Computers, Materials & Continua CMC, vol.65, no.1, pp.87-107, 2020

Privacy Preserving Blockchain Technique to Achieve Secure and Reliable Sharing of IoT Data

Bao Le Nguyen[1], E. Laxmi Lydia[2], Mohamed Elhoseny[3], Irina V. Pustokhina[4], Denis A. Pustokhin[5], Mahmoud Mohamed Selim[6], Gia Nhu Nguyen[7, 8] and K. Shankar[9, *]

Abstract: In present digital era, an exponential increase in Internet of Things (IoT) devices poses several design issues for business concerning security and privacy. Earlier studies indicate that the blockchain technology is found to be a significant solution to resolve the challenges of data security exist in IoT. In this view, this paper presents a new privacy-preserving Secure Ant Colony optimization with Multi Kernel Support Vector Machine (ACOMKSVM) with Elliptical Curve cryptosystem (ECC) for secure and reliable IoT data sharing. This program uses blockchain to ensure protection and integrity of some data while it has the technology to create secure ACOMKSVM training algorithms in partial views of IoT data, collected from various data providers. Then, ECC is used to create effective and accurate privacy that protects ACOMKSVM secure learning process. In this study, the authors deployed blockchain technique to create a secure and reliable data exchange platform across multiple data providers, where IoT data is encrypted and recorded in a distributed ledger. The security analysis showed that the specific data ensures confidentiality of critical data from each data provider and protects the parameters of the ACOMKSVM model for data analysts. To examine the performance of the proposed method, it is tested against two benchmark dataset such as Breast Cancer Wisconsin Data Set (BCWD) and Heart Disease Data Set (HDD) from UCI AI repository. The simulation outcome indicated that the ACOMKSVM model has outperformed all the compared methods under several aspects.

[1] Faculty of Information Technology, Duy Tan University, Da Nang, 550000, Vietnam.

[2] Computer Science and Engineering, Vignan's Institute of Information Technology, Visakhapatnam, 530049, India.

[3] Faculty of Computers and Information, Mansoura University, Mansoura, 35516, Egypt.

[4] Department of Entrepreneurship and Logistics, Plekhanov Russian University of Economics, Moscow, 115093, Russia.

[5] Department of Logistics, State University of Management, Moscow, 109542, Russia.

[6] Department of Mathematics, College of Science & Humanities in Alaflaj, Prince Sattam bin Abdulaziz University, Alaflaj, 16278, Saudi Arabia.

[7] Graduate School, Duy Tan University, Da Nang, 550000, Vietnam.

[8] Faculty of Information Technology, Duy Tan University, Da Nang, 550000, Vietnam.

[9] Department of Computer Applications, Alagappa University, Karaikudi, 630003, India.

[*] Corresponding Author: K. Shankar. Email: drkshankar@ieee.org.

Received: 18 May 2020; Accepted: 15 July 2020.

Keywords: Blockchain, optimization, elliptical curve cryptosystem, security, ant colony optimization, multi kernel support vector machine.

1 Introduction

In the era of big data, blockchain technology gained attention and prominence as the optimum technology to decentrally protect the data integrity and ensure data quality. All the data stored in blockchain can be copied and checked by all the nodes in the network. This provides reliable protection against attacks that violate data integrity [Li and Palanisamy (2018)]. For individuals, educational documents now describe their educational qualifications. These notes are of great importance for further education and their personal career. The main attribute of these records is the basic element with which, the records can restore the original historical situation. Therefore, these records are required for students, educational institutions and employers. With the development of information technology, the educational documents can be digitized [Li and Han (20190)]. E-commerce is becoming increasingly popular due to various factors such as different products, fast transactions, time, places and businesses. However, the disclosure of users' personal data such as 1) identification data, 2) addresses and 3) telephone numbers has become the main challenge in online trade activities [Jiang, Wang, Wang et al. (2019)]. In Industry 4.0, the amount of data generated by connected devices in the IoT model has increased enormously. Data leaks can occur at any point of time between data storage, data transmission and data exchange. This can lead to serious problems for both owners as well as suppliers [Lu, Huang, Dai et al. (2019)]. There is an increasing interest shown upon using blockchain technology to promote medical and electronic health services in the recent times. A decentralized and reliable blockchain has shown enormous potential for secure exchange of electronic Health Records (EHR) in various areas of electronic health services and for the management of data access in many medical facilities [Nguyen, Pathirana, Ding et al. (2019)].

Another risk associated with file sharing is peer-to-peer networks. In this area, the user copies whatever he or she believes to be an expensive file from the boot loader. However, the downloaded file is useless instead of which fake content is stored on the system for a hidden purpose. Although IoT technology seems to be exciting and solves many problems in real time, it is challenging to ensure security and data protection in IoT platform due to its features such as low processing power, distributed behavior and lack of standardization. To get rid of this disadvantage, researchers from industry and science concentrate on the basics of blockchain and started adapting blockchain-based cryptocurrency models for IoT applications [Rahulamathavan, Phan, Rajarajan et al. (2017)]. Support Vector Machine (SVM) is a kind of controlled learning model that can be used to efficiently classify the data across all ML models. Therefore, SVM is used in many areas especially to solve real classification problems in smart cities with IoT support [Shen, Tang, Zhu et al. (2019)]. Blockchain was first proposed and applied in digital currency. Other uses of blockchain are currently being carefully explored, and the announcements are made almost daily about how it impacts everyday life. In line with this, the blockchain has been examined in the area of financial services to ensure trust,

simplicity and efficiency in financial transactions [Tahir and Rajarajan (2018)]. EHR sharing has received widespread attention and research in industry as well as research institutes. In this research area, data protection, data security and compatibility are considered as the most important issues [Wang, Zhang, Zhang et al. (2019)].

A distributed consensus algorithm ensures that the network can perform efficient self-service, information gathering, and has an encryption mechanism to ensure point-to-point transmission security. Blockchain technology is almost similar to cars network [Xu, Liu, Li et al. (2018)]. The recent studies show that the blockchain is applied in a variety of industries such as advertising, business development, healthcare and logistics, and these findings are similar to AI and AI. High-level transactions, for instance financial transactions, require similar protection to protect the user privacy [Yaji, Bangera and Neelima (2018)]. However, in some applications, it is better not to release the entire content of the transaction though the transaction mechanism can be allowed to perform. For example, an application that handles real estate sales should keep the transaction amount confidential. Hackers attempt to track the flow of stolen coins but it remains difficult because the developers use a lot of addresses. Such money laundering can also be used [Yasusaka, Watanabe and Kitagawa (2019)]. Blockchain is a new technology that can offer a variety of benefits to mobile business applications. This technology provides the maximum efficiency and confidentiality in the practical usage of sharing alerts. Blockchain technology is very convenient for app developers who can design and develop the application in a secure manner from business point of view [Devi and Pamila (2019)]. The authors assessed the existing studies and propose a secure DML model for a network of approved blockchains to solve the critical issues described. It can provide better system performance compared to other low-resolution blockchains [Kim, Kim, Hwang et al. (2019)].

