International Journal of Services Technology and Management

ISSN online: 1741-525X - ISSN print: 1460-6720
https://www.inderscience.com/ijstm

An improved hybrid (HHO-FFO) algorithm for healthcare and secure data transmission

Basetty Mallikarjuna

DOI: 10.1504/IJSTM.2024.10069911

Article History:

Received:	25 August 2023
Last revised:	07 May 2024
Accepted:	22 November 2024
Published online:	28 March 2025

An improved hybrid (HHO-FFO) algorithm for healthcare and secure data transmission

Basetty Mallikarjuna

Department of Information Technology,
School of Computing Science and Engineering,
Institute of Aeronautical Engineering,
Dundigal, 500043, India
Email: basettymalli@gmail.com

Abstract: Support vector machines (SVM) and optimisation algorithms like hybrid harmony search optimisation (HHO) and firefly algorithm (FFO) have revolutionised machine learning and data optimisation techniques. This article delves into the novel approach of integrating SVM with the hybrid Harries Hawks-fruit fly optimisation (HHO-FFO) algorithm to enhance healthcare services and ensure secure data transmission over blockchain networks. By exploring the synergies between SVM, HHO-FFO, and blockchain technology, this article highlights the potential for improved predictive analytics in healthcare, robust data security measures, and efficient information exchange. This model is useful to data analysts who desire to train SVM classifiers to access encryption data via communication through comparable data provided by the SVM classifier parameter values enhanced by a hybrid HHO-FFO algorithm. Extensive experiments are performed to demonstrate that the method can safely train hybrid SVM classifiers with relatively high accuracy.

Keywords: privacy protection; support vector machine; SVM; encrypted IoT data; machine learning; blockchain; homomorphic cryptosystem; hybrid Harries Hawks-fruit fly optimisation; HHO-FFO.

Reference to this paper should be made as follows: Mallikarjuna, B. (2024) 'An improved hybrid (HHO-FFO) algorithm for healthcare and secure data transmission', *Int. J. Services Technology and Management*, Vol. 29, Nos. 2/3/4, pp.274–295.

Biographical notes: Basetty Mallikarjuna is currently working as a Professor in Institute of Aeronautical Engineering. He worked as an Associate Professor in School of Computing Science and Engineering Galgotias University. He worked as an Assistant Professor in the Department of Computing Science and Engineering GITAM University Hyderabad Campus, Rudraram Village, Patancheru Mandal, Telangana and also worked as an Assistant Professor in NBKRIST Vidyanagar, Vakadu, (raffiliated that time Sri Venkatewara University, Tirupati). He completed his BTech in Computer Science Engineering from Annamacharya Institute of Technology and Sciences Rajampet (presently Annamachrya University), MTech in CSE from VIT University Vellore Tamil Nadu, and PhD at School of Computing Science and Engineering from Barathiar University Coimbatore.

1 Introduction

Combining advanced technologies like hybrid (HHO-FFO) algorithm with the secure framework of blockchain has emerged as a promising solution for enhancing data transmission and security in the healthcare sector. This article delves into the intricacies of this innovative approach, shedding light on its potential to revolutionise data protection in healthcare settings. By exploring the synergy between the hybrid algorithm and blockchain technology, we aim to provide a comprehensive overview of how this amalgamation can address the challenges of secure data transmission while ensuring the confidentiality and integrity of healthcare information (Parker, 2020). Most of the protection problems happened within the network during money transactions, patient's information saving in hospitals, etc. To cut back the protection issues happened want some powerful security methods within the world (Zheng et al., 2017; Mallikarjuna et al., 2020b, 2020c). One of the powerful technologies for these issues is blockchain technology. In 2008, Sathoshi Nakamotto introduced the bitcoin cryptocurrency method for the transaction then, it developed by using blockchain technology (Tse et al., 2017). Imagine a dynamic duo of algorithms coming together like Batman and Robin but for data security in healthcare. The hybrid (HHO-FFO) algorithm combines the power of two optimisation algorithms, harmony search (HS) and firefly algorithm (FA), to enhance data security and transmission efficiency over blockchain networks (Biswas and Muthukkumarasamy, 2016). Kamanashis Biswas introduced blockchain methodology through intelligent devices for securing communication in a smart city (Bhulania and Raj, 2018; Shen et al., 2020; Baliyan et al., 2020). Think of optimisation algorithms as digital detectives solving complex puzzles to improve system performance and efficiency. The hybrid (HHO-FFO) algorithm combines the strengths of HS and FA to fine-tune data transmission processes, enhance encryption techniques, and bolster cybersecurity defences in healthcare settings.

Ittay Eyal developed cryptocurrency blockchain protocols in FinTech to urge secure bank-to-bank and interbank transactions. In FinTech method new possibilities are developed to secure the transactions and supply affection cooperation in FinTech industry and engineering community (Mettler, 2016). The principles of blockchain are often explained by using Bitcoin transactions. And it had been not only employed in the banking systems, it had been developed for the whole economy to solve the issues. By integrating HS and FA, the hybrid (HHO-FFO) algorithm creates a powerful synergy that enhances data security, confidentiality, and integrity in healthcare data transmission over blockchain networks. This innovative approach promises to mitigate risks, strengthen defences, and elevate the standards of data protection in the ever-evolving healthcare landscape

Nowadays, the globe needs the most innovative technology within the digitised world. The blockchain technology, all transactions and details are recorded, and everybody can connect, send and verify the main points because it is an open ledger (Eyal, 2017). Blockchain technology is e strong robust method to cut back the price and provides modifications within the economic field. Ali Dori developed blockchain technology to maximise the safety in vehicular ecosystems (Ahram et al., 2017). This chain raises new modules are constantly connected (Nguyen, 2016). Asymmetric cryptography and distributed consensus algorithms are used for e-healthcare consumer security and general ledger stability (Salomaa, 2013; Mallikarjuna et al., 2020b, 2020c).

Blockchain technology usually consists of main features of decentralisation, persistence, anonymity, and audibility. With these features, blockchain may deeply save the price and develop effectiveness (Dorri et al., 2017). The large number of anxious IoT devices makes them easily accessible targets for attackers to build large-scale botnets (Mallikarjuna, 2020b; Rodríguez-Esparza et al., 2020; Mallikarjuna et al., 2020b, 2020c).

Nowadays the globe needs the most innovative technology within the digitised world. The blockchain technology all transactions and details are recorded and everybody can connect, send and verify the main points because it's an open ledger (Eyal, 2017). Blockchain technology is a strong method to cut back the price and provides modifications within the field of economics. Ali Dori developed blockchain technology to maximise safety in vehicular ecosystems (Ahram et al., 2017). This chain raises new modules that are constantly connected (Nguyen, 2016) Asymmetric cryptography and distributed consensus algorithms are used for e-healthcare consumer security and general ledger stability (Salomaa, 2013; Mallikarjuna et al., 2020b, 2020c).

Blockchain technology usually consists of the main features of decentralisation, persistence, anonymity, and audibility. With these features, blockchain may deeply save the price and develop effectiveness (Dorri et al., 2017). The big number of anxious IoT devices creates them easily accessible targets for attackers to build large-scale botnets (Mallikarjuna, 2020b; Rodríguez-Esparza et al., 2020; Mallikarjuna et al., 2020b, 2020c).

