Computers, Materials & Continua
DOI: 10.32604/cmc.2022.024501
Article

Tech Science Press

Malware Detection Using Decision Tree Based SVM Classifier for IoT

Anwer Mustafa Hilal[1,*], Siwar Ben Haj Hassine[2], Souad Larabi-Marie-Sainte[3], Nadhem Nemri[2], Mohamed K. Nour[4], Abdelwahed Motwakel[1], Abu Sarwar Zamani[1] and Mesfer Al Duhayyim[5]

[1]Department of Computer and Self Development, Preparatory Year Deanship, Prince Sattam bin Abdulaziz University, AlKharj, Saudi Arabia
[2]Department of Computer Science, College of Science and Arts, King Khalid University, Mahayil Asir, Saudi Arabia
[3]Department of Computer Science, College of Computer and Information Sciences, Prince Sultan University, Saudi Arabia
[4]Department of Computer Science, College of Computing and Information System, Umm Al-Qura University, Saudi Arabia
[5]Department of Natural and Applied Sciences, College of Community-Aflaj, Prince Sattam bin Abdulaziz University, Saudi Arabia
*Corresponding Author: Anwer Mustafa Hilal. Email: a.hilal@psau.edu.sa
Received: 20 October 2021; Accepted: 25 November 2021

Abstract: The development in Information and Communication Technology has led to the evolution of new computing and communication environment. Technological revolution with Internet of Things (IoTs) has developed various applications in almost all domains from health care, education to entertainment with sensors and smart devices. One of the subsets of IoT is Internet of Medical things (IoMT) which connects medical devices, hardware and software applications through internet. IoMT enables secure wireless communication over the Internet to allow efficient analysis of medical data. With these smart advancements and exploitation of smart IoT devices in health care technology there increases threat and malware attacks during transmission of highly confidential medical data. This work proposes a scheme by integrating machine learning approach and block chain technology to detect malware during data transmission in IoMT. The proposed Machine Learning based Block Chain Technology malware detection scheme (MLBCT-Mdetect) is implemented in three steps namely: feature extraction, Classification and blockchain. Feature extraction is performed by calculating the weight of each feature and reduces the features with less weight. Support Vector Machine classifier is employed in the second step to classify the malware and benign nodes. Furthermore, third step uses blockchain to store details of the selected features which eventually improves the detection of malware with significant improvement in speed and accuracy. ML-BCT-Mdetect achieves higher accuracy with low false positive rate and higher True positive rate.

Keywords: Blockchain; malware detection; classification; feature selection; internet of medical things

1 Introduction

The Internet of Things (IoTs) is the interrelation of mechanical and digital machines with unique identifiers (UIDs) with an ability to transfer data in a network without human intervention. An ecosystem of web enabled smart devices with sensors to collect and send data from the environment is a IoT ecosystem. The computing paradigm has changed with the advancement in the smart devices to facilitate our day-to-day activities. These advancements have enabled the implementation of Internet of Medical Things (IoMTs) which communicates through smart medical equipment. In IoMT, medical devices are equipped with wireless technology like Bluetooth or Wi-Fi to enable communication to promote IoMT technology. The future of the medical world will be shaped better with the integration of Augmented Reality (AR), Artificial Intelligence (AI), Blockchain technology, Machine Learning and sensors. With many advantages in IoMT technology, there are few challenges that need to be resolved while designing an IoMT system. The issues to be concentrated are: Security challenges, Interoperability and privacy. The privacy issues may be replay, man-in-the-middle attack, impersonation, privileged-insider, denial of service attacks (DoS) and malware attacks. Malignant attacks need to be prioritized which is malware attacks that deals with confidentiality and integrity. Health care data is considered to be very confidential and sensitive to be disclosed or altered by unauthorized person. The number of IoT devices are increasing day by day and is roughly 6.1 billion smartphone users in 2021 [1,2]. With the consistent use of Internet devices attackers are prone to hack the sensitive data [3]. The architecture of IoMT is shown in Fig. 1.

