International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 10
Article Received: *22 August 2023* ***Revised:*** *12 October 2023* ***Accepted:*** *26 October 2023*

Security Privacy Process Involvement in Cloud Security for Data Preservation against Data Malicious Activity

K Prabu[1], Dr P Sudhakar [2]
[1]School of Computing Science and Engineering, Galgotias University, UP, India.
k.prabu@galgotiasuniversity.edu.in
[2]School of Computing Science and Engineering, Galgotias University, UP, India.
p.sudhakar@galgotiasuniversity.edu.in

Abstract— Cloud data sent from the person is attacked, leading to data hacking. Data classification can be made by malware detection, leading to the data warehouse technique and data storage. The cloud data from a particular internet protocol address cannot be hacked. Only random cloud data is hacked. Even though this leads to some illegal issues. The method of managing the cloud data and maintaining the factor to hack illegal cloud data has been proposed. The method of malware detection and ML-based end-to-end malware detection are used in calculating the time efficiency. The malware detection and defence method has been introduced for managing the data tracking and the system's formation to hack unwanted data. The time efficiency calculation for the data transmitted in the network has been enabled for the cloud data sent and received. The data from each router makes the data store 12% of the unwanted compared to the original messages. The factor for managing the individual aspect to produce the data is 30% of the database. This will contain 20% of the data in formulating the cloud storage system, which makes the data classifications. 4% of redundant data from the database has been enveloped for the data classifications. Meanwhile, the data attack can be evaluated using the malware detector and also manages classification method for evaluation of data and formation of the system to produce data from the appearance of Secure data clouds.

Keywords: Cloud Data Classification; Cloud Security; Data Tracking; Malware Detection; ML-Based Malware Identification

I. INTRODUCTION

The computer-related evidence and the network vulnerabilities manage the data and the criminal activity. Computer Cloud Security is preserving and uncovering lost and encrypted data for the secure data transaction. The protection system and the digital attacks make the sensitive information and the business processes deployed. The protection of the data and the protection of the information is done for the industry's system. The risk of digital security is the protection for the risk, and the reputation of the customer has been proposed. Some of the security issues are data leakage, hacking, and ransomware. The attacks which enable data hacking are active and passive [1]. Managing security attacks and mechanisms is related to the number of credit cards and sensitive data. The estimation enables home automation and smart city data for intelligent services and helps data security from hacking. Device protection and malware defence and protection techniques have been promoted. This technique predicts the software in a stable platform for allowing it in the transforming time—managing the data for security reasons [2]. The involvement of the data and the type of evolution and evolving factor for malware detection by using the software can be done in this research. Providing the data or the information to travel in the specific part is done using the instance router for transferring the data [3].

The ML-based end-to-end malware detection method was used in calculating the time efficiency, which is improved in its time while comparing the 0.9 Ms of data and the time accuracy. The routing takes place in the data transmission very quickly and instantly. The server gives a way to manage the data in the shortest part to the destinations. The distributed information system works the processing technique a, the number of physical devices a, and the total processing of data required for the system management, enabling the complete processing of the proposed information [4]. The primary purpose of the distributed system is to manage the integrated, coherent network; the definition is the technopedia, and the integrated network for sharing data facilities is proposed [5,6]. The sharing of resources and the network connection, which manages the information and the processing of data, is done using different types of applications, and the distributed system contains advantages and disadvantages, which act as a distributed system [7]. The security of the data in which the DIS manages the data and the social networks for the mobile system and online banking is proposed. The software and hardware components contain the efficiency, reliability,

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 10
Article Received: *22 August 2023* ***Revised:*** *12 October 2023* ***Accepted:*** *26 October 2023*

accessibility, and fault tolerance offered. Some elements used in the distributed system are the data store, controller, and database for analyzing the data from the smart homes and the cities [8-10]. The process of managing the configuration of the system, the replication of the system, and the formation of the system in the distributed system has been proposed. The objective of this research is as follows:

1. The data attacks are made using malware defence and the detection technique for saving the data from the attacks and illegal activities from the routing.
2. The tracing of the data and the technique of the routing of the data is done while transferring the data.
3. For calculating the efficiency of time, the ML-based end-to-end malware detection method has been introduced using the data classifications has been elaborated.
4. Classification of the data can be able to manage the data which is received from the smart cities and the evaluations.

The section of the paper is divided into: In section 1 introduction of the article has been elaborated. In section 2, the related work, the analysis of the existing document, has been written. In section 3, the methods and results have been proposed; in section 4, the conclusion and future work have been whitened.

II. LITERATURE REVIEW

From the review of [1] discussed Cloud Security in higher education, detected in academic misconduct, is proposed. The process of maintaining the portable document format and the inserting of the hidden glyphs and the alternative matching of the software and the plagiarism-based collusion and the cheating of the balance probabilities for the text-matching software, and the detection of the document and the plagiarism-based detection of the text can be maintained by the plagiarism of the repurposed of the criminal data which is collected from the database. The FTK and autopsy technique method has been proposed to detect plagiarism.

The review of [2] discussed and proposed NLP-based Cloud Security from the online communication for the investigation platform for the criminal investigation, and the communication based on the NLP is submitted. Maintaining the vectorization of the data is classified based on the features. The method of feature selection is done for the generation of cyberspace. The data collected in the communication and the vectorization phase has been maintained in the generation classifications. Also, the vectorization of the log analysis for the selected data is proposed and can be presented using the investigation platform.

The review of [3] discussed and analyzed the privacy preservation of the data, and the AI-related collaboration manages the medical-related data to diagnose the system to produce the test sensitivity of the visual explanation and the communication cost for the data in the hospitals. The data management in digital health and the method of federated learning of the local models has been proposed using the training process. The sharing of the data and the performance of the data is analyzed, and the secure transmission is done using the federated learning framework.

From the review of [4] also discussed, this study involves online communication based on the NLP-based Cloud security management and online communication for the data. The investigation related to the criminal and civil-related data is stored and analyzed securely using the NLP. This platform compares the data and the classification, which generates the proposed Log analysis approach. Maintaining security based on the social media data and the paper related to health data is combined to make the data secure while transmitting the data from one place to another.