Generally, the extensive adoption of smart products is based on the capability of organizations to offer systems which assures enough data integrity while guaranteeing sufficient user privacy [Namasudra, Roy, Vijayakumar et al. (2017)]. In light of these issues, earlier studies indicate that the blockchain technology is found to be a significant solution to resolve the challenges of data security exist in IoT [Namasudra and Roy (2017); Namasudra (2018)]. At the same time, with the ever-evolving nature of newer statistical techniques infringing user privacy, artificial intelligence (AI) algorithms designed for user privacy can offer a dynamically adaptive solution for preserving user privacy over the rising multidimensional relationships that datasets create [Namasudra, Devi, Kadry et al. (2020)]. In Though various models have been available in the literature, there is still a need to increase the performance of the security model [Li, Wang and Yang (2019); Alguliyev, Aliguliyev and Sukhostat (2020)]. Besides, the blockchain and hybridization model can lead to effective results over the compared methods.

In this study, the authors introduce a training program called Secure ACOMKSVM, a privacy-preserving Secure Ant Colony optimization with Multi Kernel Support Vector Machine (ACOMKSVM). This program uses blockchain to ensure protection and integrity of some data while it has the technology to create secure ACOMKSVM training algorithms in partial views of IoT data, collected from various data providers. Elliptical Curve Cryptography (ECC) is used to create effective and accurate privacy that protects

ACOMKSVM secure learning process. The researchers demonstrated the efficacy and safety of a dynamic ACOMKSVM. In this study, the authors deployed blockchain technique to create a secure and reliable data exchange platform across multiple data providers, where IoT data is encrypted and recorded in a distributed ledger. The safe blocks were developed like a safe ECC. The security analysis showed that the specific data ensures confidentiality of critical data from each data provider and protects the parameters of the ACOMKSVM model for data analysts.

2 Literature survey

With increasing use of Video Surveillance Systems (VSS), more and more people started showing their interest towards privacy issues. Though most of the people in general view 'surveillance' as a means of preventing crime, they do not accept aggressive surveillance of their personal lives. However, there is still no simple and secure solution to protect the confidentiality of VSS. The recent success of Blockchain (BC) technologies and Internet of Things (IoT) applications shed light on this complex issue. Fitway et al. [Fitwi, Chen and Zhu (2019)] proposed a lightweight blockchain-based data protection scheme (lip-pro) for border surveillance cameras. This scheme allows the VSS to restrict the privacy of people who have copied the video without any compromise. VSS, developed by Lipsy System, converts it into a federal blockchain network. This can perform integrity tests, fuzzy key management, functionality sharing and video access. It is useful in the implementation of policy-based data protection measures on external devices for real-time video analysis without any network congestion.

Diabetes is one of the most common global diseases and requires daily self-care to combat it. Diabetes self-monitoring currently uses state-of-the-art innovations such as Internet of Things (wearables and medical sensors) to evaluate and track the information on well-being. Azbeg et al. [Azbeg, Ouchetto, Andaloussi et al. (2018)] reported IoT and blockchain-based stage to facilitate diabetes' surveillance and help patients manage their disease properly. The study organization coordinated the Internet of Things with blockchain innovations so as to ensure patient protection, ongoing data collection and ongoing exchange with respective clinical teams.

With the introduction of big data, it becomes highly important to create a powerful and effective calculation of Artificial Intelligence to process a large amount of information. In general, the information consists of several sections and is transmitted geologically, which contributes to the appropriation of artificial intelligence. Traditionally-assigned AI computing uses a reliable focus server on the basis of Ace standards and focuses on the security issue in direct learning models. However, the protection of indirect learning and security models is eliminated. To deal with these problems, Chen et al.'s research [Chen, Ji, Luo et al. (2018)] on blockchain proposed a decentralized system of secure protection and learning called Learning Sync for a typical learning model (linear or nonlinear) without a targeted and reliable server. In particular, this study created a decentralized Stochastic Gradient Descent (SGD) in order to test the entire blockchain price model. In Decentralized SGD, the authors created various restrictive structures to ensure the security of each assembly. Further they also offered a common learning chain to protect the structure from Byzantine attacks. A hypothetical study was conducted about the

classification and safety of the proposed teaching method. At the end, the researchers completed the Ethereum training chain and demonstrated its viability and productivity through extensive testing.

Since the state of the system offers various options for information range, the trend towards 'intelligent' systems has led to its development. The existence of various structures for exchange/transmission of information is considered as an important factor that provides insightful control/management at an intellectual stage. However, security and protection issues are usually addressed by providing administrations with custom correspondence, such as: attacks on the use of viability and distribution of funds. Gai et al. [Gai, Wu, Zhu et al. (2019)] proposed a Permissioned Blockchain Edge Model for Smart Grid Network (PBEM-SGN), which combines square chain and limit registration methods to solve three remarkable problems: brilliant systems, information security, and viability security. This study used group tags and strategies to confirm covert channels and ensure customer safety. The best security measures were taken in this study through clear agreements that were updated on the blockchain. The tests conducted in this study evaluated the appropriateness of the proposed approach.

Electric cars are integral parts of V2G systems and are driven by system alike other electric vehicles. It is possible to regularly supply the frame with alcohol. V2G installment payment records allow you to dynamically monitor, organize, evaluate and use the data upon customer behavior and increase the productivity. In any case, though a safe and reliable exchange process is still a challenge, the information about the company and customers in installments can result to real information insurance problems. Gao et al. [Gao, Zhu, Shen et al. (2018)] organized and strengthened the information business with the help of security system that was developed on the basis of square chain. This had information security as a base for V2G to protect the personal data of customers. This strategy allows one to add and track information based on the blockchain strategy. Thus the confidentiality of customer offers is ensured and the viewing of episodes by specialized customers also gets increased. This work heavily relied upon Hyperledger to carefully evaluate its feasibility and feasibility.

Currently, New Zealand does not have a complete Electronic Health Record (EHR) system integrated into a huge number of clinical organizations, for example B. Ambulance, clinic and specialists. Due to its advantages, blockchain innovation is an ideal phase for New Zealand to create a wide range of ECM structures. Huang et al. [Huang, Qi, Asghar et al. (2019)] investigated a MedBlock that records a longitudinal section of the patient's medical history and allows the patients to accept or revoke access to their records. MedBlock uses an encryption tool to protect the clinical information while the access control is dependent on consent. It shows how blockchain can act as a freely accessible HER environment predominantly in New Zealand. It further shows how blockchain affects the whole field of clinical innovation.