- To recommend a hybridised secure SVM training system over blockchain-based encrypted IoT data (Shen et al., 2019; Ioffe, 2017; Mallikarjuna, 2019a, 2019b).
- To use blockchain system for building safe and integrity data transmission in healthcare (Mallikarjuna and Reddy, 2019), reliable data transmission between end users, in which IoT data is encrypted and posted to the distribution ledger.
- For designing safe building blocks, like safe polynomial multiplication and safe comparison, using homomorphic cryptosystem, Paillier, build a safe SVM training algorithm (Mallikarjuna et al., 2020a), requiring two interactions on one repetition, without the required of third trustworthy.
- Every vendor's data is initially encrypted with Paillier and then posted to a distribution ledger (Sun et al., 2020; Zhang and Zhao, 2018).
- The selection of SVM classifier optimal values of kernal parameters (Wang et al., 2020).
- Let the SVM classifier parameter values be optimised through a hybrid Harries Hawks and fruit fly optimisation algorithm (HHO-FFO) (Kassab et al., 2019).
- Extensive experiments are performed to demonstrate that the method can safely train hybrid SVM classifiers with relatively high accuracy (Le Nguyen et al., 2020).

2 Background

In the digital age, where data breaches and cyber threats lurk around every virtual corner, safeguarding sensitive healthcare information is paramount. Patient privacy, confidentiality, and the integrity of medical records must be protected at all costs. The hybrid (HHO-FFO) algorithm serves as a shield, fortifying the walls of healthcare data

systems against potential intruders and unauthorised access. The specter of data breaches and privacy violations haunts the healthcare sector, raising concerns about the safety and confidentiality of patient information. Safeguarding sensitive data from cyber threats, unauthorised access, and breaches is a pressing challenge that requires robust security measures and innovative solutions like the hybrid (HHO-FFO) algorithm.

Azaria et al. (2016) have introduced a way called MedRec for network security in the medical field. During this paper, medical stalk holders were participated in blockchain miners. This method was easy to access medical information's and gave an immutable log. Using this method can receive data from different forms of endpoints. However, it needed further development (Pinno et al., 2017).

Hou (2017) introduced e-government-based Bitcoin technology. During this paper, it had been discussed how blockchain contributes to the event of e-government. Quality and quantity were improved in government services and had information transparency and accessibility. Also, had an event in the information sharing across the different organisations, but the drawbacks of this method were difficulties found during this method and had lack of mature application presented in it. And also, the major problem was cost and reliability (Li, 2018).

Ølnes and Jansen (2017) have introduced blockchain technology to enable the smarter government, highlighting recent technology's innovative potential. During this paper, the more intelligent technology had more information capabilities and contained promising benefits in it.

But the disadvantage of this method was more questions were raised related this technology. Also, important factors for locating adaption were not found (Li et al., 2019).

Xia et al. (2017) introduced medshare technology using access control protocol and encryption methods in blockchain security to handle patient' information' in hospitals. During this paper, the distributed ledger MedBlock allowed efficient electro-medical records (EMR). The most advantage of this method was better information security and a better level efficiency (Salian et al., 2019).

Bhulania and Raj (2018) introduced the strategy called heterogeneity cloud computing, which gave the outline of frame work and protocols for handling healthcare data. I contained enhanced existing applications and maintenance cost is low. The main drawback was managing enterprise data ware house issue (Ajayi et al., 2019).

Kaur et al. (2018) have introduced the blockchain and cryptographic hash technology for solving the problems like value, reliability and trust. During this technology, the user had satisfaction with the use of cryptocurrency. But the disadvantage of this method was a continuation of this technology needed further more research within the area of cost reduction (Casino et al., 2019).

Chen et al. (2019) have designed a storage method for managing the blockchain of personal medical data and cloud storage. In addition, a service framework to share a medical record was explained. Moreover, the medical blockchain characteristics were presented and investigated by a full evaluation with outdated systems.

The proposed methodology storage and sharing system are not dependent on third parties, and no party has absolute authority to influence processing governments by utilising secure, distributed, open and cheap database technology presented on this promising technology (Kumar et al., 2018).

Guo et al. (2018) have presented a signature system in terms of attributes with multiple authorities, during the patient endorses a message consistent with the attribute

without revealing any information other than the evidence that has been shown to it. Besides, it consists of numerous establishments devoid of single or central trust to create and assign the patient's public/private keys that prevent custody trouble and adjust to the data storage mode disseminated within blockchain. To share the seeds of critical pseudo-random function between authorities, this protocol opposes collusion attack from N of N – 1 corrupt authority. At belief of computational bilinear Diffie-Hellman, strictly shown that, based on impossibility of falsification and the ideal privacy of attribute signer, this signature arrangement based on attribute is safe within the arbitrary oracle model (Dhawale and Kamboj, 2020).

3 Preliminaries

3.1 Notations

From streamlining patient data exchange to enhancing drug traceability and clinical research, blockchain technology is a game-changer in the healthcare industry. By leveraging blockchain's distributed ledger system, healthcare providers can improve interoperability, enhance data security, and foster trust among stakeholders in the ecosystem. Dataset S is a set of m records not sorted through size |S|, which is i^{th} record on S, implies a label corresponding toward x_i. Classify Y and Y_i as two applicable parameters of the HHO-FFO algorithm. λ implies learning rate on this utilise partial homomorphic cryptosystem known as Paillier as a array type of notation cryptosystem, and let [[n]] implies the encryption of n in Paillier.

Table 1 Notations

Title	*Notation*
Dataset	S
Dataset size	|S|
i^{th} record of S	x_i
Classification HHO-FFO	Y, Y_i
Learning rate	λ
Paillier array	let [[n]]

3.2 Block chain system

In Mallikarjuna et al. (2020b, 2020c), blockchain is an exposed and dispersed ledger that takes the form of block lists that is initially intended to record transactions on cryptocurrency systems, for example, Bitcoin. It allows reliable transactions between a group of entrusted participants. Recently, numerous alternative blockchain platforms, like Hyper Ledger, Ethereum, and EOS, have been suggested and used to a diversity of application scenarios. Based on the restriction for blockchain users, blockchain platforms are roughly classified in three groups, namely public blockchains, private blockchains, and consortium blockchains. Blockchain contains numerous advantageous characteristics that makes it inherently appropriate for reliably sharing data.

3.2.1 Decentralised

Like the distributed ledger, the blockchain is constructed into the peer-to-peer network without necessitating for third party or central administrator (Mallikarjuna et al., 2020b, 2020c). The system contains multiple copies of the ledger information (Mallikarjuna et al., 2020b, 2020c), which prevents data loss in the event of a unique failure.

3.2.2 Tamper-proof

Blockchain utilises consensus algorithms, like proof-of-work (PoW), for managing the correct creation of innovative blocks. Therefore, data manipulation is sometimes not practical based on calculation overhead, which makes it impossible to change the data recorded in volumes.

3.2.3 Traceability

Transactions among parties on blockchain system can be simply confirmed by the rest of the participants. Often, any transaction is tracked, and in addition, the data owner may gain at real time, for example, all bit of information that is employed through third party.

Although blockchain consists of numerous benefits over other systems, it is not ideal, while it serves as a platform for sharing knowledge thanks to their liability of information privacy toward possible attacks. Initially, entire transactions are posted on blocks at plain text type, exposing the sensitive information on transactions to some of the participants with adversaries (Gao et al., 2018). Thus, security and privacy anxiety must be dealt with carefully while using blockchain as a platform for sharing information.

3.3 Problem formulation

This section explains the topic of secure hybrid SVM (Mallikarjuna et al., 2020a) training on encryption data collected as numerous parties with modelling of the system, threat model and style objectives.