From the review of [5] discussed also, this study manages the automation, and the valuable security-related data for smart homes has been proposed for determining the common problems in smart devices has been submitted. The data in the intelligent homes manage the issues, and the data classifies the cloud security data to manage the intelligent devices. The process of solving the various security attacks and the devices from mobile and the unwanted factor for attacking the data is proposed. Also, the prevention of the data related to health and the element to produce the health data are presented.

From the review of [6] discussed, the investigation of the cloud security based on the industrial revolution and the maturity of the nodes which transmits the data and the transferring of the time which calculates the DF readiness and the benchmarking of the five databases has been enabled for the time taken for the data transfer in the nodes of the network has been calculated. Also, the DF organization and the capacity for developing the management are presented by implementing this in the current system. The time management of the system and the factor which accepts the DF organization has been enabled in this proposed system.

The review of the manuscript [7] discussed the video forgery recognition in the cloud security data for managing the credit of the cyber security has been enabled for the data transfer in the timely management from the IoT network has been enabled. Also, the integrity and the confidentiality of the expression rate, the tradition of the security system, and the integrity of video of cloud security have been enabled for the streaming video content and the Internet daily where vid Y involves this in the currently proposed system, the process of maintaining the time calculations is presented.

III. SECURITY PRIVACY PROCESS INVOLVEMENT IN CLOUD SECURITY

Cloud computing delivers computational resources like IT infrastructures and data centers to store and process data over the Internet as the cloud allows to rent space for storage from

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 10
Article Received: *22 August 2023* ***Revised:*** *12 October 2023* ***Accepted:*** *26 October 2023*

service providers in most fields like a hospital, marketing, business, and so on, because of the growth of data. Thus, as data use increases, the requirement for a storage medium is also increasing, so the use of the cloud grows higher, but security is the primary concern due to the large amount of sensitive data. Data security is improved by identifying the malicious attack and managing the spell to increase network availability. This ensures that the data and applications in the cloud are readily available for authorized users. Providing security to the system prevents the data from being lost and maintains complications by regulating data privacy. Cloud security is the only way to effectively secure data and resources in cloud computing environments [11].

3.1 Importance of Cloud Security and Data Collection

As the cloud is the most effective storage medium, it has several sensitive data that need to be prevented from malicious activities to increase availability and reduce the latency of the cloud. The data stored in the cloud for later access are collected for malware detection. Totally 1000 data were collected from the cloud database with various types of data like documents, images, videos, and so on with multiple file formats, and also they varied in size. 643 data were found to be malicious, and 357 were expected [12]. Then also, the history of network behaviors was gathered to see at which stage the data was affected during transmission.

3.2 Improve malware detection

The presence of malware activity in the data during data transmission through the network or from the cloud is found using the detection process. There are many techniques for detecting malware. One of the effective methods is the machine learning-based detection method. Improving ML-based end-to-end malware detection, th reduces the time taken to complete the detection process. The ML-based detection is based on the dataset, which contains both the features of malicious and standard data for testing and training. The system is trained with harmful data and behaviors for effectively finding the attacks. The training phase contains the feature extraction process in which the features of malicious and standard data are based on the behavior analysis method; these extracted features help classify the harmful or standard data. Before transmitting data to the requested user, it checks whether it is stored in a public or private cloud [13,14]. If the requested data is in the public cloud, it gets transmitted directly to the user because it does not contain confidential data. Otherwise, if the data is found in a private cloud, then the system evaluates whether a request is received from an authorized user or not, and when the user is authorized, data gets transmitted else, and the process gets restricted.

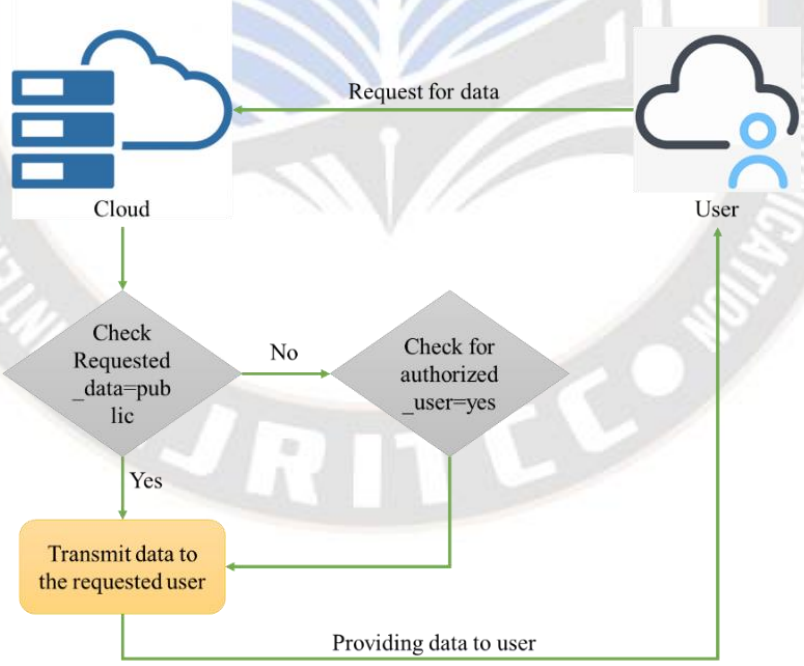

Figure.1 Request evaluation model in the cloud

Whenever the user needs to access the data stored in the cloud, the user transmits an HTTP request for data utilization as different organizations utilize the cloud to utilize resources like storage, computation, platforms, service, and so on. The service providers provide two types of cloud services, namely public and private cloud [15]. Sensitive data like healthcare, banking, and so on are stored in the private cloud, which must be accessed only by authorized users enrolled in the user list. The public cloud stores data publicly to allow access to each user. Thus, to provide security to data, an evaluation is

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 10
Article Received: *22 August 2023* ***Revised:*** *12 October 2023* ***Accepted:*** *26 October 2023*

conducted to find the availability of data for users based on their preferences. When the user is found authorized for private data or data requested in the public cloud, data transmission to the user is established. This model is shown in the above figure. 1.

During the process of data transaction in a network, the data might be affected or theft by an unauthorized person that can be detected using the ML technique with an end-to-end method. Thus, the detection is wholly based on feature extraction. To improve the feature extraction end-to-end process, the features of data are continuously monitored for every 1m distance the data present in the network to identify the malware effectively [16]. This method aims to determine when the data gets affected due to malware activity in a minimal amount of time to protect the data. It provides practical and accurate detection of files or data in the network for a transaction by training the system with the features of malicious attacks and network behavior to increase the accuracy of identifying malware.