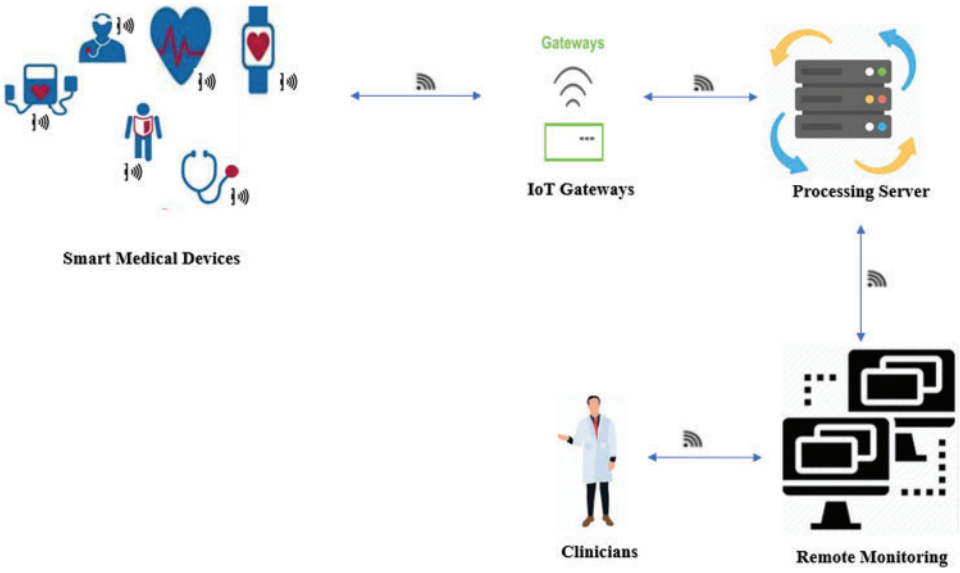

Figure 1: Internet of medical things architecture

The existing malware detection methods seems to be not efficient which is evident from recent attacks by Mirai Brickbot botnets. Due to the lack of good protection technique, bot nets create distributed denial-of-service (DDoS) attacks in smart things environment. These attacks may be very dangerous to the people which may even lead to death. This leads to development of many innovations to protect and prevent the attack in IoMT by IoT researchers in IoT security domain. Hence it is very essential to enable a strong security mechanism and a framework to detect the threatening attacks in IoMT where the transmitted clinical data is highly sensitive and confidential [4–6]. The advantages of smart technology and its usage in the near future motivated to develop a malware detection framework.

Since nowadays all the devices are driven towards the Internet of Things it becomes essential to protect us from the problems caused due to the growth in technology. These smart devices are connected through a network to share data with different entities like servers, sensors and IoT devices. From the literature it is clearly evident that the new blockchain technology has also stepped into IoT to enable strong security mechanism [7–9]. Blockchain technology ensures reliable data sharing in IoT environment which is based on distributed computing. With an intention to detect the malware in this smart IoT era, this paper enhanced a novel malware detection framework by using machine learning techniques to detect and train the IoMT malware detection which in turn creates a huge database. This database stores the results of the models in the blockchain framework. The proposed ML-BCT-Mdetect frame work integrates machine learning techniques and blockchain methodology to ensure effective detection of malwares. Fuzzy C Means (FCM) clustering algorithm is employed to extract relevant features useful for malware detection. Further Decision tree based SVM is used for multi feature classification. Finally, the data related to malware is stored in blockchain database to ensure efficient dynamic detection. New malwares which are detected during the run time is also added to the blockchain database for further similar malware detection. The contribution of the work is as follows.

1. We propose a ML-BCT-M detect framework for malware detection in in IoMT devices using blockchain
2. FCM clustering is used to extract the relevant malware from real features considering the membership values for detection process.
3. A multi-feature decision tree based SVM algorithm is used to classify real data from malware from the samples to achieve high accuracy.
4. In addition to the above, the proposed framework uses blockchain database to store the results of the machine learning models to pass the malware details to all the users.

The brief introduction is followed by related work in Section 2. Section 3 describes the proposed methodology. Experimental results discussed in Section 4. Section 5 concludes the paper with future research idea.

2 Related Work

Existing methods to meet the challenges and issues related IoMT devices are reviewed in this section. A software that is delivered in the network to infect the resources or affects the other software is called as malicious software. Malwares provides remote access to the infected system. They are also transferred from system to system and might attack sensitive data [10–13]. Wellness based health care systems are developed with Internet of Things where the healthcare devices monitor and send the sensitive and confidential health data to the cloud which can be accessed by IoT devices. This ensures IoT to facilitate processing and analysis of real time health care data [14, 15].

Dinakarrao et al. [15] developed a machine learning based malware detection mechanism for IoT devices. The performance of malware detection is improved by applying machine learning algorithms. Further the results are stored in distributed malware database which is a blockchain framework. A graph-based convolution neural network (CNN) mechanism is developed by Aslam et al. [16] to detect the malware like IoT bots. Experimental results proved that proposed method classifies the benign and IoT malware with highest accuracy. Xu et al. [17] creates a malware detector named as HaRM which uses the low computational cost classifier to use IoT resource for IoT malware detection. Proposed HaRM achieves high accuracy and also gives the range of estimation state to prevent the further spread of malware.

Raje et al. [18] developed a Blockchain-based framework to preserve patient anonymity with Bluetooth enabled smart phones. Contact of public is traced using smart phone and this data is stored in cloud. This data from cloud is accessible by the health department and the government. People could do their regular activities in a secured manner to keep them safe. Thus, the author proves that proposed Adaptive Neuro-Fuzzy Interference System (ANFIS) system to predict the status of COVID, and the proposed method achieves accuracy rate of 95.9% that is proved from experimental analysis.

Ouaguid et al. [19] presents a contact tracing scheme that preserves privacy using blockchain technology to bridge the user/patient and the authorized solvers to desensitize the user ID and location information. The authors show that their proposed model has secured higher security and privacy and is battery friendly and globally accessible. Beep Trace develops and implements digital contact tracing applications that can overrule COVID-19 with the features of providing timely framework to developers and researchers.