3.3.1 Modelling of system

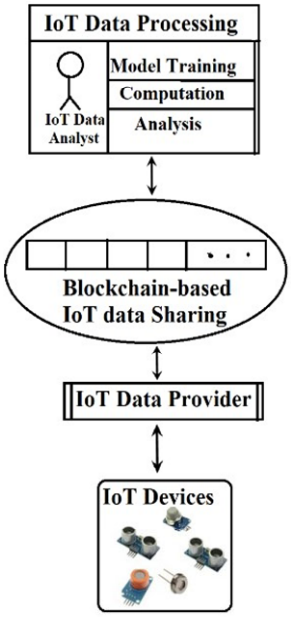
Visualise a data-driven IoT ecosystem, demonstrated at Figure 1 (Mallikarjuna et al., 2020b, 2020c).

- IoT devices can detect and transmit ZigBee, 3G/4G, and Wi-Fi (Mallikarjuna, 2020a, 2020b).
- IoT data providers gather fundamental knowledge of IoT devices in their own domains. Since the expensive benefit of knowledge providers, IoT data generally includes responsive information. Therefore, every data provider encrypts their IoT data to some extent with homomorphic encryption and records the information on the blockchain.
- IoT platform based on blockchain is a dispersed database, in which the encrypt IoT data collected as entire data providers is stored on shared ledger. With a built-on consensus mechanism, IoT will guarantee that the data is shared securely and in a conversion-based manner.

- The goal of the IoT data analyst is to process the IoT data evidence within blockchain-based site (Mallikarjuna, 2020a, 2020b), taking complete benefit of rising analytics systems.

Data analysts must contact appropriate providers to get SVM classifier training parameters. Threat model based on the system model labelled in Figure 1, every entity has numerous threats and interactions. The efforts are devoted to designing a privacy preservation system to train completed SVM models across various IoT providers, initially assuming the pressures for data privacy through interaction among data providers and analysts. Regarding this, the information analyst to be an honest but enthusiastic adversary; the information analyst should honestly go after the pre-designed ML training protocols, other than it will be interesting.

Figure 1 System model of the IoT ecosystem (see online version for colours)



Source: Shen et al. (2019)

Assume the subsequent two threat models have dissimilar attack competencies, which is usually based on sensitive data that the data analyst may obtain (Shen et al., 2018).

4 Proposed methodology

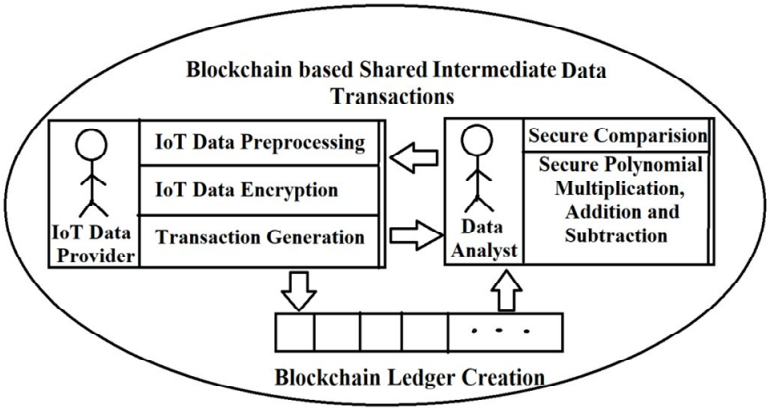
4.1 The construction of hybridised secure SVM

This section suggests the structure facts of the proposed privacy-protecting hybrid secure SVM training system for encrypted IoT data based on blockchain.

4.2 System overview

Consider the data analyst aims to train SVM models using information gathered as many IoT data providers (Shyry, 2014). The hybrid Secure SVM system overview is demonstrated at Figure 2 (Shen et al., 2018).

Figure 2 System overview



Source: Shen et al. (2018)

The existing key management mechanism will be used to manage the information providers' encryption capability. The data analyst wants to train an SVM model that may evaluate encrypted data on a global ledger and accumulate a secure training algorithm through numerous essential components like safe comparison and safe addition of polynomials (Shen et al., 2019, 2020).

4.3 Encrypted data sharing via block chain

Nowadays, explain the information exchange process. To facilitate the model's exercise, data events for a similar training task are pre-processed locally and represented by identical feature vectors, without loss of generalisation. For storing the encrypted IoT data within blockchain, describe a particular transaction configuration. There are two fields in transaction format: input and output (Mallikarjuna et al., 2019a, 2019b). The input field contains the information provider's address encrypt data, and the IoT device (Mallikarjun et al., 2020d). The equivalent output field has the address of information analyser, encrypt data, and IoT device types.

The length of every instance of encrypted data stored within blockchain as 128 bytes, supporting the belief that the length of the private key as 128 bytes (Mallikarjuna, 2020a, 2020b). The IoT device type (Mallikajruna, 2020a, 2020b) section is four bytes long. Similar to the PoW mechanism, based on the existing consensus algorithms, a particular mining terminal transaction is sealed as the most innovative module and qualified to be added to the current chain.

4.4 Building blocks

As explained in the result section, this will always ensure the privacy of numerous IoT providers, and the goal is to design a privacy preservation system to train SVM models on various private datasets offered through various IoT providers (Mallikarjuna, 2020a, 2020b). The fundamental building blocks to achieve such goals (Mallikarjuna et al., 2019a, 2019b).

Several optimisation methods are able to resolve the SVM model parameters on the equation (1) SVM classifier are optimised by a hybrid Harries Hawks and fruit fly optimisation algorithm. HHO is an optimisation strategy for the SVM dual plan (Dua and Graff, 2019; Mallikarjuna et al., 2020a) and works well for linear SVM and sparse data.

Applying HHO in encryption can incur terrible computing and communication costs (Mallikarjuna et al., 2019a, 2019b). FFO compatible with SVM optimisation (Mallikarjuna et al., 2020a) is easy and competent, engaging a very low amount of vector comparison and multiplication. Select HHO-FFO optimisation algorithm for improving the SVM sample parameters on the equation (1). HHO-FFO turns the primary SVM into a complex factor that minimises the loss of experience through the penalty factor, as shown in equation (2)

$$\min_{w,b} \frac{1}{2}\|w\|^2 + C\sum_{i=1}^{n} L\left(w, b, \left(u_i, v_i\right)\right) \tag{1}$$

Here, the correct part of the hinge loss function is,

$$C\sum_{i=1}^{n} L\left(w, b, \left(u_i, v_i\right)\right) = C\sum_{i=1}^{n} \max\left\{0, 1 - y_i\left(wu_i - b\right)\right\} \tag{2}$$

where C implies main classification penalty, which generally takes the value $\frac{1}{n}$ the fundamental form is

$$u_{m+1} = u_m - \lambda\nabla\left(u_m\right) \tag{3}$$

$$\nabla_t = \lambda w_t - \sum_{i=1}^{n} I\left|\left(wu_i + b\right) < 1\right| \times u_i v_i \tag{4}$$

4.5 Safe polynomial multiplication

For training the SVM model safely, explain the safe polynomial multiplication employed at the HHO-FFO algorithm. By Paillier's homomorphic property, it may simply acquire safe addition and subtraction. An additively homomorphic properties on Paillier may be explained as $[[n_1 + n_2]] = [[n_1]] \times [[n_2]] \pmod{N^2}$ and subtraction homomorphic properties may be explained as Shen et al. (2019) is the modular multiplication inverse, which performs that $[[n]] \times [[n]]^{-1} \bmod N^2 = 1$ (Shen et al., 2020) on Paillier.

