**Indonesian Journal of Electrical Engineering and Computer Science**
Vol. 26, No. 2, May 2022, pp. 974~988
ISSN: 2502-4752, DOI: 10.11591/ijeecs.v26.i2.pp974-988

# A model for blockchain-based privacy-preserving for big data users on the internet of thing

**Ihab L. Hussein Alsammak[1], Mohammed F. Alomari[2], Intedhar Shakir Nasir[3], Wasan H. Itwee[4]**

[1]Ministry of Education, Directorate General of Education of Karbala, Karbala, Iraq
[2]Ministry of Education, Directorate General of Education of Thi Qar, Thi Qar, Iraq
[3]Department of Family and Community Medicine, College of Medicine, University of Karbala, Iraq
[4]Ministry of Construction, Housing, Municipalities and Public Works/General Directorate of Water and Sewerage/Karbala Sewerage Directorate, Iraq

**Article Info**

***Article history:***

Received Nov 11, 2021
Revised Feb 11, 2022
Accepted Mar 9, 2022

***Keywords:***

Big data users
Blockchain
Internet of things
Privacy-preserving
Smart cities

**ABSTRACT**

Recently, with the emergence and growth of the internet of things (IoT) as a promising vehicle for sustainable development, the concept of 'smart cities' has advanced significantly. However, many challenges inhibit the development of using IoT applications in smart cities, such as issues of privacy, scalability, trust, security, and centralisation. On a daily basis in smart cities, the IoT generates a large amount of data (big data) which could potentially be used for questionable or suspect purposes by attackers. The weight of the security issues surrounding big data must be acknowledged as the associated technology is continuously developing. To solve this issue, a strategy that secures important and potentially sensitive user information on a distributed blockchain and transmits non-sensitive information to the primary system by controlling the size of the blockchain is proposed. This solution cannot be achieved in traditional blockchain because it requires too many resources. The model is composed of three proposed algorithms: the first aims to allocate data to each user; the second performs the process of searching for data, and the third confirms the communication process. Experiments have proved that this proposed protocol for blockchain has excellent byzantine fault tolerance. The final experimental results of the proposed model established that the algorithms effectively meet the performance requirements.

***Corresponding Author:***

Ihab L Hussein Alsammak
Ministry of Education, Directorate General of Education of Karbala
Karbala, Iraq
Email: ihab_layth@karbala.edu.iq

## 1. INTRODUCTION

The internet of things (IoT) is essentially the utilisation of internet networks to connect and interlink computers and other technologically-enabled devices, and is recognised as being one of the most significant facilitating technologies in relation to application in smart cities [1]. In the IoT, the data is gathered from several physical sensors and devices in a real-time mode and subsequently shared over wireless networks [2]. The primary benefit of IoT applications for peoples' lives is achieved through big data analytics from information produced by the IoT and collected on smart devices. Thus, the term big data has become popular due to numerous developing technologies and applications present everywhere in daily life, such as smart homes, smart cities, smart grids, online e-commerce services, and social networks. Big data produced for IoT applications may implement and facilitate efficient data trading, providing a way to share and further increase the usefulness of data. For example, Facebook, Amazon, Tencent, and Alibaba collect big data on their user platforms [3]. These companies take advantage of technologies such as data mining and machine learning to analyse big data and inform decisions so as to improve their services. In todays' business climate, big data has become invaluable and has created a new data market pattern which includes DataExchange and Datacoup [4], [5]. However, the risk of privacy breaches associated with IoT technology may dissuade people from agreeing to participate in or contribute to IoT data analytics. Whilst IoT data-gathering could significantly assist decision-making, it is vital to ensure security and privacy throughout the data collection process. For example, it is possible that the collection of smart meter data could help citizens of an area to use energy more efficiently; however, the power usage data of the single user contains individual-specific behaviour patterns (such as being at home), which can have serious ramifications once disclosed. Therefore, a number of challenges must be overcome to achieve efficient data trading on the big data uses. The first is to ensure that a data consumer has the data available. The second is the privacy of a data provider that does not want to reveal its real identity to the data consumer.