Afonso et al. [20] classified files as benign or malicious by constructing decentralized firewall using blockchain technology. The authors used a Deep Belief Neural network (DBN) as direction engine. In the proposed method, 10,000 files are used to train the model to classify gray scale images into two classes. Afonso et al. [20] developed a method named as ANDROSCANREG (Android Permissions Scan Registry) which extracts and analyses the requested permissions in android application using blockchain technology. This method uses two blockchain namely: PERMBC and BTCBC. PERMBC analyses, validates and prepares the raw results to pertain in second block chain whereas BTCBC saves the history of permissions of all applications scanned through financial transactions. Intruders private data with the administrator permissions are encrypted and destroyed by downloading and installing the malicious modules in the file.

Shaukat et al. [21] proposed a dynamic API calls and framework calls to track and study booster vector machines, J48, IBk, BayesNet Pool, BayesNet K2, Random Forest, and Naive Bayes were used for their approach and found that the proposed model outperformed the existing ones. The machine learning like SVM, Linear regression, naive bayes, etc. are described in article [22] for security detection. Also role of ML in security application are discussed in article [23]. The AI advantages and needs for future employment is discussed in paper [24]. Machine learning used in cyber security and detection of malware is discussed in paper [25].

3 Proposed MLBCT-M Detect Methodology

One of the main challenges in internet of medical things is handled by proposing a malware detection scheme using Machine Learning technique and blockchain technology. The proposed method MLBCT-Mdetect employs two machine learning techniques namely: feature extraction and classification then it develops a blockchain based detection framework. Feature extraction and classification approaches trains the model and uses blockchain to distribute the new malware information. Distributed ledger records all type of malware that helps to train the model to detect malware efficiently. Dynamic malware detection is enabled in this model by placing the detected malware data into the blockchain database. Implementing the proposed system will run in the following manner. Developed machine learning models will identify the malware and retrain the model for effective detection. Information regarding to the new malware is stored in the blockchain. Intruders might introduce a new attack which is also stored in the blockchain database. The architecture of the proposed framework is shown in Fig. 2.

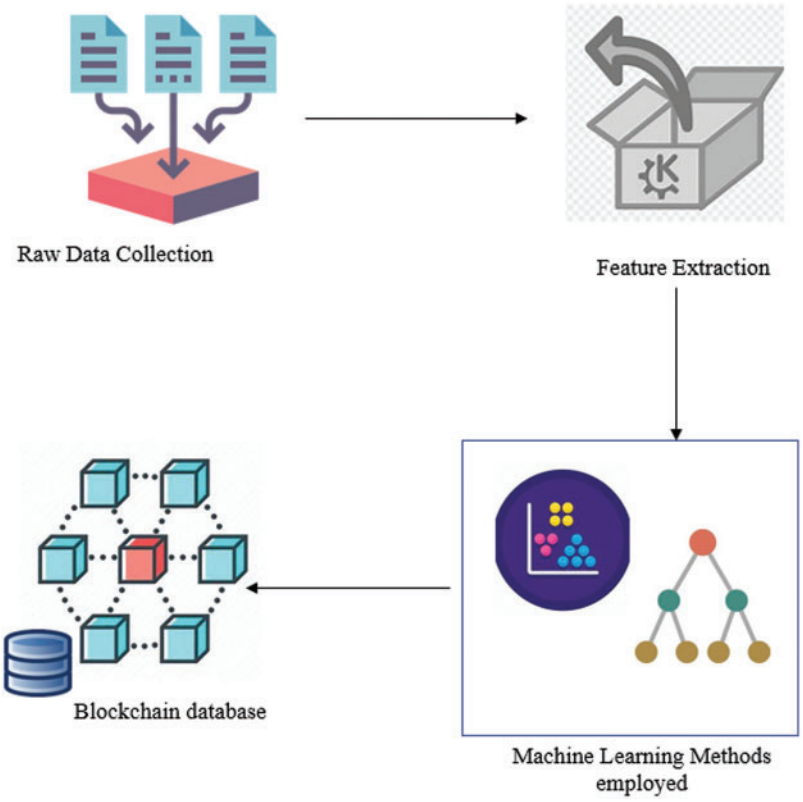

Figure 2: Architecture of proposed framework

3.1 Fuzzy C Means Feature Extraction

Feature Extraction is initiated by taking raw data as input. The input given is (xi, ti) in which xi representing set of attributes and ti represents the label. Si attributes which is a set of xi is extracted for classifying the malware nodes and benign nodes.

The steps involved in Fuzzy C Means (FCM) feature extraction are Pre-processing, clustering the data and extracting the features for classification. In the pre-processing stage, all the attributes are converted to numeric data to be used for clustering process. Medical data can be in any form in the case of ECG and EEG signals, Haar wavelet is used to compress the waves into predefined points. Few data values are normalized within the range of 0 to 1. Clustering stage is the heart of feature extraction where it takes pre-processed data as input and labels are removed. FCM algorithm is described below in Algorithm 1.