The recent developments in the Internet of Things (IoT) made the Internet of Vehicles (IOV) and Intelligent Transport Systems (ITS) ready for future use. Intelligent Transport Systems (ITS) requires Vehicular ad-hoc networks (VANETs) in which Intelligent Vehicles (IV) act as primary vehicles. In order to ensure the best and most reliable operation of VANET, IVs are important to provide internet association with a secure system and a reliable source of

information (provenance). Javaid et al. [Javaid, Aman and Sikdar (2019)] used Physical Unclonable Functions (PUFs) in order to ensure consistent quality of information. The driver design shows that it can improve traffic confidence and ensure the security of the information business without any compromise on the confidentiality.

In Medhane et al. [Medhane, Sangaiah, Hossain et al. (2020)], a blockchain enabled distributed security model utilizing edge-cloud and software defined networking (SDN) is introduced. Here, the security attacks are detected are attained and the cloud layer and the security attacks are subsequently minimized at the edge layer of the IoT network. The SDN based gateway provides dynamic network traffic flow management, which contributes in the security attack detection by computing doubtful network traffic flows and reduces security attacks by hindering doubtful flows. In Ren et al. [Ren, Liu, Ji et al. (2018)], a blockchain technology is used for building the primary incentive process of nodes as per data storage for wireless sensor networks (WSNs). Here, the nodes which stores the data gets a reward as digital money. Besides, this method employs provable data possession for replacing proof of work (PoW) in actual bitcoins for performing mining and storing new data blocks.

In Xia et al. [Xia, Tan, Wang et al. (2019)], a trading model of the power surplus market is developed and a smart contract for multi-party bidding power resources depending upon blockchain technology, and attained the decentralized power trading decisions for ensuring the details is symmetric as well as fair. Besides, the credibility technique is developed by examining the client's recent transaction record and developed a respective punishment mechanism for strengthening the limitation on the execution of offline point-to-point power transactions. In Zhang et al. [Zhang, Zhong, Wang et al. (2020)], the possible issues, challenges and opportunities for the design of numerous blockchain based systems in the future. In Gu et al. [Gu, Yang and Yin (2018)], a privacy protection of location data mining has been presented. Besides, a location data record privacy protection model is developed using differential privacy mechanism and make use of the structure of multi-level query tree to query and publish location data on database. In He et al. [He, Zeng, Xie et al. (2017)], a distributed privacy preserving model for random linear network coding in smart grid has been presented. It makes use of the converged flows character of the smart grid and make use of homomorphic encryption function for reducing the complexity exist in the forwarding node.

In Min et al. [Min, Yang, Wang et al. (2019)], an efficient Boneh, Goh and Nissim (BGN) type parallel homomorphic encryption algorithm has been introduced. Particularly, the presented model makes use of the features of the multi-nodes in cloud platform for conducting parallel encryption using block matrix multiplication, and concurrently perform the group-wise ciphertext computation. In Yin et al. [Yin, Ju, Yin et al. (2019a)], a new privacy protection technique using location sensitivity for location recommendation has been proposed. It makes use of location trajectory and check-in frequencies for setting a threshold for classifying the sensitivity level of the locations. In Yin et al. [Yin, Shi, Sun et al. (2019b)], a new privacy-preserving collaborative filtering technique has been presented based on differential privacy protection and time factor. In Yin et al. [Yin, Zhou, Yin et al. (2019c)], a privacy protection is integrated to machine learning, in which a logistic regression is applied for

local differential privacy protection is developed for achieving classification process using noise addition and feature selection. Though various models have been available in the literature, there is still a need to increase the performance of the security model. Besides, the blockchain and hybridization model can lead to effective results over the compared methods.

3 Proposed methodology

In this study, the authors introduce a training program called Secure ACOMKSVM, a privacy-preserving Secure Ant Colony optimization with Multi Kernel Support Vector Machine (ACOMKSVM). This program uses blockchain to ensure protection and integrity of some data while it has the technology to create secure ACOMKSVM training algorithms in partial views of IoT data, collected from various data providers. Elliptical Curve Cryptography (ECC) is used to create effective and accurate privacy that protects ACOMKSVM secure learning process. The researchers demonstrated the efficacy and safety of a dynamic ACOMKSVM. In this study, the authors deployed blockchain technique to create a secure and reliable data exchange platform across multiple data providers, where IoT data is encrypted and recorded in a distributed ledger. The safe blocks were developed like a safe ECC. The security analysis showed that the specific data ensures confidentiality of critical data from each data provider and protects the parameters of the ACOMKSVM model for data analysts.

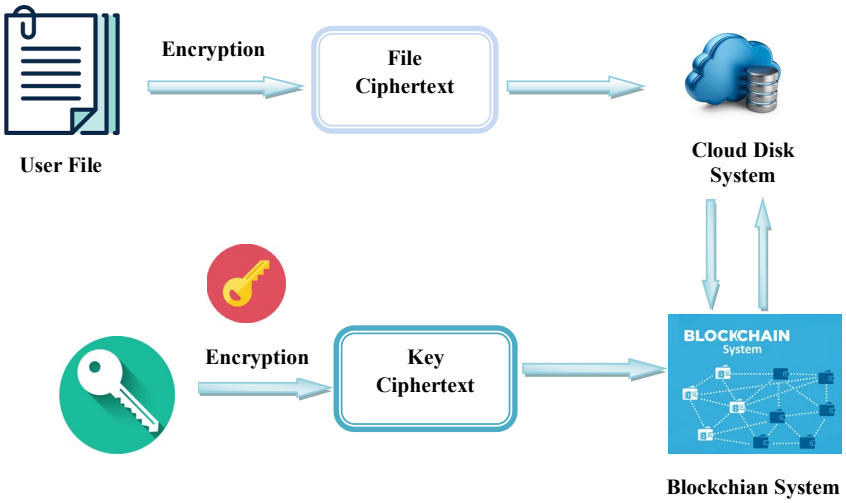

Figure 1: Privacy preserving block chain structure

Here, two or more IoT data providers are allowed to consult with an IoT data analyst to steal the privacy of other partners. The following assumptions are made: There may be interest in the personal information of other areas that actually enforce the protocol, but not others. Two or more participants can work together in this process. As passive adversaries, they follow the protocol while at the same time, they try to increase the privacy of others from the values they learn. The current study program aims at

protecting the privacy of each member and securely configure the ACOMKSVM model. Specifically, the confidentiality of each IoT data provider lies in their IoT records along with the parameters of IoT Data Analyzer ACOMKSVM model. The security objectives are defined as follows:

1. The confidentiality of IoT data analytics and the confidentiality of each IoT data provider face competent, but honest competitors.

2. When two or more conflicting parties collide, the confidentiality of each IoT data analyst and each IoT data provider is kept confidential.