The special characteristics of IoT, which include big data, memory capacity, processor capacity, bandwidth, and battery life make IoT security, trust, and privacy in sustainable smart city design challenging to maintain. However, the interconnection of different IoT sensors in smart networks leads to a variety of potential threats to IoT devices in smart cities. There are two possible types: cyber-attacks and physical assaults. Physical assaults are initiated when the assailants are closer to equipment and hence the sensors or devices in the network can be modified or tampered with [6]. It is critical that key aspects, which encompass safety, privacy, confidence, centralising, and scalability, are given high priority throughout the entire IoT infrastructure development in smart cities [7].

Therefore, security and public safety become important factors to avoid traditional crime, natural disasters, cyber-terrorism, and even cyber-crime. In 2017, IoT-world reported IoT security and privacy expenditure of approximately $700 million, and this is expected to reach $4.4 billion by 2022 [8]. There are many laws and hard rules to be published and standardized to make smart cities more trustworthy, reliable, sustainable and secure. Fundamentally, this means that cooperation, collaboration, and transparency amongst all stakeholders, entities, citizens, policies, and the community must be upheld. These security threats make smart cities vulnerable. Among all the concerns related to smart cities, the security threats ranked second through a survey of previous studies from i-SCOOP with approximately 100 IoT leaders [9]. The Threat Report prepared by Symantec stated the total number of attacks globally remains high. Therefore, researchers suggested that many security systems are required to defend smart cities against attacks. Among these systems is the Intrusion Detection System, which has been considered an essential security solution in identifying network and computer attacks. Additionally, other techniques that rely on algorithms such as clustering algorithms [10], and differential privacy algorithms [11] have been adopted to protect data security in most social network databases. However, this kind of algorithm is inadequate when using large databases due to randomness and sometimes poor data availability. The truth should thus be inferred from the inconsistent results and these unreliable and insecure IoT nodes are expected to be found and addressed [12]. Therefore, having trustworthiness in IoT nodes is vital in the establishment of holistic smart cities.

In this context, blockchain can be a viable option for distributed cloud support and fog infrastructures for IoT-capable smart cities and should therefore be carefully researched. To protect the privacy of websites, the research in [13], [14] have proposed blockchain as a more effective method than previous algorithms and techniques. The greatest advantage of using blockchain is that the operation of the system is not affected by damage or loss of nodes in the databases, and to break any system, the attacker would need to breach at least 51% of the nodes; thus, this has the potential to improve the security of big data [15], [16]. In smart cities, users are referred to as nodes and the nodes in blockchain technology do not require mutual trust between users to share data. Therefore, the above technology allows anyone in the network to share data and make the system transparent as the data used in the system is jointly maintained since each user node contains all the data. In other words, the data is divided into sensitive and other insensitive data, and sensitive information and passwords must be stored securely and protected from any attack, especially in relation to social networking sites. Moreover, the non-sensitive information is available to everyone; for example, publications, which can be stored physically.

There are numerous studies focusing on the issues of data security, privacy, and trust with the goal of detecting and preventing cyber-attacks. However, there are other challenges that must be addressed to develop safe and sustainable smart cities. The following are the main challenges:

a. The design of a safety system to separate regular behaviours effectively from abnormal observations with a high detection rate and accuracy in the IoT, fog, and cloud dynamic and wide city network is a significant challenge [2], [17].
b. Another difficult problem is developing a strategy of privacy-preserving to modify the original information to ensure that private knowledge and personal data remain confidential even after mining [18], [19].

c. Evaluation of the security mechanisms' efficacy with actual IoT-based information which represents actual IoT-based cyber threats in the world is also a challenge [2], [18].
d. Ensuring distributed IoT infrastructure in-chain and off-chain storage in the smart city, which is highly scalable with real-time data sharing platforms, is a complex undertaking. The decentralized design promotes overall scalability and failure tolerance in smart cities. It is difficult to ensure verifiable, traceable, and dependable services with time signs utilizing existing cloud architecture [20], [21] .

Our contributions:

a. We focus on the advantages of blockchain technology to promote coordination between many untrusted parties to IoT and symmetric encryption so as to allow calculation for encrypted data without exposing raw data in a new scheme during the IoT data aggregation process. The benefit of blockchain infrastructures is that it removes the big data single-point failures.
b. In this paper, we employ blockchain technology to secure the privacy of users in big data settings and a customer power processing data storage approach for addressing the above-mentioned smart city challenges. Blockchain technology facilitates connections amongst users without a trusted centralised structure.