Algorithm 1: FCM

Input: All Data points
Output: k clusters
Step 1: Initialize $U = [u_{ij}]$ membership matrix $U^{(0)}$
Step 2: Calculate center vectors $c^{(k)} = [c_j]$ with $U^{(k)}$

(Continued)

Algorithm 1: Continued

Step 3: find $C_i = \frac{\sum_{j=1}^{n} u_{ij}^{m} x_j}{\sum_{j=1}^{n} u_{ij}^{m}}$

Step 4: update U(k), U(K + 1)

Step 5: Compute $u_{ij} = \frac{1}{\sum_{k=1}^{c} \left(\frac{\|x_i - c_j\|}{\|x_i - c_k\|} \right)}$

Step 6: if $\|U^{(k=1)} - U^{(K)}\| < \in$ then stop else go to step 2

Initial step is to select the number of clusters and initialize the membership matrix U. Cluster centers are calculated using cluster centers are chosen in such a way that centers should be cluster to points with higher membership value. After computing the cluster centers U is updated as per the cluster center location. New membership value of a point is calculated with the distance of the point from all cluster centers. The same process is repeated until the membership matrix is minimized. The attributes here do not take part in contributing to cluster centers even though they are obtained in K-dimensional space. The steps implemented for extracting features are shown in Algorithm 2.

Algorithm 2: Feature extraction

Input: n clusters, k attributes
Output: Relevant Features

```
Dist = φ, mdis = φ, Attr = φ
For i = 1 to k
For j = 1 to n − 1
For l = j to n
   Dist = dist(U) min (dist)
End for
End for
   mdis = (mdis) Union min (dist)
end for
for i = 1 to k
   attr = attr union max (mdis)
end for
end
```

The list of attributes is listed in 'attr' in which the most relevant attributes are listed first in 'attr' and least relevant attributes are at the end of 'attr'. The most relevant attributes are chosen for the next stage in the proposed method. The workflow of proposed MLBCT-Mdetect is depicted below in Fig. 3.

3.2 Multi-Feature Classification

SVM based decision trees are used for multi featured classification. Previous studies have shown DREBIN [26] was developed for statistical analysis to build datasets based on application programming interface. SVM was found to be efficient in malware detection. Attribute of proposed MLBCT-Mdetect is shown in Tab. 1 and the flowchart of SVM based decision tree is shown below in Fig. 4.

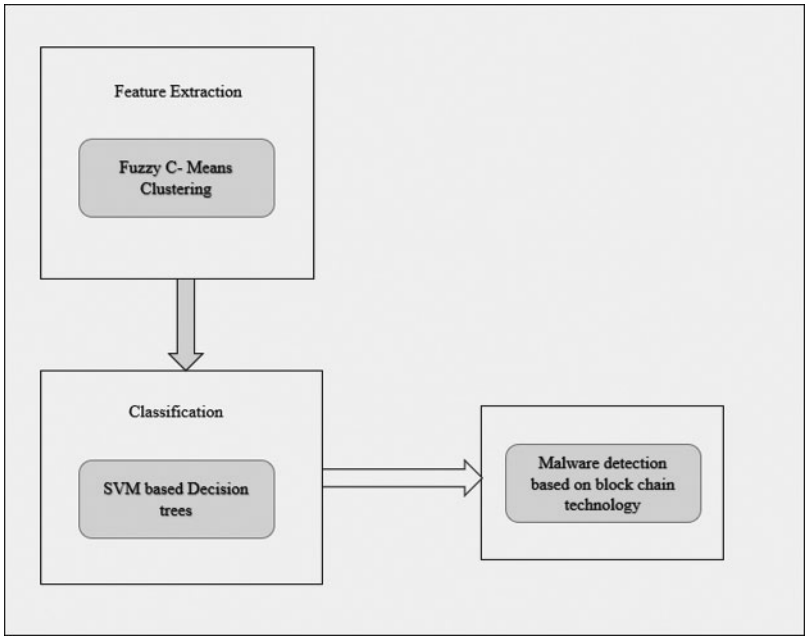

Figure 3: Workflow of proposed MLBCT-Mdetect

Table 1: SVM classifier attributes

Attribute	Description
T	Training dataset (x_{i1}, x_{i2} … x_{in})
D	Data collection attributes
D_t	Training dataset–attribute subset
W_i	Weight
A_i	Attribute
C	Class set
x_i	Training instance

3.3 Blockchain Based Malware Detection

Blockchain technology with consensus mechanism is gaining more attention. Different consensus algorithms namely Proof of Work (PoW), Delegated Proof of Stake (DPOS), Practical Byzantine Fault Tolerance (PBFT), Proof of Stake (PoS) gains deep insight into IoMT data stored in block chain. A framework is designed where a blockchain based framework is used for storing malware information. Benefits of security and fault tolerance between node are the characteristics of consensus mechanism. All the nodes can communicate with each other nodes very easily and any node can join the network or leave the network in a comfortable way. All the nodes can transfer information to the neighbouring nodes. A request response pattern is built by synchronous block. Malware features are stored in storage layer and the blockchain provides all information through distributed blocks. Features stored in blocks cannot be modified and features such as risky permission and suspicious API are stores in block which

cannot be altered. Tab. 2 shows the blockchain attributes and Fig. 5 depicts the blockchain based malware detection structure for IoT devices.