A dataset B is a type of transaction record with its dimensions, $|B|$ where Ri denotes the i^{th} record of B, and Si denotes the same label as *Ri*. Set w and b to two corresponding ACOMKSVM parameters. Slope learning ∇t is a downward slope in the implementation of ACOMKSVM learning algorithm and λ is the learning rate. In this article, a more or less homogeneous cryptosystem called ECC cryptosystem was used and was referred to the encryption, while [[m]] represents the encryption of m under ECC.

3.1 Elliptic Curve Cryptography (ECC)

Elliptic Curve Cryptography (ECC) is a method of encrypting public keys, set in the algebraic structure of elliptic curves in bounded fields. This short key is faster and requires less computing power than other first-generation encryption public key algorithms. The advantages of ECC over RSA are particularly important in wireless devices, where computing power, memory and battery life are limited. Equivalent ECC security requires smaller keys that are equivalent to encryption outside the ECC (based on simple Calois fields). Both private and public keys, created by the ECC system, protect the encrypted data. The general equations of the elliptic curve are shown in Eq. (1),

$$S^2 = r^3 + ar + b \pmod{y} \tag{1}$$

Here a, b and y are random numbers and spaces equals y from $0 \, to \, n-1$.

By changing the above values, different values y are attained and so many points are achieved. From these points, the private key is selected. The public key is also calculated from the private key. The public key formula is shown in Eq. (2).

$$pu(k) = pr(k) * y \tag{2}$$

where, $pu(k) \, and \, pr(k)$ -depict public and private keys. Then the public key is calculated. Following is the process that shows the usage of encryption and encryption keys.

3.1.1 Encryption

Encryption is the process of encoding information and data, especially to prevent unauthorized access. Here are the following two cipher text keys Eq. (3),

$$d_1 = K \times y \tag{3}$$

where K ranges from $1 to \, n-1$

$$d_2 = message + K \times pu(k) \tag{4}$$

These are the two keys to the cipher text.

3.1.2 Decryption

Decryption is the process of getting encrypted or encrypted text into other data and converting it into computer-readable and understandable text. This term can be used to refer non-manual encryption of data, as a method of data encryption, using appropriate codes or keys. With this method, one can get a real message.

$$Message = c2 - pr(k) * c1 \tag{5}$$

The original message is received with private key. In nodes, the messages are encrypted with public and private keys. The encrypted messages are eventually sent to the base station with optimal cluster header. The Grass hopper optimization Algorithm is used here to select the optimal key in ECC. After encryption, the document is stored in the cloud with an access structure that defines the types of users who can access the document.

3.2 Privacy preserving ACOMKSVM classification

In the current study, during training, the readiness of the ACOMKSVM rule is updated, which, as a rule, creates equivalent conditions. Thus it implies the need to update these ACO conditions and some ideal conditions. MKSVM is a guided learning model that provides hyperplane with maximum advantage with which the test information can be characterized. An information expert can be deployed here to prepare the ACOMKSVM models based on the information retrieved from various IoT information providers. Each IoT information provider processes few examples of IoT information, encrypts it locally using their own keys and communicates with the receiver with a record dependent on the common square chain and perform the exchanges. An information expert, who needs to prepare the ACOMKSVM model, can access the encrypted information recorded in the Global Book and use a safe learning strategy with several preparatory modules. The relationship between the information expert and each data provider remains crucial for sharing intermediate results in the learning process.

There are adequate evidences available for the problem i.e., the consequences of ants' growth can be obtained using a probability conversion strategy based on determining the number of pheromones in the path and on the heuristic dependence of a limited multifaceted nature.

- Explanation of a strategy for providing meaningful results that are suitable for complex results, in explicit world conditions.
- A difficulty-reliant heuristic operation (η) determines the impact of the article which can be related to the running subtotal.
- A pheromone update controller decides how to restore the pheromone (τ).
- The sequence of changes in probability depends on the value of heuristic ability (η). and on the importance of pheromone path (τ) associated with reactivation of the device.

3.2.1 Pheromone initialization

At first, the ground state of the pheromone is protected for all properties of I and their earthly estimates, l. There are many pheromones in each channel while on the contrary, it undeniably corresponds to the size of each individual virtue, which induces the accompanying condition:

$$\tau_{il}(h=0)=\frac{1}{\sum_{i=1}^{x} y_i} \tag{6}$$

where x is the absolute number of features and y_i is the number of qualities in the field of materials i.

3.2.2 Rule construction

The control gets improved by blowing each print in turn. The decision of the joint depends on the probability specified in Eq. (7).

$$p_{il(t)}=\frac{\tau_{il(t)}.\eta_{il}}{\sum_{i`}^{a}\sum_{l}^{bi}\tau_{il}(t).\eta_{il},\forall i\in I} \tag{7}$$

where η_{il} implies the indicator of the unshakeable for $term_{il}$, τ_{il} quality of the multifaceted nature for the measurement of the pheromone (at time h), currently available in the accession phase and embraced by I and dignity, represents a great uniqueness that has not yet been fulfilled in the field of properties *i*.

3.2.3 Heuristic function

The use of heuristics η depends on the number of realities associated with property i and the number of realities transferred per condition n.

$$Info\,H_{il}=\sum_{w=1}^{k}\left[\frac{FreqH_{il}W}{\left|H_{ij}\right|}\right]*\log^2\left[\frac{Freq\,H_{il}W}{\left|H_{il}\right|}\right] \tag{8}$$

where *k* is the size of classes, $\left|H_{il}\right|$ denotes the sum of conditions in the segment H_{il} (evaluation of the state taking into account that A_i has value V_{il}), freq H_{il} , w is the set of fragment states H_{il} among class and a is the general arrangement property.

$$\eta_{il}=\frac{\log(K)-Info\,H_{il}}{\sum_{1}^{x}\sum_{l}^{yi}\log_2(K)-Info\,H_{il}} \tag{9}$$

Despite the inadequate control point H_{il} , the development of underground insect decreases. Further, the more accurate the control point $Term_{il}$, higher the accuracy of the requirements for ants. With the help of primary class of nature including authoritative

foundations, this tipping point can be applied to the class and this should be pursued with a certain moderate speed. The correct hypothetical methodology is proposed, and its use requires a critical improvement in quality. The result is considered as the space of the structure satisfying condition of Eq. (10).

$$Q = \left[\frac{TruePositive}{TruePos + FalseNeg} \right] * \left[\frac{TrueNegative}{FalsePos + FalseNeg} \right] \tag{10}$$

where True Pos is the number of terms remembered for manual and the class associated with the draft manual is included. A False Pos is an unexpected class compared to a regular False Neg which contains a class of impromptu. This denotes the number of provisions which do not offer any policy guidance. True Neg is the number of conditions that do not extend the manual and contains a class other than the class prescribed by the manual.

$$\tau_{il}(H+1) = \tau_{il}(h) + \tau_{ij}(h) * Q \forall term_{il} \in \tag{11}$$

In order to personify the event of weeding pheromones in the legal conspiracy of insect provinces $Term_{il}$, the size of pheromones of those not-required, in the developed law, can be ignored. The absence of inactive articulatory pheromones τ_{il} is achieved by reducing each and every score and divide the scores of each person τ_{il}.