Motivated by this, we propose a new model based on blockchain to solve the problem of data synchronization and data storage by applying to gradually build a verifiable database in order to eliminate malicious activity. The main contribution of this paper is proposing a data storage blockchain paradigm. We are developing a mechanism that is built-in opposite the current database that will gather sensitive data so as to address data synchronization issues and enhance user workstation performance.

The rest of this paper is organized as shown in: Section 2 discusses works related to blockchain background and big data security. Section 3 introduces the proposed model for blockchain technology with an outline of these models. Section 4 validates the model observation and discusses experiment and performance evaluation. Section 5 concludes the paper and describes the future work that is planned.

## 2. RELATED WORK

The privacy-preserving of big data collection has been a research concern because, throughout the data collecting process, it can ensure the privacy of sensitive information. Indeed, with the internet of things, many solutions have already been proposed to overcome this issue. Through analysis and reading the related work studies, the relevant proposals are outlined for some areas, with a focus on preserving user privacy based on distributed data collection techniques, safeguarding user raw data according to homogenous data encryption, and protecting user identification based on blockchain technology.

Xing *et al.* [22] and Alsammak *et al.* [23] employed K-means to protect the privacy of social networks' big data. Each K-mean cluster iteration utilises two algorithms that maintain privacy and confidentiality. In the first algorithm, every participant finds the next cluster, the centre of which is concealed from others. The second algorithm calculates the cluster centres so that participants do not discover others inside the same cluster. The experiment findings demonstrate that this strategy is robust to collusion attacks. This is an efficient approach for preserving participants’ privacy; however, the data protection impact differs from K-means clustering outcomes.

Yang *et al.* [24] and Alsammak [25] proposed smart data storage and a self-adapting access control system for IoT privacy protection, in order to maintain the security of healthcare data. A smart data sharing mechanism is established to allow all authorized or official users in numerous ranges of the system to access the patients' historical medical data. A new twofold access control system ensuring that authorized medical staff are allowed access to all patient medical data with normal circumstances has been developed to solve the issue that previously, those administering first aid treatment could not access any historic patient data. Moreover, this allows first aid treatment using a password breaking glass access technique which will recover the historic data of the patient. Concerning overhead storage, they have developed a secure method of deleting duplicate medical files. Upon deletion, all users who were authorized through the various access policies can access the rest of the files. The results show acceptable computation and storage costs performance.

Yang *et al.* [26] suggested a dynamic cross-domain collection authentication system, which would allow the patients of several institutions to communicate safely in groups. Essentially, a group of patients use GKA to create a group key and their information is safeguarded. Moreover, a group agreement process assures that the key may be identified by approved patients with the same symptoms. This technique promotes both anonymity and traceability of patients to prevent recovery of patient identities and symptoms in medical institutions. Experiments confirm that the system is secure and performs effectively.

In order to encrypt and randomize the query in a given session, Ren *et al.* [27] proposed an exclusive encryption homomorphism (XOR). The algorithm prevents leakage of data and access patterns and keeps specific characteristics after randomization in data structures. A homomorphism evaluation key is used to calculate the search evaluations on demand, which improves cloud protection. Encryption of XOR homomorphism provides a higher level of security than recent search encryption techniques, thereby decreasing the risk of attackers leaking search patterns. The results of their study demonstrate that their scheme is effective and feasible.

Sun *et al.* [28] has proposed a new algorithm named dummy location privacy (DLP) for the purpose of efficiently maintaining privacy. The authors considered that external attackers will exploit collateral information. The proposed algorithm for maintaining privacy and data security was adopted by choosing an ideal and dummy location. The outcomes of their experiment show that ADLS is very likely to find information about the reallocation, whereas DLS is unlikely to expose users' real locations.

Gao *et al.* [29] developed a V2G network payment method using blockchain-based privacy-preserving, which can fulfil data sharing and protection requirements inside the V2G network. They preserved the privacy of traders in their research by adopting a digital signature registration method. The new payment method may perform payment audits following the process while protecting the privacy of data. The payment method on a blockchain architecture ensures that the payment procedure is reliable. This transaction becomes irreversible and unrepudiated once the transaction is recorded. The experiment results confirm that the approach is feasible and successful. However, each node in the network has a copy of the global ledger in the blockchain network that contains every record of transactions and some additional characteristics. Hence, the memory and time consumption requirements of this approach are fairly unacceptable.