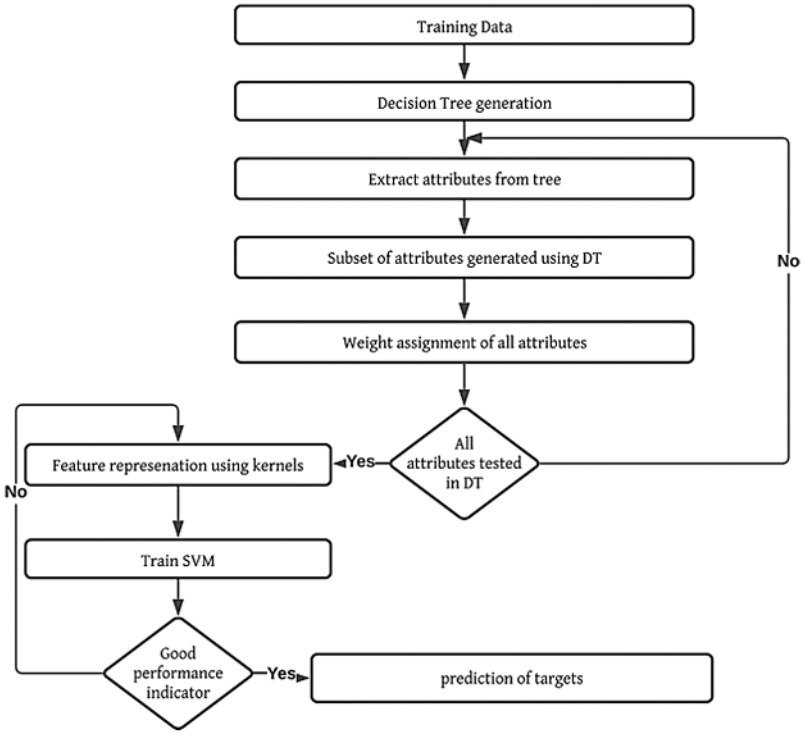

Figure 4: Flowchart of SVM based decision tree

Table 2: Blockchain attributes

Keywords	Definition
Pre-hash	Preceding block hash value
Version number software	Number to track the protocol or to update
Timestamp	Stores time of block
Transaction count	Number of malwares in current block
Root	Malicious codes detected by block

The users are protected from malicious application through blockchain technology. The two sections of a block are head section and data section. Head section stores root, version number, hash value etc . . . Data section stores the details of the malware like name, type of family, permission data, sensitive behavior data APK feature and transaction hash. Exact information stored in distributed malware database increases the speed and accuracy of detecting the malware. The frauds are detected efficiently by the unique hash value. Malware name, package features, hash value permission feature, API call feature of the malware are stored in every data block.

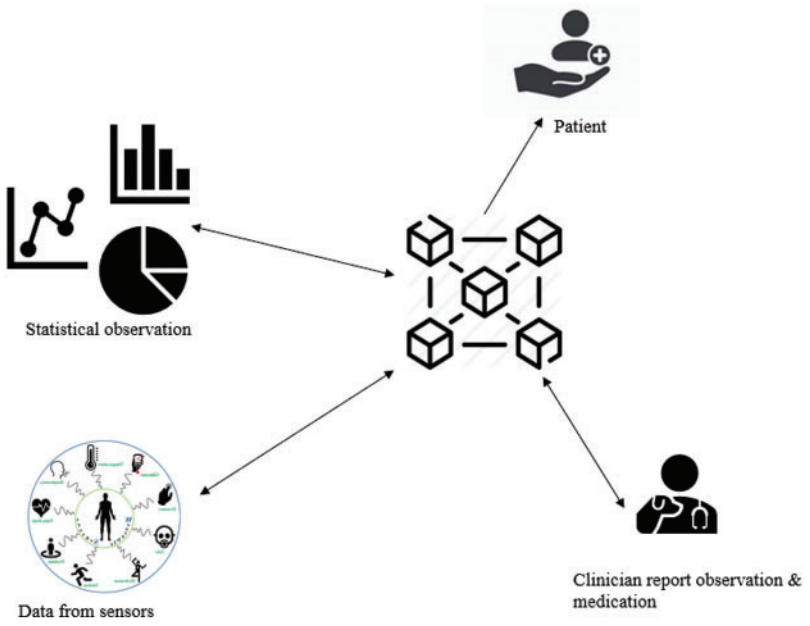

Figure 5: Blockchain based malware detection for internet of things

4 Results and Discussions

The dataset used for evaluating the proposed MLBCT-Mdetect has infected and uninfected an application which counts to 545 benign and 421 malware applications. True Positive Rate (TPR), false positive Rate (FPR) and Accuracy are the measures considered for evaluating the proposed scheme. Comparison of the performance of proposed method leads to be applied in malware detection in IoMT devices. MLBCT-Mdetect surpasses the results of the existing models in terms of dynamic detection of malware. New malwares are also added dynamically in the blockchain for efficient detection that improves the accuracy further. MLBCT-Mdetect proves to be effective by integrating techniques from machine learning models and blockchain technology for the effective detection of malwares in IoMT devices.