After evaluating the request to find an authorized user or not, the requested data gets transmitted from the cloud to the user end through a network each time the authorized user is detected. Using end-to-end detection from the sender to the receiver end, feature extraction monitors the data continuously [16]. The data flow path or distance is segmented into 1m each, also known as different states of the transaction, for improving the monitoring process. Then, each segmented length is determined for ML-based identification so that when the data or network is affected by the trade, it will be accurately identified to provide a high range of security to the cloud (Figure 2).

The presence of malware during the data transmission from the cloud server to the user is identified using an improved end-to-end machine learning method. Initially, the cloud server checks whether the user requesting the data is from the public or private cloud. If the requested data belongs to the public cloud, then the system transmits the requested data. Otherwise, the requested data belongs to the private cloud, and then the system needs to verify the user access. Each user has a separate and unique user id, name, and password. Before entering it, get and check for the user id is exists on the server user list [16]. If it exists, then it allows access to the data and transmits data to the user; otherwise, it restricts access to data.

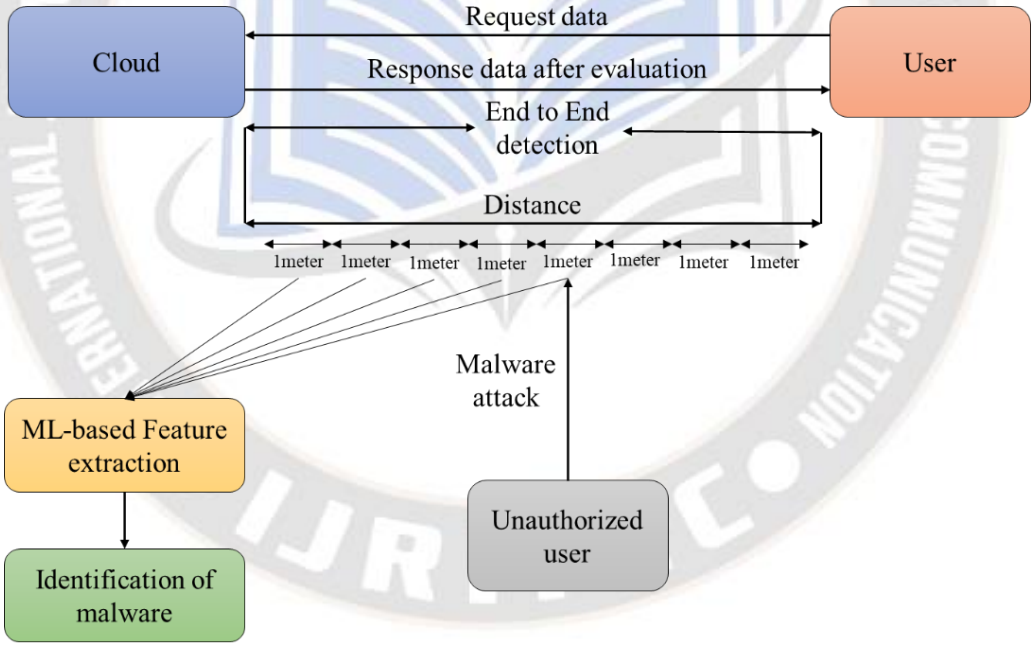

Figure.2 Improved end-to-end ML-based malware identification model

Pseudocode For Malware Detection Using Improved End-To-End Machine Learning Method

Input: user request
output: identify malware detection
for each new request
if (requested_data=public)
response to request
else if (requested_data=private)
user_id= get_user_id (user id, user name, password)
if (exisits_user_id)
allow access
transmit data = send (response to request)
else
restrict request

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 10
Article Received: *22 August 2023* ***Revised:*** *12 October 2023* ***Accepted:*** *26 October 2023*

end if
end if
while data transmission
for all (data)ϵ datasets do
IE-EML(e)
end for
determine D (cloud-user)
split= D (each 1m)
for each 1m D
perform IE-EML(e)in 1m
if (detects= abnormality)
identify abnormality as malware
else
continue process
until covering the D (cloud user)
end if
end for

Malware may be present during the data transmission process, so it will be detected using an improved end-to-end machine-learning method. The data transmission distance between the cloud and the user is initially determined and then split into each 1m for detecting the correct place of malware attacks [17]. For each 1m distance of a whole data transmission distance, if any abnormal activity is detected, then identify these activities as malware; otherwise, this checking process is continued until analyzing the entire space between the cloud storage and the user [18].

3.2.1 Security concerning the Processing time

The security of the cloud is entirely based on identifying, monitoring, and preventing attacks on private data. Processing times determine the total amount of time taken to complete a process. In the existing system, the time taken to complete the process is 0.09ms, but in the proposed method, improving malware detection by a continuous evaluation process, the time taken to identify the malware gets reduced to 0.04ms. Thus, the proposed system helps improve data security by reducing the processing time [19].

3.2.2 Cloud Data Tracking

After identifying malware during data transmission using an improved ML-based end-to-end detection tracking process which helps to find in which path unauthorized access is performed for restringing the data being used to avoid attacks, tracking is the process of monitoring the flow of data in the network to reach a particular destination securely. It involves collecting and analyzing data to find the number of nodes the data transfer and determine the time stamp to find the occurrence of time delay [20]. This method aims to determine the location and direction of targeted data in the network using a routing table containing the information essential to forward the packet in the best path to the destination. Each package includes information on its origin and destination. Routing Table provides the device with instructions for sending the container to the next hop on its route across the network.