In order to protect vehicles' locations and trajectories, Liao *et al.* [30] proposed a VSN system and 5G based on MFemtocell technologies. They measure the vehicle location and their privacy through an enhanced composite metric KDT and increase the probability of swapping pseudonyms using a dynamic group division (DGD). This system consists of four main components: initial system, group generation, exchange of pseudonyms, and group cancellation that fulfil the dynamic 5G character. The results of the researchers' simulation verify that DGD can efficiently preserve the privacy and vehicle location in 5G VANs.

Christidis and Devetsikiotis [31] proposed blockchain technologies for IoT. The combination of the blockchain with the IoT was described as supporting the sharing of services and resources, establishing a market for services around various devices, and the Crypted and verified automation of several current time-intensive procedures. Digital assets were also taken into consideration in privacy and online transactions. Cryptographical verification may be performed by combining smart contracts and blockchain with IoT technology. In addition, the cost and time requirements of the process may be significantly improved. However, some configurations require considerable caution when being adopted, as blockchain solutions often lead to rising latency lower and transaction output and the challenge of privacy protection in blockchain techniques.

Recently, there has been increased academic interest in blockchain technology. For instance, the Pramanik *et al.* [32] reported that approximately 15% of banks are already utilising blockchain technology, and there has been substantial investigation of its use in relation to IoT. Additionally, topics such as the impact of blockchain on healthcare, investment, supply chains, and transportation have come under significant scrutiny. The authors highlighted the need for preserving privacy in blockchain technology based IoT and the challenges of blockchain technology privacy in relation to IoT systems. In 2017, blockchain technology expenditure was $333.5 million, and this figure was expected to reach $2.3 billion by 2021. Previous studies on the global use of blockchain technology were derived from 22,500 sources within the date range of 2016 to 2021, as shown in Figure 1. IoT's unprecedented growth has created opportunities for the new community, such as means of accessing, sharing, and opening the data. However, the lack of trust is one of these projects' most significant weaknesses, and due to gaps in integrity and security of the data flows, businesses have faced various obstacles in IoT adoption.

Khan *et al.* [33] focused on the scope of healthcare, discussing security challenges on the smart grid to maintain sustainable development. Relying on blockchain technology, a sophisticated network for healthcare applications has been created to automate medical records by mobile application model denominate HDG. Bibri [34] focused on the sustainable environment in smart cities, proposing a framework for sensor data applications. Park and Park [35] studied blockchain technology and security issues, applying security case studies in cloud computing environments including attacks. Li *et al.* [36], the authors review the security of blockchain technology based on real attacks and scanning threats. Researchers analysed the associated vulnerabilities and their security solutions. Blockchain is one of the most reliable and safest architectural frameworks for the construction of a parallel intelligence transport management system. blockchain technology in the proposed system enables the allows building of an ecosystem that is more efficient, notably for crowd-funding technologies through the development of a safe, dependable, decentralized, and independent system. Blockchain technology challenges are being surveyed by Prasahant *et al.* [37] discussed security and privacy while developing the most secure possible solutions. The authors evaluated algorithms related to security and privacy, and challenges of opportunities and consensus. Liu *et al*. [38] proposed approach examines issues related to data storage, data transmission, privacy and security within a framework based on blockchain technology, but dependent on a central server.

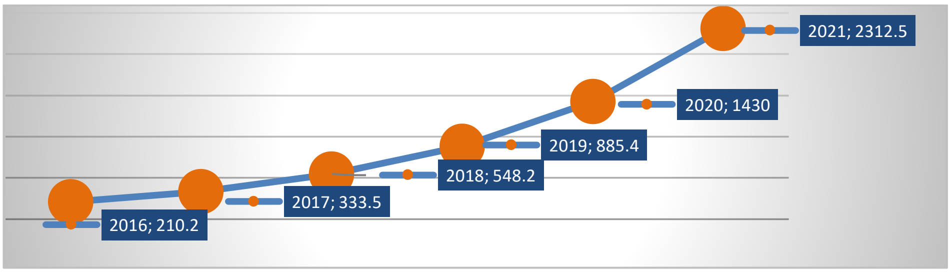

Figure 1. Blockchain-based technology around the world over the past years

Finally, researchers may ask why blockchain? There are many reasons for focusing on blockchain, as smart cities face many technological challenges in deployment and implementation. They can be summarized given as:

- In order to improve the city and extend effective services there is a necessity to efficiently collect and analyse data, so data reliability and integrity is essential, and any unauthorized modification in data may lead to disastrous outcomes.
- Over time, the applications and number of devices become more complex in smart cities, thus they require flexibility in devices and nodes. To achieve these demands, decentralized systems have been relied upon as they are more convenient and flexible than traditional centralized systems in smart cities.
- On the other hand, in a city, the citizens have a powerful affinity for transparency. That means the government should convey certain information to them. This sharing of data between citizens can improve city management and decision making.