True positive rate is computed using Eq. (1).

$$TPR = \frac{T_P}{T_P + F_N} \tag{1}$$

False positive rate is computed using Eq. (2).

$$FPR = \frac{F_P}{F_P + T_N} \tag{2}$$

Accuracy is computed using the below Eq. (3).

$$Accuracy = \frac{T_P + T_N}{T_P + T_N + F_P + F_N} \tag{3}$$

The importance of extracted features is shown through the experimental results. The clustering method used in the proposed MLBCT-Mdetect optimizes the features with the results shown in Fig. 6. Red colour indicates the malware samples and blue colour indicates benign samples.

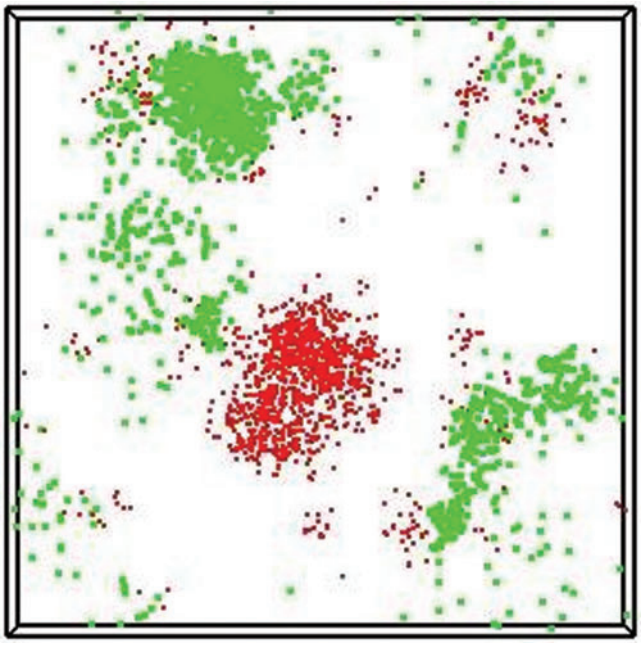

Figure 6: Clustering benign and malware samples

The proposed MLBCT-Mdetect is employed and compared with three classifiers namely: Naïve bayes, K-Nearest Neighbor (KNN) and Random Forest. The results of the above classifiers are shown in Tab. 3.

Table 3: Results observed from different classifiers

Algorithms	Accuracy	TPR	FPR
Naïve Baye	87.78	82.2	56.3
KNN	85.12	81.1	58.23
Random forest	86.23	80.12	54.21
DT-SVM	98.87	97.8	17.23

It is observed from the above table that accuracy percentage is higher with DT-SVM classifier with 98.87% compared to Naïve bayes, KNN and Random Forest with 87%, 85% and 86% respectively.

It is evident from Tab. 3 that SVM classifier achieves better accuracy compared to other classifiers which is employed in proposed method. MLBCT-Mdetect is efficient in terms of feature extraction and speed to detect the malware and benign samples. Fig. 7 clearly depicts the TPR and FPR for Naïve Bayes, KNN, Random Forest and SVM. Support vector machine scores highest TPR rate compared to other classifiers and FPR also seems to be less compared to Naïve bayes with 56%, KNN with 58%, Random Forest with 54% and SVM with 17%. To prove the efficiency of MLBCT-Mdetect the results are compared with n-grams malware detection. Results of proposed and existing method are compared

in terms of accuracy and processing time which is shown in Figs. 8 and 9. To show that the proposed method is significant, the results are compared with existing state of art method malware detection which is implemented for other applications. The detection is proved to be effective by comparing MLBCT-Mdetect and n-grams in terms of Accuracy of detection, precision rate and recall rate.