3.2.4 Pheromone update rule

The change in pheromone is performed after each subterranean insect gained control according to the condition (16) below. Since the researchers are doing this to simplify the ACO, an extended guide is attained. These rules are provided as a contribution to MKSVM. This secure MKSVM prepares multicomponent encoded information, including a structure model, hazard model, and structure objectives.

3.3 Multi kernel support vector machine

The authors' efforts include the creation of an ACOMKSVM model information provisioning plan for numerous IoT providers. The study considered the information security threats when transferring the information between information providers and information experts. The information expert is considered as a genuine challenger with curiosity. Thus, the information researcher can indeed follow the predefined agreements on the preparation of ML. At the same time, he or she may be interested in the context of information who may try to find out more by analyzing the confusing information in the center of the traffic information calculation.

The best properties available for the characterization rule are passed to Fusion Multi kernel support vector machine. A site selected from past history is productively used to disable two modules. According to the standard for managing nonlinear methods, the current research deployed SVM classifier. There are two important steps in SVM procedure such as readiness phase and the simple phase.

Training phase: Currently, the output of the attribute selection is 0 which is provided as an input to the preparation phase. The input utility offers a set of values that cannot be alienated. Almost every possible placement is separated by a difficult level. In

Lagrangian scheme, one can specify the partition of the standard vector of restless level during the problem of divergent core. In this regard, the kernel symbolizes several tasks related to the point product for a certain type of attribute record. However, recording a position in large size range can result in an unnecessary evaluation period and demands huge memory requirements. As a result, a certain work begins the initial task of the kernel, which is authorized to openly evaluate the scalar product in the interval between measurements of better quality. A frequent revision of the kernel task is provided as follows (Eq. (12)).

$$K(E,F)=\varphi(E)^{T}\varphi(F) \tag{12}$$

From this point of view, the most common core problems include linear kernel, polynomial kernel, Quadratic Kernel, sigmoid kernel and radial base problem. Following is the list of terms for other kernel problems.

For Linear Kernel: $linear_{k}(E,F)=e^{T}f+c$ (13)

where e,f inner products are represented in a linear kernel, and c is a constant.

For Quadratic Kernel: $quad_{k}(E,F)=1-\dfrac{\|e-f\|^{2}}{\|e-f\|^{2}+c}$ (14)

where e,f are the polynomial kernel function vectors in the input space.

For Polynomial Kernel: $poly_{k}(E,F)=\left(\lambda e^{T}f+c\right)^{e},\lambda>0$ (15)

For Sigmoid Kernel: $sig_{k}(E,F)=\tanh\left(\lambda e^{T}f+c\right),\lambda>0$ (16)

The ACOMKSVM performance is constantly focused on core diversity. In this case, where the attribute break is linearly indivisible, it should be recorded with better quality through the core of the radial basis problem in the measurement break. This ensures that the task looks linearly separable. By combining any two kernel tasks, one can also change the outstanding accuracy that cannot be achieved when using a single kernel task.

The original method predicts the original ACOMKSVM which is designed for remarkable development in the categorization system. At this point, two kernel problems such as linear and quadratic kernel problems are common to delay the excellent presentation relationships. It is easy to predict a combination of the Eqs. (21) and (22) of the standard, as recommended in the original method. In the current study, the reciprocal kernel task was successfully deployed in ACOMKSVM and the kernel task $avg_{k}(E,F)$ standard is shown below in Eqs. (17) and (18).

$$avg_{k}(E,F)=\frac{1}{2}\left(lin_{k}(,E,f)+quad_{k}(E,F)\right) \tag{17}$$

$$avg_{k}(E,F)=\frac{1}{2}\left(\left(e^{T}f+c\right)+\left(1-\frac{\|e-f\|^{2}}{\|e-f\|^{2}+c}\right)\right) \tag{18}$$

The kernel support vector machine describes the usage of two kernels namely B. linear and quadratic. This is done based on the classification principle of search links. By combining

two results, the results standard is completed and are intended for classification.

Testing phase: During training, productivity is achieved by choosing a classification depending on the phase of the experiment. Here, the productivity determines the cost of living or absence of ACOMKSVM algorithm. A comparative study was conducted since it results are of great interest and practically applicable.

3.4 Blockchain systems

In order to store the encrypted IoT information in blockchain, the authors depict an exceptional exchange structure. The exchange project mainly consists of two areas such as information and performance. The information field contains the location, coded information and the type of the IoT gadget of the information provider. In service field, the location, coded information, and IoT gadget type of the information auditor are present. The addresses, in both fields, derive the hash estimate of 32 bytes. The encoded information is obtained from ECC calculation. If the length of each instance of encoded information stored in a rectangular network is 128 bytes, then the length of the private key is 128 bytes while a part of the IoT gadget type is 4 bytes. After another exchange, the hub communicates with the information provider in blockchain organization to P2P organization, where the research centers can verify the accuracy of the exchange.

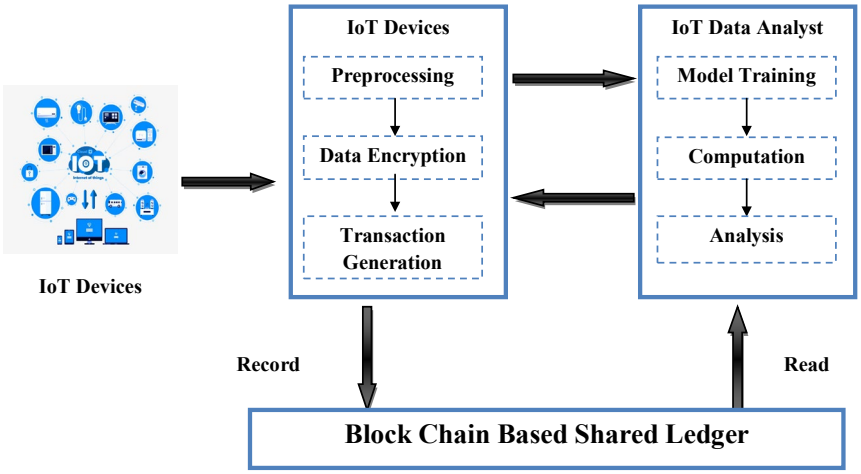

Figure 2: Proposed block chain-based privacy preserving secure data transmission system

Blockchain is an open and appropriate record, as summarized by Squares, which is originally intended to record the exchanges in cryptographic money frameworks such as Bitcoin. It takes into account the trustworthy exchange between the meetings of suspected members. Blockchain levels such as Hyper Ledger, Ethereum and EOS have been recently proposed and are currently used in a variety of application scenarios. Depending on the access controls for blockchain clients, the blockchain phases can be divided into three classes such as open blockchains, private blockchains, and consortium blockchains. The blockchain has some required functions that are suitable for trading reliable information:

- Decentralized. Like a transmitted disk, a blockchain is based on the distribution system without the need of an outsider or a trustee. The framework contains some duplicates of information recorded in the registry which prevents the misfortune of information when there is a single purpose of frustration.
- Tamper-proof. Blockchain uses constant conventions, e.g., Proof of Work (PoW) to control the option and to create new squares. In this sense, the information control is generally contradictory from a computational cost point of view. So the information recorded in the squares remains unchanged.
- Traceability. Different members can effectively control the exchange between two meetings in the blockchain framework. The information owner can track each exchange and use it continuously. For example, by accepting the rates for all information used by a stranger.