Blockchain technology has been deemed the optimum means of addressing the challenges related to smart cities and their data that have been discussed above, as it encompasses the key components required to be successful. Blockchain has several merits (decentralization, immutability, democracy, pseudonymity, security, and transparency), and these merits facilitate transparent city management and decision-making, guarantee data integrity, and create a democratic smart city. Blockchain is supported by many core technologies, including the cryptographic hash, distributed consensus algorithm, and digital signatures, and it operates in a decentralized environment. The blockchain architecture in general is composed of six main layers: the data layer, consensus layer, network layer and incentives. Over the past years, due to distributed blockchain architecture, the blockchain technique was used in large enterprises to recover their security infrastructure and for analysing and extracting data, as shown in Figure 2. This framework enables monitoring of the system, tracking each device and its interactions, and recording every action performed. Accordingly, blockchain technology has attracted significant attention from both academia and industry, and there are many studies about checking the use of these technologies in IoT, especially in the context of smart cities.

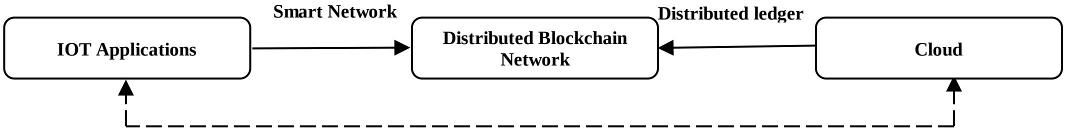

Figure 2. Blockchain technique architecture (analysis data and extract it)

In general, blockchain technology can be categorized into permissioned blockchain and public blockchain. The permissioned as in hyper ledger, allows only approved entities to join the network, while as in Bitcoin, the public blockchain allows anyone to join and contribute to the network [34], [39]. However, when blockchain users incorporate it with their business, they should be aware if it meets the requirements. For this reason, to test different blockchains, a blockchain testing mechanism is required. In recent studies, this test is divided into two phases: standardization and testing. Furthermore, in traditional blockchain technology, there is a weakness in terms of data synchronization since all nodes must Synchronize with the entire database to ensure consistency. When the system in blockchain has an enormous number of users, and these users form social chains, most of the database files exceed 1000 GB, which is the most serious weakness in social chains. A new model should be designed to address these issues. To defeat advanced attacks, collaborative intrusion detection with the development of IoT has been widely studied in recent years through exchanging data. Social networks like Facebook and Twitter do not save transaction data for this reason. Then in [40], [41] efforts are concentrated on confidence management.

## 3. SYSTEM MODEL

### 3.1. The major objectives of the system model

Although many researchers have studied the subject of big data collection for IoT applications, there is still a need to address numerous challenges in order to resolve the issue of privacy-preserving in this field. First, all data produced is stored, aggregated, and analysed by a central authority, so the only point of trust must be eliminated by storing the data in a distributed manner. Second, all the raw data produced by the smart devices is given to a trusted party to be collected through an end-to-end encryption data collection method to overcome detection. Finally, to ensure three security properties: privacy of data, data integrity, and the sending identity control, a confidentially-controlled solution must use asymmetric encryption, hash and digital signature features (i.e., authentication data). To the best of our knowledge, none of the proposed solutions consider any of the aforementioned data privacy aspects, from the user's consent to data analysis, covering the whole IoT data life cycle.

### 3.2. Blockchain model and distribution principle

This section describes the model proposed in this article. Furthermore, the proposed solution, as mentioned above, is based on blockchain technology which is also discussed in this section. In fact, while using the offered services, users want to protect their privacy. Thus, multi-user collaboration to aggregate IoT data precludes individual customer data. However, IoT data must be collected by network management and a trustworthy aggregator. This problem is addressed by creating a model system to improve the privacy of users while maintaining the accuracy of big data. Thus, our system model is based on: (i) Blockchain data storage technology; (ii) An intelligent contract acting as a controller for the aggregation of data; and (iii) A homomorphic encryption technology enabling the calculation of encrypted data without trusting a consumer or aggregator.