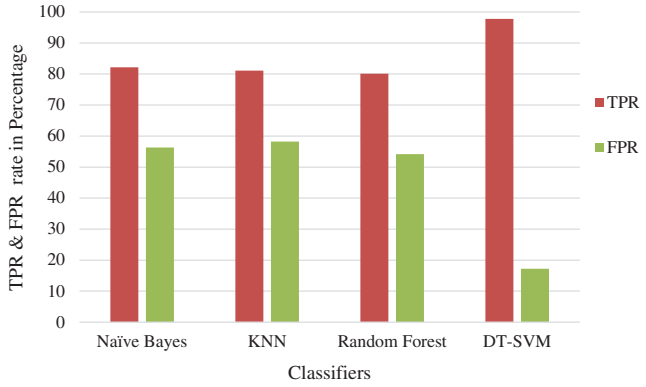

Figure 7: Comparison of TPR and FPR in classifiers

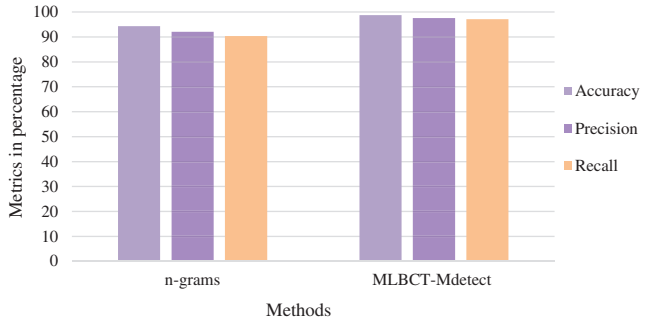

Figure 8: Accuracy, precision and recall of proposed and existing method

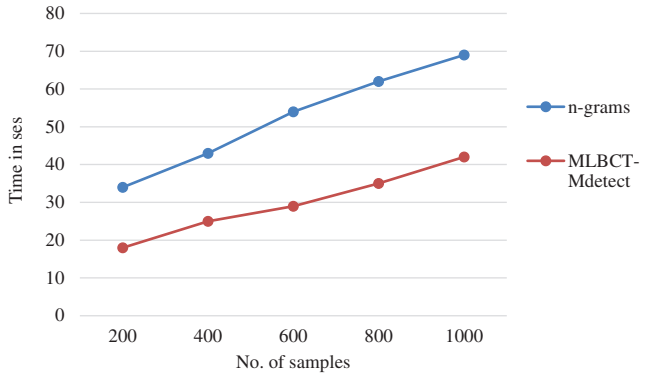

Figure 9: Comparison of processing time

MLBCT-Mdetect proves to be very efficient from the Fig. 9 with accuracy 98%, precision 97% and recall 97% whereas, n-grams malware detection seems to be not very efficient as MLBCT-Mdetect in terms of all compared measures.

Fig. 9 compares the processing time of MLBCT-Mdetect and existing n-grams method which clearly depicts the speed of the proposed method. Experiment is carried out for different number of samples and proved that the proposed MLBCT-Mdetect processes at a higher speed for all number of samples.

5 Conclusion and Future Enhancements

The technological advancement has driven us to smart environment with Internet of Things. IoT applications are diverse from sensing, agriculture, smart city development, smart vehicles and also set a path towards smart health care system (IoMT) which is the utmost essential application. With the wide use IoMT applications, there is more possibility of intrusions which may lead the patient health to critical stage. With an objective to detect the malwares in IoMT applications, this works proposes a novel scheme MLBCT-Mdetect to dynamically detect the malwares by integrating machine learning algorithms with block chain technology. Information regarding the intrusions is processed using machine learning algorithms and stored in blockchain database and transferred over the network to detect the further malwares efficiently. The new malwares detected are also added in the blockchain network during the runtime. The clustering method employed in the MLBCT-Mdetect extracts the relevant features to identify the samples into to malware samples and benign samples. In addition, classification is performed with Decision tree based SVM to address multi feature issues to achieve accuracy. Experimental results prove that the proposed method is excellent in terms of accuracy, precision and recall. The classifier (decision tree based SVM) employed in this work also outperforms with the existing Naïve bayes, KNN and Random Forest. MLBCT-Mdetect proves to be efficient in detecting the malwares with 98.78% accuracy and takes only 42 s to process 1000 samples. The limitation of the research is security cannot be highly achieved. This work can be enhanced further by implementing deep learning technology and also can be improvised by applying security mechanisms.

Acknowledgement: The authors would like to acknowledge the support of Prince Sultan University for paying the Article Processing Charges (APC) of this publication.

Funding Statement: The authors extend their appreciation to the Deanship of Scientific Research at King Khalid University for funding this work under Grant Number (RGP 1/279/42). www.kku.edu.sa.

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

References

[1] J. S. Park, T. Y. Youn, H. B. Kim, K. H. Rhee and S. U. Shin, "Smart contract-based review system for an IoT data marketplace," *Sensors*, vol. 18, no. 10, pp. 3577, 2018.

[2] B. L. R. Stojkoska and K. V. Trivodaliev, "A review of internet of things for smart home: Challenges and solutions," *Journal of Cleaner Production*, vol. 140, pp. 1454–1464, 2017.

[3] M. Damshenas, A. Dehghantanha, K. K. R. Choo and R. Mahmud, "Android: An android behavioral-based malware detection model," *Journal of Information Privacy and Security*, vol. 11, no. 3, pp. 141–157, 2015.

[4] Z. Liu, L. Zhang, Q. Ni, J. Chen, R. Wang *et al.,* "An integrated architecture for IoT malware analysis and detection," in *Proc. Int. Conf. on Information Technology & Systems*, Seattle, USA, pp. 127–137, 2018.