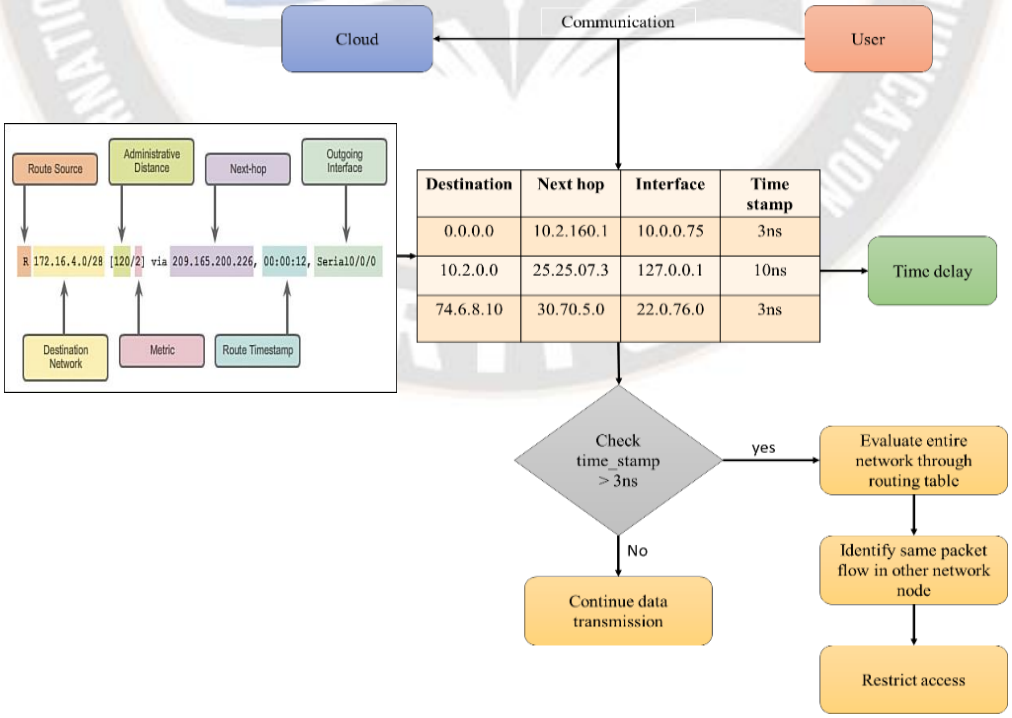

Figure. 3 Data tracking model

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 10
Article Received: *22 August 2023* ***Revised:*** *12 October 2023* ***Accepted:*** *26 October 2023*

When the connection is established between two systems for communication, the routing process also gets triggered to provide the shortest path to transmit the data in a minimum time. But, in this method, a routing table is used for routing and tracking the data with the help of its attributes like destination, next hop, interface, and time stamp. The time consumed to transmit data from one network node to another is 3ns. It is standard, and when it increases, it is determined that there is a time to declare presenting to some unauthorized activity. Then the process flow of the entire network is evaluated through the routing table [18]. When the same packet is detected in a different path, then the additional flow of data in the unauthorized course is restricted and only transmitted to the determined destination without any security issues (Figure 3). The process continuously monitors the data packets moving paths to reach the goal. During this process, we need to find the nodes that participated, the time taken to complete the data transferring process and the occurrence of time delay. Each packet contains information about its origin and destination [19]. Routing Table provides the device instructions for sending the container to the next hop on its route across the network.

Pseudocode for tracking the network routing

```
begin
define: routing table RT (network_id, destination,
        outgoing_interface, timestamp 'T')
while data transmission do
for each node in N network
if (data =broadcast)
determine D(cloud-server)
for each 1m distance, do
update routing table
find changes in T
if (T>3ns)
evaluate routing table in N
if (identify= same DP in another route)
restrict data transmission
end if
else
continue data transmission
update routing table
end if
end for
end if
end for
end while
```

The routing table is used for monitoring or tracking the route of the data moving by estimating the attributes like destination, next hop, interface, and time stamp. Then the process flow of the entire network is evaluated through the routing table. Initially, the distance between the source and destination is determined, and the communication routing process also adopts the path which takes the minimum time to reach the goal. The standard time stamp for completing the data transmission process is 3ns [21]. When the time stamp is increased for a particular routing, it is identified as some other unauthorized activity performed due to this activity, and the time delay has occurred. When detecting duplicate data packets flowing through another unauthorized route, it is restricted and only transmitted to the determined destination without any security issues.

IV. RESULT AND DISCUSSION

In this section, we evaluate the proposed system's effectiveness based on the dataset and the performance metrics accustomed to verifying the performance of our proposed ML-based malware detection method. Then we discuss the observational results in detail. We used 1000 data from the cloud database to evaluate malware detection, including documents, images, videos, etc. We use 643 data with malicious behavior and 357 with average behavior data. We compare the proposed system with different classifiers for detecting standard and malware behavioral data [5]. The higher the Precision, Recall, and accuracy, the better the recognition effect. TP (True Positive) represents malicious data correctly labeled as hostile, and FN (False Negative) represents benign data wrongly labeled as malicious. FP (False Positive) means malicious data incorrectly marked as innocent. Because F1 measure and accuracy aggregate the results of Precision and Recall, they show the model's overall performance. The higher F1 and accuracy may explain why the identification approach is more effective [9].

To evaluate the effectiveness of the proposed scheme with various classification models illustrated in Table 1. In experiments, we employed the cross-fold validation technique to the classifier models from the prospect of stability and to elude the over-fitting. We compared our experiments using the 10-cross validation [10].

Table.1 Precision, Recall, F-Measure, and Accuracy for the proposed method

Classifier	Data count	Precision	Recall	F-measure	Accuracy
ML-based end-to-end detection	1	89.72	88.29	88.99	89.00
	2	89.81	90.02	89.91	90.00
	3	90.61	90.23	90.41	90.50

	4	90.84	90.61	90.72	90.80
	5	89.72	88.92	89.31	89.40
	6	88.63	89.78	89.20	89.20
	7	89.06	90.25	89.65	89.70
	8	90.42	89.51	89.96	90.00
	9	88.63	89.58	89.10	89.10
	10	89.85	89.73	89.78	89.80

We used the below metrics for evaluating the performance of our proposed detection method, which is as follows:

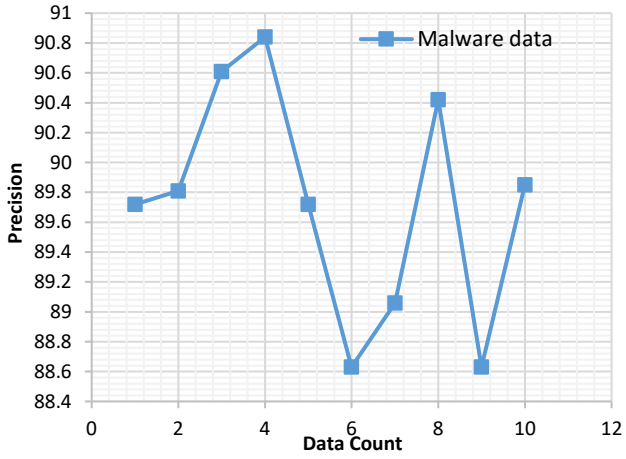

Figure 4. Precision vs data count analysis

We can see from Figure 4. That is the precision value of the increasing data count during transmission. Our proposed ML-based end-to-end malicious detection methods give a better result in higher precision [22]. Precision is the division of true positives with the sum of true positives and false positives or the ratio of correctly identified malicious activity from the whole user's activity. The mathematical representation of precision is as follows as shown in eqn(1):

$$\text{Precision}=TP/(TP+FP) \quad (1)$$

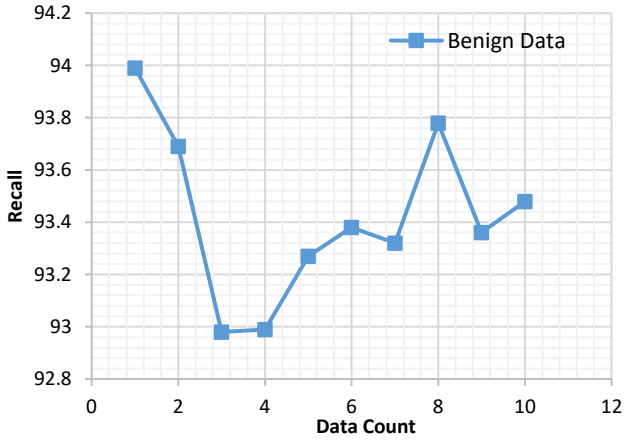

Figure 5. Recall vs data count analysis

A recall is the fraction of true positives with the sum of true positives and false negatives. Figure 5 shows the recall value for increasing the count of data. Our proposed ML-based end-to-end malicious detection methods give a better result in light of recall. But the recall value contrasts with precision which is slightly weaker. The equation for calculating recall is shown in eqn(2) as follows:

$$\text{Recall}=TP/(TP+FN) \quad (2)$$

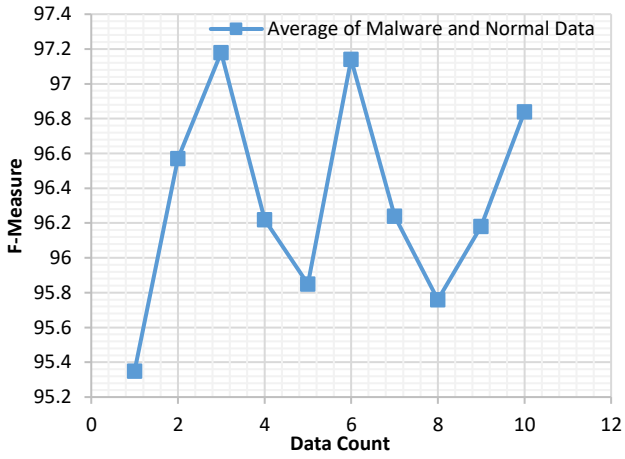

Figure 6. F-measure vs data count analysis

Figure 6 depicts the F-measure value of the proposed methods concerning the increasing data count during transmission. F-measure includes the false negative and false positive and the weighted average of precision and recall. An offered has a better score for accuracy and memory that will lead to a good *F*-measure value for the proposed model. From this result, the f-measure of a proposed system is better, and it shows a harmonic mean and justifies the strength of the classification model [23]. The formula is shown in eqn(3) as follows:

$$F1-\text{Score}=2*\text{Precision}*\text{Recall}/(\text{Precision}+\text{Recall}) \quad (3)$$

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 10
Article Received: *22 August 2023* ***Revised:*** *12 October 2023* ***Accepted:*** *26 October 2023*

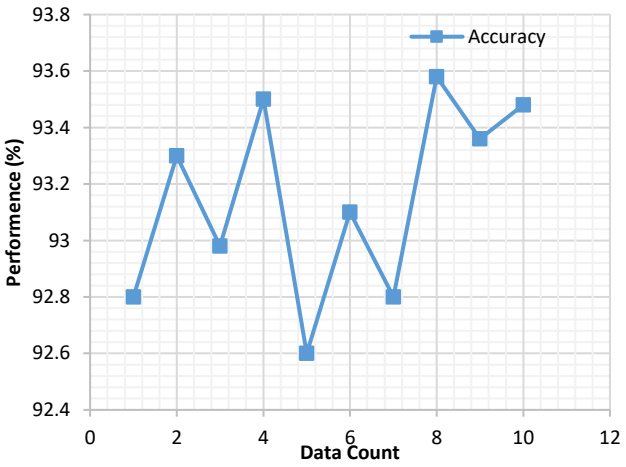

Figure 7. Accuracy vs data count analysis

The way of considering the best classifier in light of detection accuracies. The accuracy of machine learning models can be found by dividing the total number of correct classifieds by the sum of actual positives and actual negatives [24]. Figure 7 shows an accuracy of a proposed method concerning the increasing data count. It can also be noted that the proposed ML provides a good detection performance of 90.9% percent; the formula in eqn (4) shown for calculating the accuracy is as follows:

$$\text{Accuracy} = \frac{TP+TN}{TP+TN+FN+FP} * 100\% \quad (4)$$

Table 2 clearly shows the practical approach for detecting malware such as Naive Bayes, K-nearest neighbors, XG Boost, and neural networks compared with our proposed method for analyzing the system's effectiveness.

