processing, ICCSP 2016, 2016, pp. 0736–0740, doi: 10.1109/ICCSP.2016.7754242.

[11] Pai, G.N., Sridhara, S.B., Shashidhara, K.S., Gangadhara, "Signal Analysis and Filtering using one Dimensional HilbertTransform," Journal of Physics:Conference Series 1706(1),2020, https://doi.org/10.1088/1742-6596/1706/1/012107.

[12] Sharma, K. S and M. R. Arun, "Priority Queueing Model-Based IoT Middleware for Load Balancing," *2022 6th International Conference on Intelligent Computing and Control Systems (ICICCS)*, 2022, pp. 425-430, doi: 10.1109/ICICCS53718.2022.9788218.

[13] S. Dhanaraj, V. Karthikeyani A study on e-mail image spam filtering techniques Paper presented at the International Conference on Pattern Recognition, Informatics and Mobile Engineering (PRIME) (2018)

[14] M. Nagabushanam, H. G. Govardhana Reddy & K. Raghavendra (2022) Vector space modelling-based intelligent binary image encryption for secure communication, Journal of Discrete Mathematical Sciences and Cryptography, 25:4, 1157-1171, DOI: 10.1080/09720529.2022.2075090.

[15] P. Ramesh Naidu, N. Guruprasad, "Design and implementation of cryptcloud system for securing files in cloud," Adv. Math. Sci. J., vol. 9, no. 7, pp. 4485–4493, 2020, doi: 10.37418/amsj.9.7.17.

[16] K. R. Swetha, Namitha A R, Manu Y M, Rashmi G R and Veera Sivakumar Chinamuttevi (2022), IOT Based Smart Health Care System to Monitor Covid-19 Patients. IJEER, 10(1), 36-40. DOI: 10.37391/IJEER.100105.

[17] M. Sheikhalishahi, A. Saracino, M. Mejri, N. Tawbi, and F. Martinelli. Fast and effective clustering of spam emails based on structural similarity. In International Symposium on Foundations and Practice of Security, pages 195–211. Springer, 2018.

[18] R. Fontugne, J. Mazel, and K. Fukuda. Hashdoop: A mapreduce framework for network anomaly detection. In Computer Communications Workshops (INFOCOM WKSHPS), pages 494–499. IEEE, 2019

[19] P. Ramesh Naidu and N. Guruprasad (2021), A High-Availability and Integrity Layer for Cloud Storage, Cloud Computing Security: From Single to Multi-Clouds, Journal of Physics: Conference Series, 1921 (1), pp. 012072. https://doi.org/10.1088/1742-6596/1921/1/012072.

[20] Lazzari, Lorenzo, Marco Mari, and Agostino Poggi. Cafe-collaborative agents for filtering emails. In Enabling Technologies: Infrastructure for Collaborative Enterprise,

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 10 Issue: 11
DOI: https://doi.org/10.17762/ijritcc.v10i11.5781
***Article Received**: 28 August 2022 **Revised**: 07 October 2022 **Accepted**: 21 October 2022*

2005. 14th IEEE International Workshops on, pp. 356-361. IEEE, 2015.

[21] Lu, Wei, Yanyan Shen, Su Chen, and Beng Chin Ooi. Efficient processing of k nearest neighbor joins using mapreduce. In Proceedings of the VLDB Endowment vol.5, no.10 pp. 1016-1027. 2019.

[22] Duan, Zhenhai, Peng Chen, Fernando Sanchez, Yingfei Dong, Mary Stephenson, and James Michael Barker. Detecting spam zombies by monitoring outgoing messages. Dependable and Secure Computing, IEEE Transactions on vol.9, no. 2 pp. 198-210. 2018.