Blockchain technology is a distributed computing model that effectively addresses the central party trust problem. Within a blockchain network, several nodes cooperate to safeguard and maintain records of shared transactions in a distributed manner, without relying on a trustworthy party. The data gathered in the blockchain are permanent records that cannot be altered or updated after creation. Immutability is coupled to safety, security, strength irreversibility, and resilience. Given that public blockchain is transparent, it is possible to verify that the data on a transaction exists at a certain time, but the real identity of the participants cannot be exposed as the anonymity of the public keys is upheld. Transactions are therefore open to the public, although they have no information linked to anybody [42].

#### 3.2.1. Data synchronization

It is worth noting that the main problem in traditional blockchain technology is data synchronization since every node in the blockchain network must synchronize the whole database and all data can be seen Figure 3. However, if there are many users of the blockchain system, the whole database file might surpass 1 TB, as frequently occurs in social chains. This is in practice the most critical factor for social chain weakness compared to centralized distributed databases because the size of the hard drive is limited and may not exceed 1000 GB, thus the ledger may occupy more than 10% of the space on the disk. Therefore, this will greatly affect the users' PC performance. To solve this problem, a new model has been built to take into account the capabilities of ordinary workstations. In order to resolve the issue of privacy-preserving for big data users in IoT applications, we proposed three algorithms, which in turn will be the new model, based on blockchain technology. This paper puts forward a new model based on three algorithms which aim to resolve the privacy issues as: an allocating data algorithm for each user, a data search algorithm, and finally, a confirmation of communication process algorithm. Figure 4 illustrates our model structure in which only personal data can be seen with a capability-based partial database.

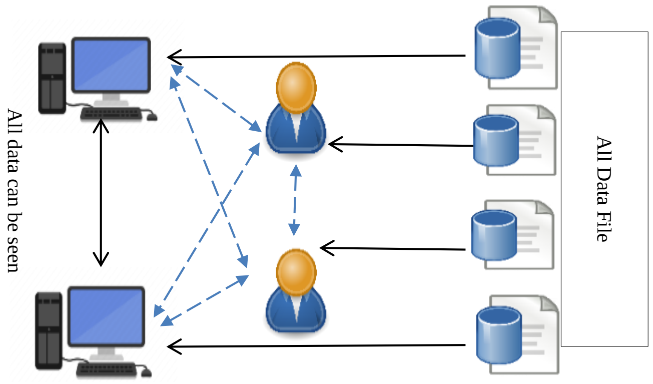

Figure 3. Structure of traditional blockchain system

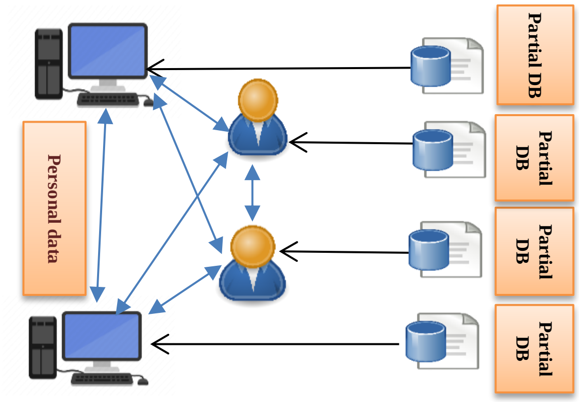

Figure 4. Structure of new model

This section shows several notations used in this paper. We refer to the user with the symbol (u) who has free HD space on his computer (S), and who has joined the system of the network of some IoT application at the given time as (t). At the time (T) the overall data created by the social chain is referred to as (I).