Despite the fact that blockchain has some application in different frameworks, it is not ideal for attack in information exchange since it do not provide the information security. Initially, all the exchanges are recorded in plain text squares, creating confidential data on the exchanges and opening access to all members, whom include competitors. In this way, safety and security should be carefully considered when using blockchain as an information transfer step.

3.5 Dataset description

To examine the strategy for this investigation, the current study used two authoritative data indicators such as Breast Cancer Wisconsin Data Set (BCWD) and Heart Disease Data Set (HDD). The BCWD attributes are based on the digitized image of a light needle, drawn from the breast mass. It also describes the characteristics of the cell nuclei in the image. Each example varies from gentle to harmful. The HDD consists of 13 numerical advantages and all the cases are classified according to Coronary Artery Disease. The typical effects of the mutual recognition of 10 contracts are shown here to avoid any unintended or heterogeneous results. For experimentation, 10-fold cross validation process is applied to split the dataset into training and testing part.

4 Result and discussions

In the current research work, each IoT data provider collected all the data from IoT devices in its domain and then performed the following functions (e.g., data encryption) based on IoT data. IoT providers and data analysts generally possess sufficient IT resources and the study used Intel i7 works with a 4-core processor (-7-3770 64-bit) with 7 IoT data providers at 3.40 GHz, 8 GB RAM and IoT data analysts. In Java Development Kit 1.8, Secure ECC and Secure ACOMKSVM were used. The parameter settings of the proposed model are given as follows. Number of epochs: 500, batch size: 40, alpha: 1, activation function: sigm, number of ants: 50 and pheromone evaporation rate: 0.1.

4.1 Accuracy

The two commonly used criteria for evaluating ML classifications were agreed. The accuracy of P was estimated based on the data for verification as shown in Eq. (19).

$$P = \frac{TP}{(FP + TP)} \tag{19}$$

And the recall R is calculated as Eq. (20)

$$R = \frac{TP}{(FN + TP)} \tag{20}$$

where TP and FP do not correctly match the numbers irrelevant (i.e., positive class and negative class) and FN denotes the corresponding number of incorrect classifications in the test.

Table 1: Evaluation of time measures of ACOMKSVM

Dataset	Total Time	P Time	R Time	ECC
BCWD	2933	2033	1578	275
HDD	1535	1145	1025	168

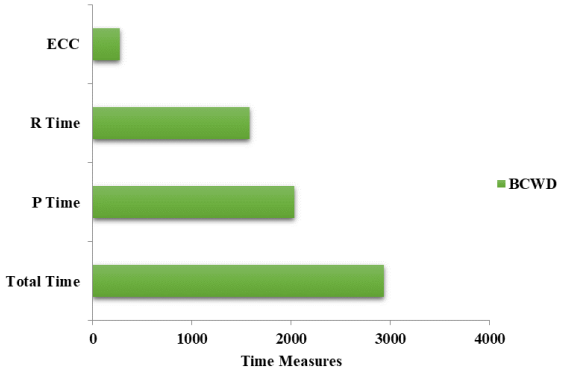

Figure 3: Graphical representation of BCWD time measures

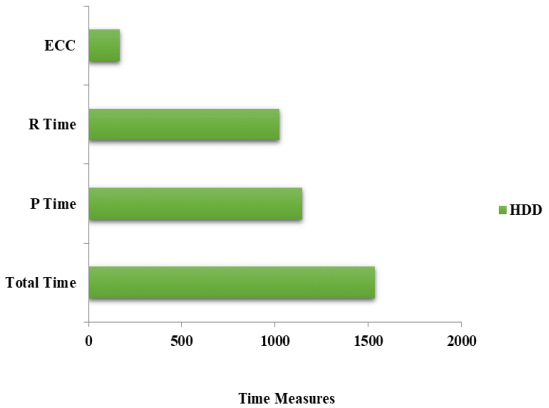

Figure 4: Graphical representation of HDD Time Measures

The performance of Tab. 1 it can be inferred that the secure ACOMKSVM can use encrypted and functional BCWD and HDD data to create SVM classifiers that consume less than an hour. In these tests, a number of p were modeled as linear. Therefore, the time P shown in Tab. 1 represents the time elapsed from more P. In the original application, the authors were able to install several parallel algorithms for public use. This scenario allowed the B to reduce time and total time. To better represent ACOMKSVM performance with regards to time, the working hours of the source are displayed in this article. Being a smooth application solution, the database with was different methods and almost all the numerical properties of the data set had all common characteristics of the data set, BCWD or HDD. The secure fuel consumption from ACOMKSVM was observed to be the best time to show South Africa.

Table 2: Proposed and existing precision measures

Input Datasets	ACOMKSVM	SVM	ACO
BCWD	92.45%	90.65%	91.56%
HDD	95.67%	92.47%	93.37%

Table 3: Proposed and existing recall measures

Input Datasets	ACOMKSVM	SVM	ACO
BCWD	92.45%	90.65%	91.56%
HDD	95.67%	92.47%	93.37%

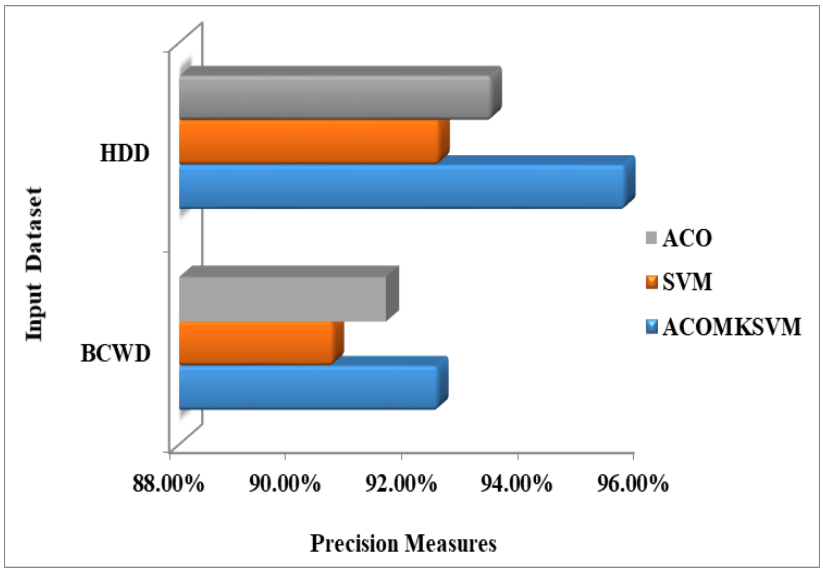

Figure 5: Graphical representation of the proposed and existing precision measures