$[[n]]^{-1}$ may be calculated using function $[[n]] \times [[n]]^{-1} \bmod N^2 = 1$. Thus, the secure polynomial multiplication maybe obtained during cypher text manipulation (Shen et al., 2019),

$$[[an_1 + bn_2]] = [[n_1{}^a]] \times [[n_2{}^b]] (\text{mod } N^2) \tag{5}$$

The security of the safe polynomial multiplication constructed through Paillier based on statistically indistinguishable Paillier (Shen et al., 2020).

4.6 Safe comparison

Safe comparison at hybrid SVM is well described as associating an encryption (unsigned) number [[n]] by stable 1. For parts A and B that contribute to the safe evaluation algorithm, neither party it may get information other than the information inferred through input. The safe comparison protocol is exhibited at given algorithm.

$$| s_3 - s_2 | < s \leftrightarrow \frac{| s_3 - s_2 |}{s_1} < 1 \tag{6}$$

$$(as_1 + s_2) = (s_1 + s_3) \leftrightarrow (a - 1) = \frac{s_3 - s_2}{s_1} \tag{7}$$

If $(as_1 + s_2) > (s_1 + s_3)$ because a is an integer, it can infer that $(a - 1) > 1 \rightarrow a > 1$, otherwise $a \leq 1$ algorithm for secure encryption:

- Input A: [[a]], 1 (Shen et al., 2019).
- Input B: A pair of keys (PK, SK) (Shen et al., 2019).
- Output B: (a < 1) (Shen et al., 2019, 2020).

Three positive integers s_1, s_2 and s_3 where $|s_3 - s_2| < s_1$.

a Send $[[as_1 + s_2]]$ and $[[s_1 + s_3]]$ to B.

b Decrypts and compare $(as_1 + s_2)$ with $(s_1 + s_3)$ and tell the result to A $a > 1$, if and only if $(as_1 + s_2) > (s_1 + s_3)$ otherwise $a \leq 1$ return $a \leq 1$.

5 HHO-FFO algorithm

The Harris Hawks and fruit fly optimisation is stimulated through cooperative behaviours, and the chasing style is known as a surprise attack. In this approach, it jumps cooperatively in different directions in an attempt to surprise it. Harris's hawks and fruit fly may expose a diversity of chasing patterns depending on the dynamic nature of scenarios and run-away patterns. This operation mathematically imitates these dynamic patterns in Harris's hawks and fruit fly behaviours for developing an optimisation algorithm that has been presented as a competitive alternative for complex problems. HHO-FFO as a stochastic met heuristic is able to tackle many complex optimisation problems. The HHO-FFO model can be expressed between exploratory and exploitative phases.

They perch randomly in different data with two preferred operator depending on probability p. This process is modeled in equation (12), where $p < 0.5$ means that the perch using the population r.

Meanwhile, if $p \geq 0.5$, the perch on the random trees around the population range. To facilitate understanding of the HHO-FFO algorithm, Table 1 presents a list of symbols used in this algorithm.

$$Y(u+1) = \begin{cases} Y_{rand}(u) - v_1 \mid Y_{rand}(u) - 2v_2 Y(u) \mid & \begin{cases} p \geq 0.5 \\ p < 0.5 \end{cases} \\ \left(Y_r(u) - Y_n(u) - v_3\left(LB + v_4(UB - LB)\right)\right. & \end{cases} \tag{8}$$

where Y_n the average data of the variable is obtained using

$$Y_n(u) = \frac{1}{M}\sum_{i=1}^{M} Y_i(u) \tag{9}$$

Here, $Y_i(u)$ represents the position for each variable in the iteration u and M is the total number for the variables. The average data can be obtained using different ways, but this is the simplest way.

Table 2 List of symbols

Description	*Symbol*
Position vector of search agent	Y, Yi
Position of r	Y_r
Position of random variable	Y_{rand}
Average position of the variable	Y_n
Swarm size, repetition counter, maximal number of repetitions	M, u, U
Random number inside (0, 1)	v_1, v_2, v_3, v_4, v_5, p
Upper bound and lower bound (Shen et al., 2019, 2020)	D, LB, UB
Energy	I, I_0

The energy drops significantly as the behaviour escapes. For modelling this concept, the energy of prey is modelled from:

$$I = 2I_0\left(1 - \frac{u}{U}\right) \tag{10}$$

When $v \geq 0.5$ and $|I| \geq 0.5$, that has sufficient energy. It can try to run away via arbitrary misleading shifts but unfortunately it cannot do it. The following rules stimulate this process.

The value of J changes arbitrarily with every repetition for simulating the behaviour. In hard besiege, if $v \geq 0.5$ and $|I|$

$$Y(u+1) = Y_r(u) - I \mid \Delta Y(u) \mid \tag{11}$$

$$X = Y_r(u) - I \mid JY_r(u) - y(u) \mid \tag{12}$$

The process described in equation (18) is called soft siege through progressive rapid dives occurs if $|I| \geq 0.5$ and $v < 0.5$.

$$S = X + Z \times LF(D) \tag{13}$$

where Z implies the flight function that can be computed by:

$$\mathrm{LF}(y) = 0.01 \times \frac{t \times \sigma}{|r|^{\frac{1}{\beta}}}, \sigma = \left(\frac{\chi(1+\beta) \times \sin\left(\frac{\pi\beta}{2}\right)}{\chi\left(\frac{1+\beta}{2}\right) \times \beta \times 2\left(\frac{\beta-1}{2}\right)} \right)^{\frac{1}{\beta}} \tag{14}$$

where t and r imply random values between (0, 1) and β represents the evade stable set toward 1.5. A last step of this process is updating the positions using:

$$Y(u+1) = \begin{cases} X & \mathrm{LF}(X) < \mathrm{LF}(Y(u)) \\ S & \mathrm{LF}(Z) < \mathrm{LF}(Y(u)) \end{cases} \tag{15}$$

The HHO-FFO also considers the hard siege through the progressive rapid dives that is presented if $|I| < 0.5$.

$$X = Y_r(u) - I\,|JY_r(u) - Y_n(u)| \tag{16}$$

The HHOFFO algorithm is hybridised with SVM for classification and feature optimisation. SVM parameters in the selected features set for all cross-validation folds.

5.1 Algorithm

Input: The population size N, maximal number of iteration U, dataset D, group classifier G, feature Y and the fitness function HHO-FFO

Outputs: The accuracy value or each iteration and the best accuracy value (Shen et al., 2019, 2020)

Initialise population

For condition not satisfied

Compute the new fitness value

Set Y_r as a data of r **for** ((Y_r))

do

Upgrade the first energy I_0 and strength J

Upgrade I using equation (14) **if**($|I| \geq 1$) **then**

Upgrade data with equation (12)

end if

if ($|I| < 1$) **then**

if ($v \geq 0.5$, $|I| \geq 0.5$) **the**

Upgrade data with equation (15)

else if ($v \geq 0.5$, $|I| < 0.5$) **then**

Upgrade data with equation (17) **else**

if ($v < 0.5$, $|I| \geq 0.5$) then

Upgrade data with equation (23)

Call the feature selection method

Call the SVM classifier

else if ($v < 0.5$, $|I| < 0.5$) then

Update the data using equation (23)
  Call the feature selection method
Call the SVM classifier **return** bet accuracy

5.2 Blockchain-based transactions

In this section the cipher text model, therefore, the recognised background model. A protocol that fulfilled two-part secure computing is safe against honest but interested opponents, and the modular sequencing system gives how to create secret protocols extremely modularly. To suggest the safety test based on two definitions (Shen et al., 2019, 2020). For further details, pass on the reader to safe two-part calculation and a consecutive segmental arrangement.