In this work, an assumption is made that there is a sufficiently large number of members in the social network, and a data file is assigned to each one. Note that the file size is confirmed and will never change. Regardless of how much data is generated by the social chain, each user has time to join the social network, and upon doing to, the user u syncs a certain amount of data, with the file size depending on u's system capacity. The data size is represented as (Z), therefore, for every user u:

$$Z_u = \frac{S_u}{100} \quad (1)$$

To ensure the performance of the model, free hard disk space of the user's system for u occupies only 1/100. In the social chain, the data stored has two key concepts, as shown in Figure 5. Now, the ledger saved in u can be defined as (Lu) and Transaction t created by u as (tu) at T0 as time in L 1. Head is an encryption transaction content that reduces the time of certification, and its body stores the transaction of encrypted contents including user behaviour, user ID, timestamp, and type of behaviour. Once the storage is allocated to the data, it is necessary to determine which part of it should be written in Z, in addition to designing a standard responsible for dividing the data files to ensure the existence of backup files. The data partition mechanism depends on stages, including the user synchronizing the Z data with the proposed sync algorithm from within the new model when connecting the social chain, and at this juncture, it may be that two different users save the same data. When the data is synchronized, each block may be marked and the number will be sent to the user.

In Algorithm 1, the process is to allocate data for every user, for each, u after hash encrypting have id as $u_{id}$ and data stores transaction i. The next steps allocate the data and mark the allocated transactions to user u, then ensures that the data size is fair. While performing the algorithm at time T1, it is assumed that

Lu1 is being revised or broken for unknown reasons, taking into account ensuring continued performance in the event of loss of node u. For any condition consequent to the timestamp and size of the social network, the review request will be rejected. Here, it is impossible to register tu in one node. Differing from the Bitcoin system, users in the proposed model do not have a ledger total, as the proposed storage algorithm does not contain private user data. We proposed the content of a request for our model, as depicted in Table 1. During the stage that commences with broadcasting the request, each u nodes defined in the package are compared to the u id that it owns. A node can fulfil the type of matching parameters if it stores data for u id.

Table 1. Contents of the model

| No | Name | Description |
|---|---|---|
| 1 | s | Free HD space in computer |
| 2 | T | time |
| 3 | I | Total information |
| 4 | u | User |
| 5 | t | Joining time |
| 6 | $u_{id}$ | User ID after hashing |
| 7 | Z | Size of the data |
| 8 | $L_u$ | Ledger saved in u |
| 9 | uaddr | User network address |
| 10 | $L_t$ | ledger generated (Δt to t) from t |
| 11 | b | Block |