Tab. 2 shows the precision analysis of the ACOMKSVM model over the compared methods on the applied two BCWD and HDD dataset. The table values indicated that the proposed ACOMKSVM model has reached to maximum precision values of 92.45% and 95.67% on the BCWD and HDD dataset respectively. At the same time, the existing ACO algorithm has exhibited slightly lower precision values of 91.56% and 93.37% on the BCWD and HDD dataset respectively. Simultaneously, the SVM model has demonstrated ineffective performance by attaining minimum precision values of 90.65% and 92.47% on the BCWD and HDD dataset respectively. Tab. 3 provides a detailed recall analysis of the ACOMKSVM model over the compared methods on the applied two BCWD and HDD dataset. The table values denoted that the proposed ACOMKSVM model has resulted to higher recall values of 92.45% and 95.67% on the BCWD and HDD dataset respectively. At the same time, the available ACO algorithm has demonstrated even lower recall values of 91.56% and 93.37% on the BCWD and HDD dataset respectively. In line with, the SVM model has lead to the worse outcome by obtaining least recall values of 90.65% and 92.47% on the BCWD and HDD dataset respectively.

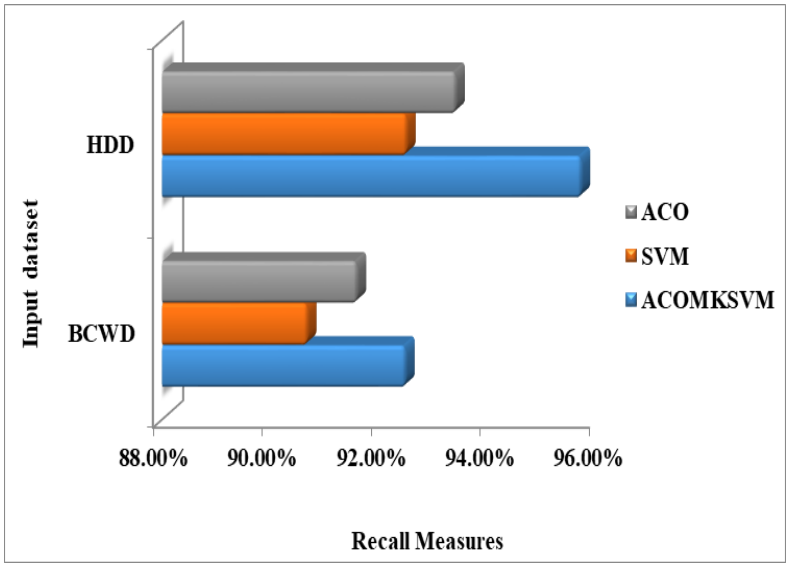

Figure 6: Graphical representation of proposed and existing recall measures

5 Conclusion

This paper has presented a new ACOMKSVM model with ECC for secure and reliable IoT data sharing. The proposed method provides protection and integrity of some data whereas it has the technology to generate secure ACOMKSVM training algorithms in partial views of IoT data, generated by different data providers. Afterwards, ECC is applied for the generation of effective and accurate privacy which protect the ACOMKSVM secure learning process. The proposed blockchain technique creates a secure and reliable data exchange platform across multiple data providers, where IoT data is encrypted and recorded in a distributed ledger. The performance validation of the

proposed model takes place using two benchmark dataset from UCI repository namely BCWD and HDD datasets. The experimental results ensured that the ACOMKSVM model has attained maximum precision and recall on all the applied dataset over the compared methods. In future, the proposed model can be extended to a framework that can be used to create a variety of ML training algorithms that protect privacy in multiple components of encrypted data sets.

Funding Statement: The author(s) received no specific funding for this study.

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

References

Alguliyev, R. M.; Aliguliyev, R. M.; Sukhostat, L. V. (2020): Efficient algorithm for big data clustering on single machine. *CAAI Transactions on Intelligence Technology*, vol. 5, no. 1, pp. 9-14.

Azbeg, K.; Ouchetto, O.; Andaloussi, S. J.; Fetjah, L.; Sekkaki, A. (2018): Blockchain and iot for security and privacy: a platform for diabetes self-management. *4th International Conference on Cloud Computing Technologies and Applications*, pp. 1-5.

Breast Cancer Wisconsin Data Set (BCWD):

https://archive.ics.uci.edu/ml/datasets/Breast+Cancer+Wisconsin+(Diagnostic).

Chen, X.; Ji, J.; Luo, C.; Liao, W.; Li, P. (2018): When machine learning meets blockchain: a decentralized, privacy-preserving and secure design. *IEEE International Conference on Big Data*, pp. 1178-1187.

Devi, G. S. P.; Pamila, J. M. J. (2019): Accident alert system application using a privacy-preserving blockchain-based incentive mechanism. *5th International Conference on Advanced Computing & Communication Systems*, pp. 390-394.

Fitwi, A.; Chen, Y.; Zhu, S. (2019): A lightweight blockchain-based privacy protection for smart surveillance at the edge. *IEEE International Conference on Blockchain (Blockchain)*, pp. 552-555.

Gai, K.; Wu, Y.; Zhu, L.; Xu, L.; Zhang, Y. (2019): Permissioned blockchain and edge computing empowered privacy-preserving smart grid networks. *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 7992-8004.

Gao, F.; Zhu, L.; Shen, M.; Sharif, K.; Wan, Z. et al. (2018): A blockchain-based privacy-preserving payment mechanism for vehicle-to-grid networks. *IEEE Network*, vol. 32, no. 6, pp. 184-192.

Gu, K.; Yang, L. H.; Yin, B. (2018): Location data record privacy protection based on differential privacy mechanism. *Information Technology and Control*, vol. 47, no. 4, pp. 639-654.

He, S. M.; Zeng, W. N.; Xie, K.; Yang, H. M.; Lai, M. Y. et al. (2017): PPNC: privacy preserving scheme for random linear network coding in smart grid. *KSII Transactions on Internet & Information Systems*, vol. 11, no. 3, pp. 1510-1532.

Heart Disease Data Set (HDD): https://archive.ics.uci.edu/ml/datasets/Heart+Disease.