Let K = (KP, KQ) be the polynomial function and π implies protocol calculation K; p is P's input and q is Q's input and P and Q prefer for computing K(p, q) using π; the view of P is the tuple

$$\text{view}_P^{\pi}(\lambda, p, q) = (\lambda; p; n_1, n_2, ..., n_m) \tag{17}$$

where n_1, n_2, …, n_m does P. establish the message describe the view of Q similarity P's and Q's outputs are $\text{output}_P^{\pi}(p, q)$ and $\text{output}_Q^{\pi}(p, q)$ correspondingly. The universal output of π is,

$$\text{output}^{\pi}(a, b) = \left(\text{output}_P^{\pi}(p, q), \text{output}_Q^{\pi}(p, q)\right) \tag{18}$$

5.3 Secure two-party computations

A protocol π privately calculates k through statistic security, if entire probable inputs (p, q) and simulators RP and RQ maintains the following (Shen et al., 2019, 2020),

$$\left\{R_A, k_2(p, q)\right\} \approx \left\{\text{view}_P^{\pi}(p, q), \text{output}^{\pi}(p, q)\right\} \tag{19}$$

$$\left\{k_1(p, q), R_Q\right\} \approx \left\{\text{output}^{\pi}(p, q), \text{view}_Q^{\pi}(p, q)\right\} \tag{20}$$

The fundamental design of a continuous modular system is: m participants execute a protocol πcall toward ideal functionary K, P and Q compute K privately sending its inputs in the direction of a trusted third party and getting the outcome, if it may show as protocol π fulfilled two-part calculation and one protocol ρ may accomplish the similar function as K privately, then it may restore the ideal protocol of K through the protocol of ρ at π, the innovative protocol π^{ρ} is safe in the honest but curious model.

5.4 Modular sequential composition

Let K_1, K_2, …, K_m be the probabilistic polynomial functionality of time and ρ_1, ρ_2, …, ρ_m protocols that compute respectively K_1, K_2, …, K_m at semi-honest adversary existence. Let D be the two-party probability polynomial function of time, π protocol that safely calculates D at K_1, K_2, …, K_m – hybrid model at semi-honest adversaries presence. Subsequently $\pi^{\rho_1, \rho_2, ..., \rho_m}$ safely calculates D at the presence of half-honest enemies.

5.5 Security proof for secure computation

The function is K:

$$K\left(\left[\left[a\right]\right]_Q, 1, PK_Q, SK_Q\right) = \left(\phi, (a < 1)\right) \tag{21}$$

The view of P is $view_P^{\pi} = (\left[\left[a\right]\right]_Q)$.

As P does not receive any messages from Q, the view only has input and three random numbers are produced. Therefore the simulator

$$R_P^{\pi}\left((a, 1); K(a, 1)\right) = view_P^{\pi}\left(\left[\left[a\right]\right]_Q, 1, PK_Q\right) \tag{22}$$

$[[a]]_Q$ is encrypted with PK_Q and $[[a]]_Q$ confidentiality is equal towards the Paillier cryptosystem utilised. Thus P may not conclude the value openly. The view of Q is,

$$view_Q^{\pi} = \left((as_1 + s_2), (s_1 + s_3), PK_Q, SK_Q\right) \tag{23}$$

S_Q^{π} execute as below:

- Creates l random coins and get $[[(n_1, n_2, \ldots, n_l)]]_Q$ by PK_Q, here l implies length of a.
- Q equally selects three positive integers c_1, c_2, and c_3 where $|s_3 - s_2| < s_1$.
- Outputs $((nc_1 + c_2), (c_1 + s_3), PK_Q, SK_Q)$.
- The distribution of (a, s_1, s_2, s_3) and (n, c_1, c_2, c_3) are identical, so the real distribution.
- $((as_1 + s_2), (s_1 + s_3), PK_Q, SK_Q)$ are the ideal distribution $(nc_1 + c_2), (c_1 + c_3), PK_Q$, SK_Q are statistically indistinguishable.

6 Result and discussion

6.1 Performance evaluation

In this section, we assess the hybrid secure SVM analysis in terms of accuracy and competence during the wide testing of real-world datasets. Initially, explain the setup of the experiment and then display the experimental outcomes to demonstrate their effectiveness and efficiency.

6.2 Experimental setup

For designing, every IoT data provider gathers entire knowledge fragments as IoT devices on their own domain to accomplish the downstream operations (for example, data encrypt) in IoT data. As IoT suppliers, and data analysers, generally have adequate calculating resources, tests are executed in systems manufactured at 3.40 GHz and eight through an Intel i7 (i7-3770 64bit) 4-core processor (Shen et al., 2019, 2020).

6.3 Dataset

To execute the strategy of this research, utilise two real-world datasets that are (Shen et al., 2019, 2020) Breast Cancer Wisconsin Dataset (BCWD) (Dua and Graff, 2019) and Heart Disease Dataset (HDD) (Detrano et al., 1989) that is openly obtainable on UCI machine learning fountain. BCWD landscapes are calculated as a digital image of the optimal injection accent of the breast mass and explain the properties of the cell nuclei present in image. Every occurrence is labelled benign or malignant (Shen et al., 2019, 2020). HDD has 14 numerical attributes, and every instance is categorised via the heart disease types. Statistics are demonstrated at Table 2. To display the typical outcomes of cross-validating 10 runs to evade adequate or contingent outcomes.

Table 3 Statistics of datasets

Dataset	*Instances number*	*Attribute number*	*Discrete attribute*	*Numerical attribute*
BCWD	698	8	0	8
HDD	295	14	14	0

6.4 Float format conversion

HHO-FFO standard algorithm executes on floating point number. Though, cryptosystem operations are accepted in integers. For the encrypted data to take actual values, it is essential to execute a format change in integer illustration earlier (Shen et al., 2019, 2020). Binary floating point number D is articulated from $D = (-1)^s \times H \times 2^C$ on international standard IEEE754, here, s implies sign bit, H implies significant number, and C implies exponent bit.

6.5 Key length setting

In public key cryptosystems, the key length is directly connected with cryptosystem safety, and a small key can be critical for insecure encryption. Particularly, homomorphic operations (that is, safe polynomial multiplication) are executed on cipher text; an extended key decreases the homomorphic functional efficiency and the lower one key enabling plain text space. Consequently, it should assume the length of the key to evading the possibility of overflow. At hybrid secure SVM, Paillier M key is fixed with 1,024 bits.

To provide a dataset for verifying the accuracy A is computed $A = l_p/(g_f + l_p)$, and the specificity (Shen et al., 2019, 2020) P is computed as $P = l_p/(g_p + l_p)$ and sensitivity S is computed $S = l_p/(g_n + l_p)$ here l_p implying numbers of relevant that is adequately categorised g_p implies a number of irrelevant, which properly categorised and g_n implies numbers of applications, which is wrongly categorised under test outcomes.

Figure 3 shows that the accuracy of the different datasets in the proposed hybridised secure SVM provides high accuracy compared with secure SVM classifier. The proposed hybridised secure SVM method provides 97.37% in the BCWD dataset and secure SVM method produce 95.68% in BCWD dataset, and SVM method produce 96.58% in BCWD dataset. The proposed hybridised secure SVM method provides 96.13% in HDD dataset, the secure SVM method produces 94.36% in the HDD dataset, and the SVM method

produces 93.21% in HDD dataset. Our proposed hybridised secure SVM method produces high accuracy compared with secure and SVM methods.