Table. 2 Precision, Recall, F-Measure, and Accuracy for various methods

Methods	Features Count	Recall (%)	FPR(%)	F-measure (%)	Accuracy (%)
Neural network [Arslan et al.]	25	88.62	8.05	95.03	91.95
Naïve Bayes [Akbar.F et al]	61	92.93	10.48	89.50	89.52
KNN [Menahem, E. et al.]	42	91.62	9.3	94.93	90.70
XGboost [Kumar, R et al.]	31	90.03	10.02	92.88	89.98
Proposed ML-based end-to-end detection	24	93.42	6.58	96.33	93.15

The accuracy of malware detection is based on several features with different algorithms in 10 folds. The graph shows that the proposed ML-based end-to-end achieved the highest accuracy in 10-fold testing. The lowest accuracy was when Naive Bayes reached the applied algorithm. Furthermore, based on this work, the finding shows that the proposed ML-based end-to-end is the best parameter at each node in the decision tree made from randomly selected numbers in feature selection [25]. In other words, this classifier operates by constructing decision trees at training time and producing the class that is a mode of the types. All classifiers show an accuracy detection increase starting from 18 features, and the stop at several features is 24. The number of components is 24. After that, the slope of the graph continues to drop until the number of members is 28. So, the result shows that detecting malicious user activity is more effective.

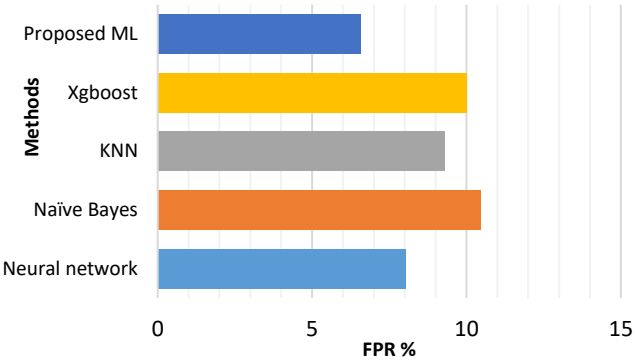

Figure 8. The contrast of false positive rate analysis

Table 2 shows a performance metrics comparison between different malware detection techniques. The FPR value is relatively high than the other methods. Figure 8 shows the false positive rate of the existing and proposed neural network, naïve Bayes, XG boost, KNN, and ML model [10]. The false positive rate of a neural network has 8.05%, and the naïve Bayes, KNN, and XG boost have an FPR of 10.48%, 9.3%, and 10.02%, respectively. The proposed ML has an FPR rate of 6.58%. In contrast with other methods, the proposed ML has a higher FPR rate, so the proposed method is better than the others.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 10
Article Received: *22 August 2023* ***Revised:*** *12 October 2023* ***Accepted:*** *26 October 2023*

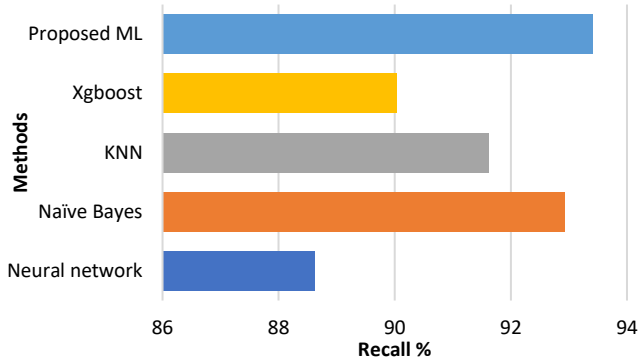

Figure 9. The contrast of recall in %

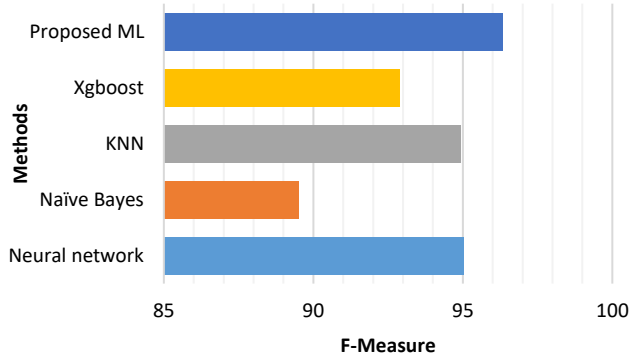

Figure 10. The contrast of the F-measure

Figure 9 demonstrates the bar chart of the recall measures of various detection methods with our proposed method. Figure 10 illustrates our proposed method's F- standards of different detection methods. F-measure shows a harmonic mean between the recall and precision of the proposed method. The proposed method recall and f-measure values are higher than the other existing methods. From this graph, we can see that the proposed ML is more effective than the other method.

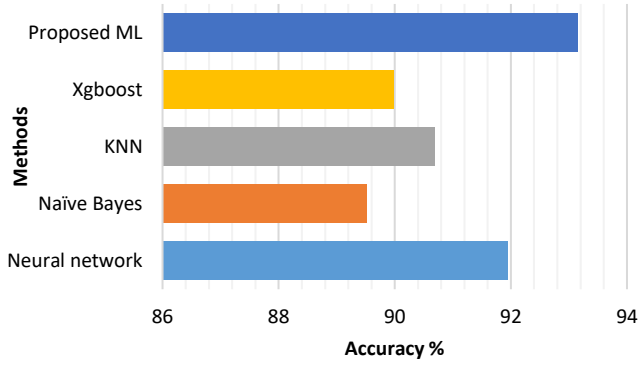

Figure 11. The Contrast of Accuracy Analysis

Figure 11 compares various malware detection methods in terms of percentage accuracy. The accuracy of a neural network, naïve Bayes, KNN, and XG, boosts 91.5%, 8.52%, 90.70%, and 89.98%, respectively. Our proposed system has an accuracy of 93.15%, which is better than the other detection techniques. The naïve Bayes is less effective than the proposed and other detection methods. Table 3 shows the processing time concerning the increasing count of data.

Table3.processing time of increasing count of data

Iteration	Distance of data moved from source to destination(meter)	Processing Time (ns)
1	0-1	3
2	1-2	4
3	2-3	3
4	3-4	3
5	4-5	4
6	5-6	3
7	6-7	4
8	7-8	3

In our proposed tracking model, the distance between the source and destination is equally separate, with a 1m distance during the data transmission. Each 1m distance the user activity belongs to the data is monitored [26]. When a malicious activity has occurred, the data transmission process takes longer than the customarily taken time data transmission. Figure 12 and 13 shows the histogram distribution of data users pass regarding response time.