Huang, J.; Qi, Y. W.; Asghar, M. R.; Meads, A.; Tu, Y. C. (2019): MedBloc: a blockchain-based secure EHR system for sharing and accessing medical data. *18th IEEE International Conference on Trust, Security and Privacy in Computing and Communications/13th IEEE International Conference on Big Data Science and Engineering*, pp. 594-601.

Javaid, U.; Aman, M. N.; Sikdar, B. (2019): DrivMan: driving trust management and data sharing in VANETS with blockchain and smart contracts. *IEEE 89th Vehicular Technology Conference*, pp. 1-5.

Jiang, Y.; Wang, C.; Wang, Y.; Gao, L. (2019): A privacy-preserving e-commerce system based on the blockchain technology. *IEEE International Workshop on Blockchain Oriented Software Engineering*, pp. 50-55.

Kim, H.; Kim, S. H.; Hwang, J. Y.; Seo, C. (2019): Efficient privacy-preserving machine learning for blockchain network. *IEEE Access*, vol. 7, pp. 136481-136495.

Li, C.; Palanisamy, B. (2018): Decentralized privacy-preserving timed execution in blockchain-based smart contract platforms. *IEEE 25th International Conference on High Performance Computing*, pp. 265-274.

Li, H.; Han, D. (2019): A blockchain-based educational records secure storage and sharing scheme. *IEEE Access*, vol. 7, pp. 179273-179289.

Li, S.; Wang, G.; Yang, J. (2019): Survey on cloud model based similarity measure of uncertain concepts. *CAAI Transactions on Intelligence Technology*, vol. 4, no. 4, pp. 223-230.

Lu, Y.; Huang, X.; Dai, Y.; Maharjan, S.; Zhang, Y. (2020): Blockchain and federated learning for privacy-preserved data sharing in industrial IoT. *IEEE Transactions on Industrial Informatics*, vol. 16, no. 6, pp. 4177-4186.

Medhane, D. V.; Sangaiah, A. K.; Hossain, M. S.; Muhammad, G.; Wang, J. (2020): Blockchain-enabled distributed security framework for next generation IoT: an edge-cloud and software defined network integrated approach. *IEEE Internet of Things Journal*. https://doi.org/10.1109/JIOT.2020.2977196.

Min, Z.; Yang, G.; Wang, J.; Kim, G. J. (2019): A privacy-preserving BGN-type parallel homomorphic encryption algorithm based on LWE. *Journal of Internet Technology*, vol. 20, no. 7, pp. 2189-2200.

Namasudra, S. (2018): Taxonomy of DNA-based security models. In: S. Namasudra and G. C. Deka (Eds.), *Advances of DNA Computing in Cryptography*, pp. 53-68. New York: Chapman and Hall/CRC.

Namasudra, S.; Devi, D.; Kadry, S.; Sundarasekar, R.; Shanthini, A. (2020): Towards DNA based data security in the cloud computing environment. *Computer Communications*, vol. 151, pp. 539-547.

Namasudra, S.; Roy, P. (2017): Time saving protocol for data accessing in cloud computing. *IET Communications*, vol. 11, no. 10, pp. 1558-1565.

Namasudra, S.; Roy, P.; Vijayakumar, P.; Audithan, S.; Balamurugan, B. (2017): Time efficient secure DNA based access control model for cloud computing environment. *Future Generation Computer Systems*, vol. 73, pp. 90-105.

Nguyen, D. C.; Pathirana, P. N.; Ding, M.; Seneviratne, A. (2019): Blockchain for secure EHRs sharing of mobile cloud based e-Health systems. *IEEE Access*, vol. 7, pp. 66792-66806.

Owiyo, E.; Wang, Y.; Asamoah, E.; Kamenyi, D.; Obiri, I. (2018): Decentralized privacy preserving reputation system. *IEEE Third International Conference on Data Science in Cyberspace*, pp. 665-672.

Rahulamathavan, Y.; Phan, R. C. W.; Rajarajan, M.; Misra, S.; Kondoz, A. (2017): Privacy-preserving blockchain based IoT ecosystem using attribute-based encryption. *IEEE International Conference on Advanced Networks and Telecommunications Systems*, pp. 1-6.

Ren, Y. J.; Liu, Y. P.; Ji, S.; Sangaiah, A. K.; Wang, J. (2018): Incentive mechanism of data storage based on blockchain for wireless sensor networks. *Mobile Information Systems*. https://doi.org/10.1155/2018/6874158.

Shen, M.; Tang, X.; Zhu, L.; Du, X.; Guizani, M. (2019): Privacy-preserving support vector machine training over blockchain-based encrypted IoT data in smart cities. *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 7702-7712.

Tahir, S.; Rajarajan, M. (2018): Privacy-preserving searchable encryption framework for permissioned blockchain networks. *IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, pp. 1628-1633.

Wang, Y.; Zhang, A.; Zhang, P.; Wang, H. (2019): Cloud-assisted EHR sharing with security and privacy preservation via consortium blockchain. *IEEE Access*, vol. 7, pp. 136704-136719.

Xia, Z. Q.; Tan, J. J.; Wang, J.; Zhu, R. L.; Xiao, H. G. et al. (2019): Research on fair trading mechanism of surplus power based on blockchain. *Journal of Universal Computer Science*, vol. 25, no. 10, pp. 1240-1260.

Xu, C.; Liu, H.; Li, P.; Wang, P. (2018): A remote attestation security model based on privacy-preserving blockchain for V2X. *IEEE Access*, vol. 6, pp. 67809-67818.

Yaji, S.; Bangera, K.; Neelima, B. (2018): Privacy preserving in blockchain based on partial homomorphic encryption system for AI applications. *IEEE 25th International Conference on High Performance Computing Workshops*, pp. 81-85.

Yasusaka, Y.; Watanabe, C.; Kitagawa, H. (2019): Privacy-preserving pre-consensus protocol for blockchains. *IEEE International Conference on Big Data and Smart Computing*, pp. 1-8.

Yin, C. Y.; Ju, X. K.; Yin, Z. C.; Wang, J. (2019a): Location recommendation privacy protection method based on location sensitivity division. *Journal on Wireless Communications and Networking*. https://doi.org/10.1186/s13638-019-1606-y.

Yin, C. Y.; Shi, L. F.; Sun, R. X; Wang, J. (2019b): Improved collaborative filtering recommendation algorithm based on differential privacy protection. *Journal of Supercomputing*. https://doi.org/10.1007/s11227-019-02751-7.

Yin, C. Y.; Zhou, B.; Yin, Z. C.; Wang, J. (2019c): Local privacy protection classification based on human-centric computing. *Human-Centric Computing and Information Sciences*. https://doi.org/10.1186/s13673-019-0195-4.

Zhang, J. Y.; Zhong, S. Q.; Wang, T.; Chao, H. C.; Wang, J. (2020): Blockchain-based systems and applications: a survey. *Journal of Internet Technology*, vol. 21, no. 1, pp. 1-14.