Figure 3 Performance evaluation of accuracy (see online version for colours)

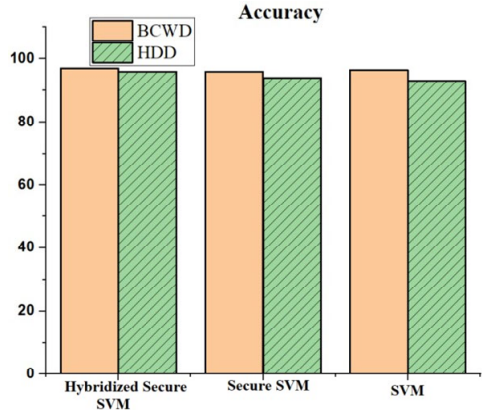


Figure 4 displays that the specificity of the different datasets in the proposed hybridised secure SVM provides high specificity compared with the secure SVM classifier. This proposed hybridised secure SVM method provides 92.68% in BCWD dataset and the SVM method produce 85.69% in BCWD dataset and SVM method produce 87.13% in the BCWD dataset. Proposed hybridised secure SVM method provides 90.98% in HDD dataset and secure SVM method produces 88.95% in HDD dataset and SVM method produces 86.78% in HDD dataset. Our proposed hybridised secure SVM method produces high specificity compared with secure and SVM methods.

Figure 4 Performance evaluation of specificity (see online version for colours)

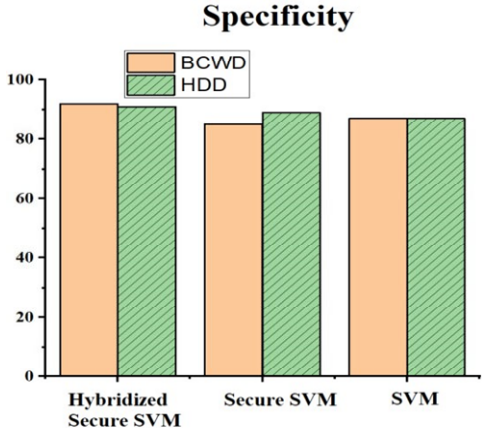
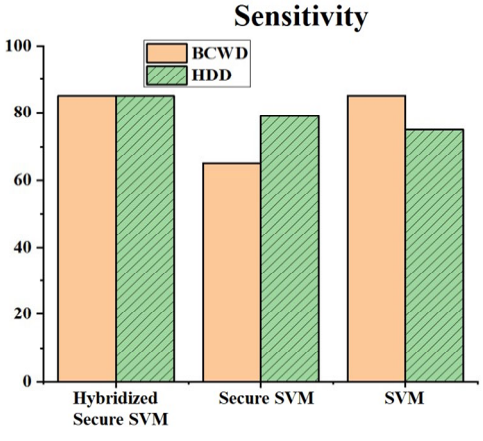


Figure 5 portrays that the sensitivity of the different datasets in the proposed hybridised secure SVM provides high sensitivity compared with the secure SVM classifier. Our proposed hybridised secure SVM method provides 86.91% in BCWD dataset and the secure SVM method produce 70.89% in BCWD dataset and SVM method produce 86.83% in BCWD dataset. The proposed hybridised secure SVM method provides

90.56% in the HDD dataset and secure SVM method produce 81.52% in HDD dataset, and SVM method produces 76.43% in HDD dataset. Our proposed hybridised secure SVM method produces high sensitivity compared with secure SVM method and SVM method.

Figure 5 Performance evaluation of sensitivity (see online version for colours)



To illustrate that protecting the privacy of every IoT data provider and safely training taxonomies does not reduce the accuracy of hybridised secure SVM, focus on the way to safely train a classifier during this manuscript, does not regulate the parameters and default parameters, recapitulates the outcomes for accuracy, specificity and sensitivity. Compared to hybrid secure SVM, secure SVM and SVM have about the identical accuracy from SVM that does not decrease the classifier accuracy. BCWD may be a dataset by entire numeric attributes, and HDD may be a dataset with entire discrete attributes.

6.6 Efficiency

Figure 6 displays the execution time of safe comparison and polynomial multiplication through encrypted datasets; it also shows the time consumption of IoT P data providers and C data analysis overall time consumption. The performance ends at Figures 4 and 5; hybrid secure SVM trains SVM classifiers by spending one hour with the encrypted BCWD and HDD dataset, which consist of suitable time consumption. In these experiments, various P's are replicated linearly. Therefore, the time P shown in Figures 5 and 6 that the accumulation of time spent through P. In actual application, it should establish that various P running algorithms at parallel, thus, the time expenditure of P and, therefore, the overall time expenditure may be drastically reduced.

Figure 6 shows the time consumption of BCWD dataset can be calculated by data supplier P and data analysis C, and then overall time expenditure can be calculated by different data providers at first time, the P time can provide 2,150 s and the C time provides 3,100 s in the BCWD dataset. At P time provides 2,000 s and C time provides 2,900 s data providers 2, at the P time can be provides by 2,050 s and C time is 3,000 s data providers 3, at the P time is provides by 2,250 s and the C time can be provides by

3,250 s data providers 4, at the P time can be provided as 2,000 s and C time provides 3,150 s data providers 5 in the BCWD dataset.

Figure 6 Time consumption of hybridised secure SVM with BCWD dataset (see online version for colours)

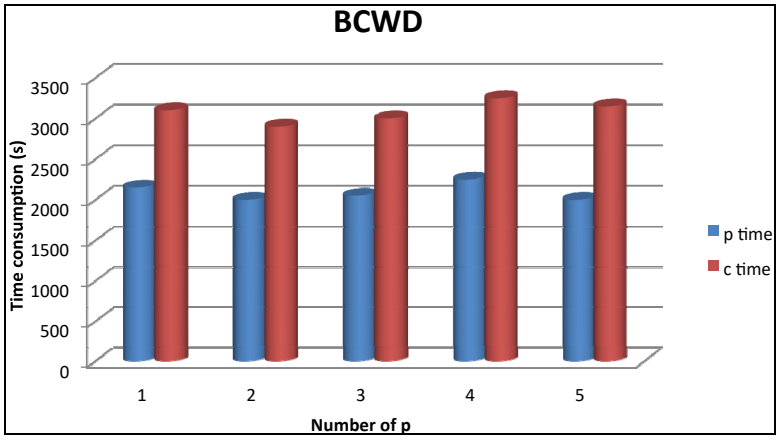
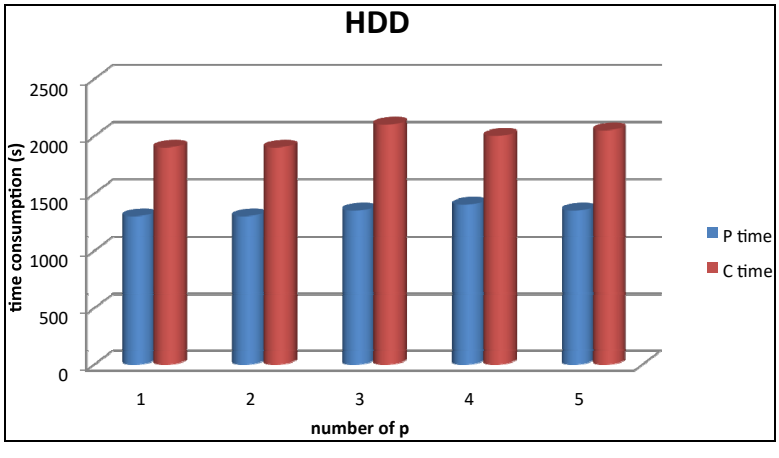


Figure 7 shows the time consumption of the HDD dataset can be calculated by data supplier P and data analysis C, and then overall time expenditure can be calculated by different data providers at first time the P time can be provided 1,300 s and the C time provides 1,900 s in data providers 1 in the HDD dataset. At P time provides 1,300 s and C time provides 1,900 s in data providers 2, at the P time can be provided by 1,350 s and C time is 2,100 s in data providers 3, at the P time is provides by 1,400 s and the C time can be provided by 2,000 s in data providers 4, at the P time can be provided as 1,350 s and C time provides 2,050 s data providers 5 in the HDD dataset.