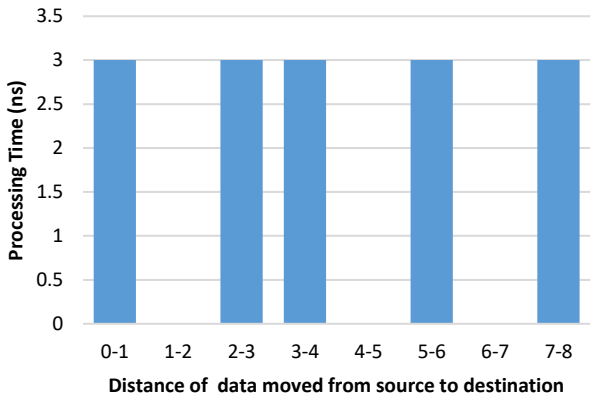

Figure 12. Regular activity of user analysis

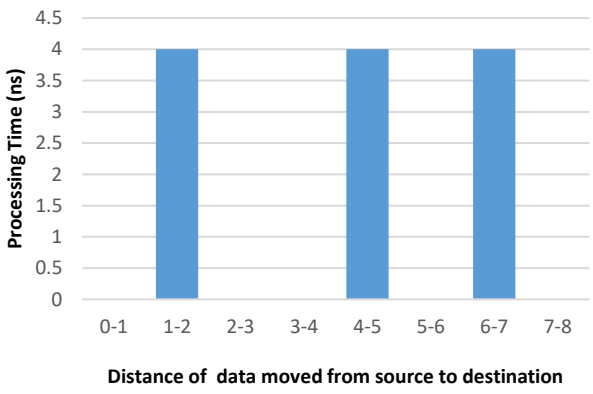

Figure 13. The malicious activity of the user analysis

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 10
Article Received: *22 August 2023* ***Revised:*** *12 October 2023* ***Accepted:*** *26 October 2023*

Figure 12 shows the average user activity during the data transmission with a standard level of response time of 3ns. Figure 13 shows the abnormal user activity during the data transmission with an oscillation level of the response time of 4ns. The response time increases, and we can detect and identify the abnormality or malware of data during a particular distance. Otherwise, the process is completely secured and reaches the destination within the pre-set response time of a user [27]. During the data transmission, the data count may vary only depending on the median and average response time and throughput. Table 4 shows the data count's median and average response time and throughput.

Table4. Performance calculation of median and average response time and throughput

No. of data	Median response time(ms)	Average response time(ms)	Throughput (Request/sec)
10	2264	3162	11.4
20	3961	4152	11.6
30	5995	6543	11.8
40	7961	8623	11.6
50	9312	10623	11.8
60	11243	11952	11.7

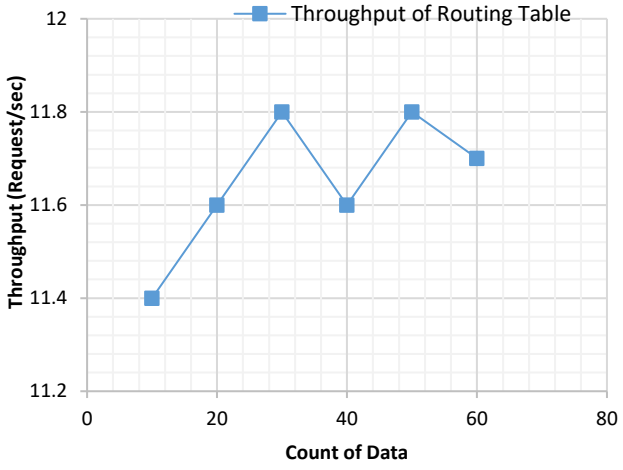

Figure 14. Analysis of the Amount of throughput during the data transmission

The proposed tracking system testing has been done to measure each response's throughput by analyzing the proposed system's scalability. Figure 14 represents the throughput with an increasing data count [28]. The count of concurrent users' data sharing increased from 10 to 60 at a similar time. The average count of users' data transmission with average response time and throughput is 11.8, which shows that 11.8 requests can be processed per second by the system.

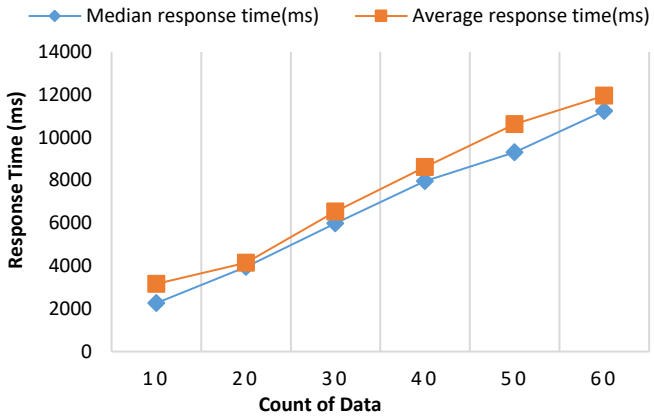

Figure 15. Response time for data transmission analysis

Figure 15 shows a response time for increasing the data count. During the data transmission, the increase in the data count leads to an increase in response time. Similarly, reducing the data count minimizes the process's completion time. Figure 15 shows the average response time in the orange line, and the median response time is in blue [29]. The average response time and median response time also linearly increased concerning the increases in the data count. And then the average response time is higher than the median response time. From this analysis, when a process's response time takes less or is equal to the pre-set time, only the performance and security of the system increase.

V. CONCLUSION

This research found the privacy issues in cloud security and the cyber security for managing the investigation of cloud security. The protection which enables the current development of various technologies has been proposed. The detection of malware for privacy in cloud security is enabled and done by detecting the malware detection technique, and the classification of the data has been proposed for the distribution of the system. Maintaining and transferring the data in the distributed information system has been enabled using the routing algorithm method. The collection of the data and the evolution of the data has been done for the development of the data in the networks. The large amount of data that satisfies the system's formation and the security concern for having the authorized data is the 400 megabytes data is unauthorized, and the 800 megabytes for the distributed data items for the innovative frequency has been done. The data is collected, and then the formation of the system, which forms the 4500 megabyte data for the information, is done. Also, the data classification is done to manage the distributive information and the differentiae factor for collecting the informative technology. The public and the private key help in the data attack items.

References

[1] Johnson, C., Davies, R., & Reddy, M. (2022). Using digital forensics in higher education to detect academic misconduct. International Journal for Educational Integrity, 18(1), 1-19.