[5] J. Su, D. V. Vasconcellos, S. Prasad, D. Sgandurra, Y. Feng *et al.,* "Light weight classification of IoT malware based on image recognition," in *Proc. IEEE 42nd Annual Computer Software and Applications Conf. (COMPSAC)*, Tokyo, Japan, pp. 664–669, 2018.
[6] V. Clincy and H. Shahriar, "IoT malware analysis," in *Proc. Annual Computer Software and Applications Conf.(COMPSAC)*, Milwaukee, USA, vol. 1, pp. 920–921, 2019.
[7] C. Esposito, A. De Santis, G. Tortora, H. Chang and K. K. R. Choo, "Blockchain: A panacea for healthcare cloud based data security and privacy?," *IEEE Cloud Computing*, vol. 5, no. 1, pp. 31–37, 2018.
[8] P. Yan and Z. Yan, "A survey on dynamic mobile malware detection," *Software Quality Journal*, vol. 26, no. 3, pp. 891–919, 2018.
[9] H. Takase, R. Kobayashi, M. Kato and R. Ohmura, "A prototype implementation and evaluation of the malware detection mechanism for IoT devices using the processor information," *International Journal of Information Security*, vol. 19, no. 1, pp. 71–81, 2020.
[10] A. Azmoodeh, A. Dehghantanha and K. K. R. Choo, "Robust malware detection for internet of battle field things devices using deep eigenspace learning," *IEEE Transactions on Sustainable Computing*, vol. 4, no. 1, pp. 88–95, 2018.
[11] O. Arias, J. Wurm, K. Hoang and Y. Jin, "Privacy and security in internet of things and wearable devices," *IEEE Transactions on Multi-Scale Computing Systems*, vol. 1, no. 2, pp. 99–109, 2015.
[12] A. K. Das, M. Wazid, N. Kumar, M. K. Khan, K. K. R. Choo *et al.,* "Design of secure and lightweight authentication protocol for wearable devices environment," *IEEE Journal of Biomedical and Health Informatics*, vol. 22, no. 4, pp. 1310–1322, 2017.
[13] R. Kumar, X. Zhang, W. Wang, R. U. Khan, J. Kumar *et al.,* "A multimodal malware detection technique for android IoT devices using various features," *IEEE Access*, vol. 7, pp. 64411–64430, 2019.
[14] H. T. Nguyen, Q. D. Ngo and V. H. Le, "IoT botnet detection approach based on PSI graph and DGCNN classifier," in *Proc. Int. Conf. on Information Communication and Signal Processing (ICICSP)*, Singapore, pp. 118–122, 2018.
[15] S. M. P. Dinakarrao, H. Sayadi, H. M. Makrani, C. Nowzari, S. Rafatirad *et al.,* "Lightweight node-level malware detection and network-level malware confinement in iot networks," in *Proc. Design, Automation & Test in Europe Conf. & Exhibition (DATE)*, Florence, Italy, pp. 776–781, 2019.
[16] B. Aslam, A. R. Javed, C. Chakraborty, J. Nebhen, S. Raqib *et al.,* "Blockchain and ANFIS empowered IoMT application for privacy preserved contact tracing in COVID-19 pandemic," *Personal and Ubiquitous Computing*, pp. 1–17, 2021.
[17] H. Xu, L. Zhang, O. Onireti, Y. Fang, W. J. Buchanan *et al.,* "Beeptrace: Blockchain enabled privacy preserving contact tracing for Covid-19 pandemic and beyond," *IEEE Internet of Things Journal*, vol. 8, no. 5, pp. 3915–3929, 2020.
[18] S. Raje, S. Vaderia, N. Wilson and R. Panigrahi, "Decentralised firewall for malware detection," in *Proc. ICAC3*, Mumbai, India, pp. 1–5, 2017.
[19] A. Ouaguid, N. Abghour and M. Ouzzif, "A novel security framework for managing android permissions using blockchain technology," *International Journal of Cloud Applications and Computing*, vol. 8, no. 1, pp. 55–79, 2018.
[20] V. M. Afonso, M. F. De Amorim, A. R. A. Grégio, G. B. Junquera and P. L. De Geus, "Identifying android malware using dynamically obtained features," *Journal of Computer Virology and Hacking Techniques*, vol. 11, no. 1, pp. 9–17, 2015.
[21] K. Shaukat, S. Luo, V. Varadharajan, I. A. Hameed and M. Xu, "A survey on machine learning techniques for cyber security in the last decade," *IEEE Access*, vol. 8, pp. 222310–222354, 2020.
[22] K. Shaukat, S. Luo, V. Varadharajan, I. A. Hameed, S. Chen *et al.,* "Performance comparison and current challenges of using machine learning techniques in cyber security," *Energies*, vol. 13, no. 10, pp. 2509, 2020.
[23] K. Shaukat, F. Iqbal, T. M. Alam, G. K. Aujla, L. Devnath *et al.,* "The impact of artificial intelligence and robotics on the future employment opportunities," *Trends in Computer Science and Information Technology*, vol. 5, no. 1, pp. 50–54, 2020.

[24] K. Shaukat, S. Luo, S. Chen and D. Liu, "Cyber threat detection using machine learning techniques: A performance evaluation perspective," in *Proc. Int. Conf. on Cyber Warfare and Security*, Islamabad, Pakistan, pp. 1–6, 2020.
[25] D. Arp, M. Spreitzenbarth, M. Hubner, H. Gascon, K. Rieck *et al.,* "Drebin: Effective and explainable detection of android malware in your pocket," *Journal of Network and Distributed System Security Symp.*, vol. 14, pp. 23–26, 2014.
[26] I. Santos, Y. K. Penya, J. Devesa and P. G. Bringas, "N-grams-based file signatures for malware detection," in *Proc. Int. Conf. on Enterprise Information Systems, ICEIS*, Portugal, Italy, vol. 9, pp. 317–320, 2009.