Figure 7 Time consumption of hybridised secure SVM with BCWD dataset (see online version for colours)



Compared to the many types of databases, entire BCWD arithmetic attribute datasets or one HDD separate entire attribute dataset, hybridised secure SVM displays good robustness based on its time consumption.

6.7 Scalability evaluation

Hybrid secure SVM considers multiple IoT data providers are involved and offer the date. To judge the scalability of method, split the dataset into numerous equal parts for simulating the various scenarios of IoT data supplier. The calculation participates in the number of IoT data suppliers when changes in time consumption are observed.

The abscissa shows the number of IoT data suppliers implicated in the calculation and that time consumption is generated. In theory, the time expenditure of the hybrid SVM is intuitively associated to the number of knowledge again and again. As the total amount of knowledge and data quality does not change, raising the number of P is not related to time expenditure. To view the outcomes that time expenditure of the magnitude of P rises as 1 to 5, the overall time expenditure incorporates a small fluctuation because (Shen et al., 2019, 2020) the program execution time is affected via other processes in the host utilised for simulation.

7 Conclusions

This article provides a unique privacy-protection SVM training system called hybrid secure SVM that addressed the challenges of knowledge privacy and data integrity by using blockchain methods for creating an HHO-FFO algorithm in which IoT data is gathered as numerous data suppliers. The Paillier homomorphic cryptosystem is used to construct a well-organised and correct SVM training algorithm that preserves privacy. To illustrate the efficiency and safety of hybrid secure SVM. In future work, arrange to enlarge a generalised framework to build a good range of machine learning training algorithms that preserve privacy in multi-part encrypted databases.

References

Ahram, T., Sargolzaei, A., Sargolzaei, S., Daniels, J. and Amaba, B. (2017) 'Blockchain technology innovations', in *2017 IEEE Technology & Engineering Management Conference (TEMSCON)*, IEEE, June, pp.137–141.

Ajayi, O., Igbe, O. and Saadawi, T. (2019) 'Consortium blockchain-based architecture for cyber-attack signatures and features distribution', in *2019 IEEE 10th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON)*, IEEE, October, pp.541–549.

Azaria, A., Ekblaw, A., Vieira, T. and Lippman, A. (2016) 'MEDREC: using blockchain for medical data access and permission management', in *2016 2nd International Conference on Open and Big Data (OBD)*, IEEE, August, p.2530.

Baliyan, M., Bandooni, A., Sharad, A., Viswanathan, R., Mallikarjuna, B. and Edison, T. (2020) 'Prediction of decay modes of Higgs Boson using classification algorithms', *Journal of Critical Reviews*, Vol. 7, No. 7, pp.300–306.

Bhulania, P. and Raj, G. (2018) 'Analysis of cryptographic hash in blockchain for Bitcoin mining process', in *2018 International Conference on Advances in Computing and Communication Engineering (ICACCE)*, IEEE, June, pp.105–110.

Biswas, K. and Muthukkumarasamy, V. (2016) 'Securing smart cities using blockchain technology', in *2016 IEEE 18th international conference on high performance computing and communications; IEEE 14th International Conference on Smart City; IEEE 2nd International Conference on Data Science and Systems (HPCC/SmartCity/DSS)*, IEEE, pp.1392–1393.

Casino, F., Dasaklis, T.K. and Patsakis, C. (2019) 'A systematic literature review of blockchain-based applications: current status, classification and open issues', *Telematics and Informatics*, Vol. 36, pp.55–81.

Chen, Y., Ding, S., Xu, Z., Zheng, H. and Yang, S. (2019) 'Blockchain-based medical records secure storage and medical service framework', *Journal of Medical Systems*, Vol. 43, No. 1, p.5.

Demidova, L., Nikulchev, E. and Sokolova, Y. (2016) 'Big data classification using the SVM classifiers with the modified particle swarm optimization and the SVM ensembles', *International Journal of Advanced Computer Science and Applications*, Vol. 7, No. 5, pp.294–312.

Detrano, R., Janosi, A., Steinbrunn, W., Pfisterer, M., Schmid, J.J., Sandhu, S. and Froelicher, V. (1989) 'International application of a new probability algorithm for the diagnosis of coronary artery disease', *The American Journal of Cardiology*, Vol. 64, No. 5, pp.304–310.

Dhawale, D. and Kamboj, V.K. (2020) 'HHHO-IGWO: a new hybrid Harris Hawks optimizer for solving global optimization problems', in *2020 International Conference on Computation, Automation and Knowledge Management (ICCAKM)*, IEEE, January, pp.52–57.

Dorri, A., Steger, M., Kanhere, S.S. and Jurdak, R. (2017) 'Blockchain: a distributed solution to automotive security and privacy', *IEEE Communications Magazine*, Vol. 55, No. 12, pp.119–125.

Dua, D. and Graff, C. (2019) *UCI Machine Learning Repository*, Vol. 37 [online] http://archive.ics.uci.edu/ml (accessed 2023).

Eyal, I. (2017) 'Blockchain technology: transforming libertarian cryptocurrency dreams to finance and banking realities', *Computer*, Vol. 50, No. 9, pp.38–49.

Gao, F., Zhu, L., Shen, M., Sharif, K., Wan, Z. and Ren, K. (2018) 'A blockchain-based privacy-preserving payment mechanism for vehicle-to-grid networks', *IEEE Network*, Vol. 32, No. 6, pp.184–192.

Guo, R., Shi, H., Zhao, Q. and Zheng, D. (2018) 'Secure attribute-based signature scheme with multiple authorities for blockchain in electronic health records systems', *IEEE Access*, Vol. 6, pp.11676–11686.

Hou, H. (2017) 'The application of blockchain technology in e-government in China', in *2017 26th International Conference on Computer Communication and Networks (ICCCN)*, IEEE, July, pp.1–4.

Ioffe, A.D. (2017) 'Variational analysis of regular mappings', *Springer Monographs in Mathematics*, Springer, Cham.

Kassab, M.H., DeFranco, J., Malas, T., Laplante, P. and Neto, V.V.G. (2019) 'Exploring research in blockchain for healthcare and a roadmap for the future', *IEEE Transactions on Emerging Topics in Computing*, Vol. 9, No. 4, pp.1835–1852.

Kaur, H., Alam, M.A., Jameel, R., Mourya, A.K. and Chang, V. (2018) 'A proposed solution and future direction for blockchain-based heterogeneous medicare data in cloud environment', *Journal of Medical Systems*, Vol. 42, No. 8, p.156.

Kumar, T., Ramani, V., Ahmad, I., Braeken, A., Harjula, E. and Ylianttila, M. (2018) 'Blockchain utilization in healthcare: key requirements and challenges', in *2018 IEEE 20th International Conference on eHealth Networking, Applications and Services (Healthcom)*, IEEE, September, pp.1–7.