[2] Sun, D., Zhang, X., Choo, K. K. R., Hu, L., & Wang, F. (2021). NLP-based digital forensic investigation platform for online communications. Computers & Security, 104, 102210.

[3] Bai, X., Wang, H., Ma, L., Xu, Y., Gan, J., Fan, Z., ... & Xia, T. (2021). Advancing COVID-19 diagnosis with privacy-preserving collaboration in artificial intelligence. Nature Machine Intelligence, 3(12), 1081-1089.

[4] Adaramola, O. O., Odigbo, C., & Elelegwu, D. O. (2022). Impact of Digital Security and Digital Forensic in Smart Homes.

[5] Thirumalaisamy M, Basheer S, Selvarajan S, Althubiti SA, Alenezi F, Srivastava G, Lin JC-W. Interaction of Secure Cloud Network and Crowd Computing for Smart City Data Obfuscation. Sensors. 2022; 22(19):7169. https://doi.org/10.3390/s22197169

[6] Ariffin, K. A. Z., & Ahmad, F. H. (2021). Indicators for maturity and readiness for digital forensic investigation in era of industrial revolution 4.0. Computers & Security, 105, 102237.

[7] Bagkratsas, I. M., & Sklavos, N. (2021, September). Digital Forensics, Video Forgery Recognition, for Cybersecurity Systems. In 2021 24th Euromicro Conference on Digital System Design (DSD) (pp. 510-513). IEEE.

[8] Ali, M. I., & Kaur, S. (2021). Next-generation digital forensic readiness BYOD framework. Security and Communication Networks, 2021.

[9] Awuson-David, K., Al-Hadhrami, T., Alazab, M., Shah, N., & Shalaginov, A. (2021). BCFL logging: An approach to acquire and preserve admissible digital forensics evidence in cloud ecosystem. Future Generation Computer Systems, 122, 1-13.

[10] Luo, X., Liao, R., Hu, H., & Ye, Y. (2022). Research on digital forensics method of 5G communication system in the future based on direct intermediate frequency sampling. International Journal of Autonomous and Adaptive Communications Systems, 15(1), 46-62.

[11] Fagbola, F. I., & Venter, H. S. (2022). Smart digital forensic readiness model for shadow IoT devices. Applied Sciences, 12(2), 730.

[12] Rughani, P. H. (2017). Artificial intelligence based digital forensics framework. International Journal of Advanced Research in Computer Science, 8(8).

[13] Mas'ud, M. Z., Hassan, A., Shah, W. M., Abdul-Latip, S. F., Ahmad, R., Ariffin, A., & Yunos, Z. (2021, January). A Review of Digital Forensics Framework for Blockchain in Cryptocurrency Technology. In 2021 3rd International Cyber Resilience Conference (CRC) (pp. 1-6). IEEE.

[14] Babun, L., Sikder, A. K., Acar, A., & Uluagac, A. S. (2019, May). A digital forensics framework for smart settings: poster. In Proceedings of the 12th Conference on Security and Privacy in Wireless and Mobile Networks (pp. 332-333).

[15] Rahim, N., Wahab, W. A., Idris, Y. I., & Kiah, L. M. (2014). Digital forensics: an overview of the current trends. Int J Cryptol Res, 4(2).

[16] Ieong, R. S. (2006). FORZA–Digital forensics investigation framework that incorporate legal issues. digital investigation, 3, 29-36.

[17] Li, S., Qin, T., & Min, G. (2019). Blockchain-based digital forensics investigation framework in the Internet of things and social systems. IEEE Transactions on Computational Social Systems, 6(6), 1433-1441.

[18] Lee, S. Y. (2022). Mobile Digital Forensics Framework for Smartphone User Analysis. Webology, 19(1).

[19] Zhang, S. H., Meng, X. X., & Wang, L. H. (2016, December). SDNForensics: A comprehensive forensics framework for software defined network. In International Conference on Computer Networks and Communication Technology (CNCT 2016) (pp. 92-99). Atlantis Press.

[20] Goni, I., & Mohammad, M. (2020). Machine learning approach to mobile forensics framework for cyber crime detection in Nigeria. Journal of Computer Science Research, 2(4).

[21] Chhabra, G. S., Singh, V. P., & Singh, M. (2020). Cyber forensics framework for big data analytics in IoT environment using machine learning. Multimedia Tools and Applications, 79(23), 15881-15900.

[22] Zaharis, A., Martini, A. I., Perlepes, L., Stamoulis, G., & Kikiras, P. (2010, October). Live forensics framework for wireless sensor nodes using sandboxing. In Proceedings of the 6th ACM workshop on QoS and security for wireless and mobile networks (pp. 70-77).

[23] Liebrock, L. M., Marrero, N., Burton, D. P., Prine, R., Cornelius, E., Shakamuri, M., & Urias, V. (2007, March). A preliminary design for digital forensics analysis of terabyte size data sets. In Proceedings of the 2007 ACM symposium on applied computing (pp. 190-191).

[24] Aluvalu R, Kumaran V. N. S, Thirumalaisamy M, Basheer S, Ali aldhahri E, Selvarajan S. 2023. Efficient data transmission on wireless communication through a privacy-enhanced blockchain process. PeerJ Computer Science 9:e1308 https://doi.org/10.7717/peerj-cs.1308

[25] Wan, X., He, J., Huang, N., & Mai, Y. (2015). Ontology-Based Privacy Preserving Digital Forensics Framework. International Journal of Security and Its Applications, 9(4), 53-62.

[26] Akbar, F., Hussain, M., Mumtaz, R., Riaz, Q., Wahab, A. W. A., & Jung, K. H. (2022). Permissions-Based Detection of Android Malware Using Machine Learning. Symmetry, 14(4), 718.

[27] Arslan, R. S., Doğru, İ. A., & Barişçi, N. (2019). Permission-based malware detection system for android using machine learning techniques. International journal of software engineering and knowledge engineering, 29(01), 43-61.

[28] Menahem, E., Shabtai, A., Rokach, L., & Elovici, Y. (2009). Improving malware detection by applying multi-inducer ensemble. Computational Statistics & Data Analysis, 53(4), 1483-1494.

[29] Kumar, R., & Geetha, S. (2020). Malware classification using XGboost-Gradient boosted decision tree. Adv. Sci. Technol. Eng. Syst, 5, 536-549.