Le Nguyen, B., Lydia, E.L., Elhoseny, M., Pustokhina, I., Pustokhin, D.A., Selim, M.M. and Shankar, K. (2020) 'Privacy preserving blockchain technique to achieve secure and reliable sharing of IoT data', *CMC – Computers Materials & Continua*, Vol. 65, No. 1, pp.87–107.

Li, J., Greenwood, D. and Kassem, M. (2019) 'Blockchain in the built environment and construction industry: a systematic review, conceptual models and practical use cases', *Automation in Construction*, Vol. 102, pp.288–307.

Li, S. (2018) 'Application of blockchain technology in smart city infrastructure', in *2018 IEEE International Conference on Smart Internet of Things (SmartIoT)*, IEEE, August, pp.276–2766.

Mallikarjuna, B. (2020a) 'Feedback-based fuzzy resource management in IoT-based-cloud', *International Journal of Fog Computing*, IGI Global Publisher, January–June, Vol. 3, No. 1, pp.1–21, DOI: 10.4018/IJFC.2020010101.

Mallikarjuna, B. (2020b) 'Feedback-based resource utilization for smart home automation in fog assistance IoT-based cloud', *International Journal of Fog Computing*, January–June, Vol. 3, No. 1, pp.41–63.

Mallikarjuna, B. and Reddy, D.A.K. (2019) 'Healthcare application development in mobile and cloud environments', in *Internet of Things and Personalized Healthcare Systems*, pp.93–103, Springer, Singapore.

Mallikarjuna, B., Sathish, K., Krishna, P.V. and Viswanathan, R. (2020a) 'The effective SVM-based binary prediction of ground water table', *Evolutionary Intelligence*, Vol. 14, No. 2, pp.779–787.

Mallikarjuna, B., Ramana, T.V., Kallam, S., Patan, R. and Manikandan, R. (2020b) 'Visualizing Bitcoin using big data: mempool visualization, visualization, peer visualization, attack visual analysis, high-resolution visualization of Bitcoin systems, effectiveness', in *Blockchain, Big Data and Machine Learning*, pp.155–176, CRC Press.

Mallikarjuna, B., Viswanathan, R. and Naib, B.B. (2020c) 'Feedback-based gait identification using deep neural network classification', *Journal of Critical Reviews*, Vol. 7, No. 4, pp.661–667.

Mallikarjuna, B., Shahjad, M. and Dohare, T.A. (2019a) 'Feed forward approach for data processing in IoT over cloud', *International Journal of Innovative Technology and Exploring Engineering*, March, Vol. 8, No. 5, pp.899–903, ISSN: 2278-3079.

Mallikarjuna, B., Shahjad, M., Dohare, T.A. (2019b) 'Master slave scheduling architecture for data processing on internet of things', *International Journal of Innovative Technology and Exploring Engineering*, March, Vol. 8, No. 5, pp.556–559, ISSN: 2278-3079.

Mettler, M. (2016) 'Blockchain technology in healthcare: the revolution starts here', in *2016 IEEE 18th International Conference on E-Health Networking, Applications and Services (HealthCom)*, IEEE, September, pp.1–3.

Mylrea, M. and Gourisetti, S.N.G. (2017) 'Blockchain for smart grid resilience: exchanging distributed energy at speed, scale and security', in *2017 Resilience Week (RWS)*, IEEE, September, pp.18–23.

Nguyen, Q.K. (2016) 'Blockchain – a financial technology for future sustainable development', in *2016 3rd International Conference on Green Technology and Sustainable Development (GTSD)*, IEEE, November, pp.51–54.

Ølnes, S. and Jansen, A. (2017) 'Blockchain technology as s support infrastructure in e-government', in *International Conference on Electronic Government*, Springer, Cham, September, pp.215–227.

Parker, C. (2020) 'Firewalls don't stop dragons: a step-by-step guide to computer security and privacy for non-techies'.

Pinno, O.J.A., Gregio, A.R.A. and De Bona, L.C. (2017) 'Control chain: blockchain as a central enabler for access control authorizations in the IoT', in *GLOBECOM 2017-2017 IEEE Global Communications Conference*, IEEE, December, pp.1–6.

Rodríguez-Esparza, E., Zanella-Calzada, L.A., Oliva, D., Heidari, A.A., Zaldivar, D., Pérez-Cisneros, M. and Foong, L.K. (2020) 'An efficient Harris Hawks – inspired image segmentation method', *Expert Systems with Applications*, p.113428.

Salian, A., Shah, S., Shah, J. and Samdani, K. (2019) 'Review of blockchain enabled decentralized energy trading mechanisms', in *2019 IEEE International Conference on System, Computation, Automation and Networking (ICSCAN)*, IEEE, March, pp.1–7.

Salomaa, A. (2013) *Public-Key Cryptography*, Springer Science & Business Media.

Sari, A. (2017) 'The blockchain: overview of 'past' and 'future', *Transactions on Networks and Communications*, Vol. 5, No. 6, pp.39–47.

Shen, M., Ma, B., Zhu, L., Du, X. and Xu, K. (2018) 'Secure phrase search for intelligent processing of encrypted data in cloud-based IoT', *IEEE Internet of Things Journal*, Vol. 6, No. 2, pp.1998–2008.

Shen, M., Tang, X., Zhu, L., Du, X. and 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.

Shen, M., Zhu, L. and Xu, K. (2020) *Blockchain: Empowering Secure Data Sharing*, pp.1–130, Springer, Berlin/Heidelberg, Germany.

Shyry, S.P. (2014) 'Novel enhanced encryption algorithm for shared key generation', in *Proceedings of the 2014 International Conference on Interdisciplinary Advances in Applied Computing*, October, pp.1–7.

Sun, Y., Liu, J., Wang, J., Cao, Y. and Kato, N. (2020) 'When machine learning meets privacy in 6G: a survey', *IEEE Communications Surveys & Tutorials*, Vol. 22, No. 4, pp.2694–2724.

Tse, D., Zhang, B., Yang, Y., Cheng, C. and Mu, H. (2017) 'Blockchain application in food supply information security', in *2017 IEEE International Conference on Industrial Engineering and Engineering Management (IEEM)*, IEEE, December, pp.1357–1361.

Vo, Q.N., Tran, N.P., Van Dat Ngo, V.H.T., Huynh, Q.T., Ha, N.H. and Nguyen, D.M. (n.d.) 'Leverage the blockchain technology to manage smart contract in asset trading'.

Wang, F., Zhu, H., Lu, R., Zheng, Y. and Li, H. (2020) 'Achieve efficient and privacy-preserving disease risk assessment over multi-outsourced vertical datasets', *IEEE Transactions on Dependable and Secure Computing*.

Xia, Q.I., Sifah, E.B., Asamoah, K.O., Gao, J., Du, X. and Guizani, M. (2017) 'MeDShare: trust-less medical data sharing among cloud service providers via blockchain', *IEEE Access*, Vol. 5, pp.14757–14767.

Xu, Z., Darong, H., Ling, Z., Bo, M. and Yang, L. (2019) 'An improved LSSVM fault diagnosis classification method based on cross genetic particle swarm', in *2019 CAA Symposium on Fault Detection, Supervision and Safety for Technical Processes (SAFEPROCESS)*, IEEE, July, pp.165–169.

Zhang, Z. and Zhao, L. (2018) 'A design of digital rights management mechanism based on blockchain technology', in *International Conference on Blockchain*, Springer, Cham, June, pp.32–46.

Zheng, Z., Xie, S., Dai, H., Chen, X. and Wang, H. (2017) 'An overview of blockchain technology: architecture, consensus, and future trends', in *2017 IEEE International Congress on Big Data (BigData Congress)*, IEEE, June, pp.557–564.