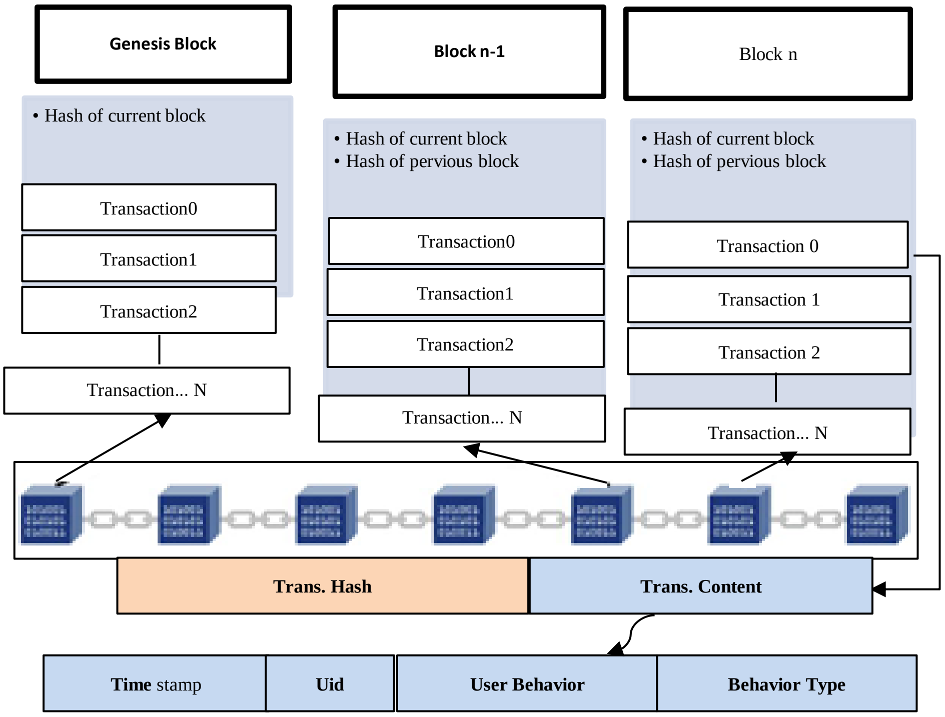

Figure 5. The data structure in the social chain

Algorithm 1. Allocating data for every user

```
1   MAKE SURE: L U
2   Parameters: Index [],i = 1,D= data. Length (), data [] = Value (0, t)
3   If: i < D Do
4   Set: Index [i] = min (data) , Delete (data [ i ]), i=i+1,
5   $L_u$= Data (get Data (i))
6   $z_u$ = $z_u$ − size (get Data (i))
7   Else Do
8   If ($z_u$ < = 0) Do Break;
9   Else go to 3
10  End if, End if
11  End
```

The second procedure followed by the data search in Algorithm 2 returns the timestamp and all nodes and their search results to u. As the transaction is encrypted, there is no threat to breaches of user privacy at this point. Another aspect that differentiates it from the Bitcoin system is that a social network may create more than 10 GB of data per day. The proposed model does not store all user data so as to reduce the computational cost and the resources required for storage; instead, the system stores sensitive data only. Therefore, the place to store the data must be determined according to its type, including general data and other unnecessary traditional data, and this is addressed with the data search algorithm.

Algorithm 2. Data search

```
Evaluate broadcast
Parameter: usid =Username, $u_{addr}$ = Addr(),$t_s$ = generate T() ,$t_u$ = null , i = 1
Initialize Req = genPack ($u_{id}$, $u_{add r}$, Type, $t_s$)
Initialize ReqPac = genPack ($u_{id}$, $u_{addr}$, Type, $t_s$)
While ($L_u$.length (i )<>0) Do
If ($L_u$[i]. $u_{id}$ = Req.$u_{s id}$ )&& ($L_u$ [ i ] .Type = Req.Type) Do
$t_u$ = $L_u$ [i]. Transaction, $t_s$ = generate T, Trans = gen Pack ($t_u$, $t_s$)
Else Do Break
$L_u$.length (i )= $L_u$.length (i )-1
End if
End
```

From the search algorithm, it is clear that the work of the proposed model behaves like an installed filter, that is, it does not replace the current databases but rather before the current database. The basis for the work of the first and second algorithms is that the new system collects sensitive data and neglects general data and packets of data collection as encrypted transactions while transmitting data to the existing insensitive database. Figure 6 illustrates the mechanism of writing data to the database.

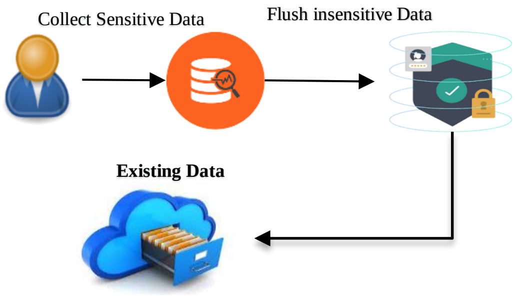

Figure 6. Mechanism of writing data to the database

### 3.2.2. Confirmation of communication

One of the most important protocols, which is the core of the blockchain, is called the consensus protocol. This protocol has been used to authenticate the transaction in the quickest possible time. However, existing protocols of consensus of the public are unsuitable in a social network since the device of a user may not function adequately. Consequently, it is essential to design a protocol that will be accepted by the majority of users' devices and that has good fault tolerance and is capable of maintaining a stable connection.

The proposed protocol in this paper is based on a time-based block generation method [43]. The basis for the proposed protocol to work is the possibility of adding one block to the consensus chain at a time. One of its advantages is that it functions safely, even if there are some bad nodes. The proposed protocol consists of two sets of elements: timestamp and $u_{id}$. The timestamp is defined as the time at which the user chooses the block and the user id after the hash as $u_{id}$. The protocol is described to achieve the desired goals where it was imposed at time t, and a block b is generated, as shown in Figure 7. Additionally, the time interval for block generation is fixed due to the method of generation. Here, a candidate will be chosen to be an owner who has the advantage that after control of the block, its computational ability will not be affected, while the rest of the candidates will keep track of the user with the highest number depending on the methods of detection for malicious users [44], [45] and according to Algorithm 3.

Algorithm 3. Confirmation of communication process

```
Parameter : c = 0, j = 1, k = 1, i=1 ,Count [$u_{id}$ .length ()] = 0
While (j ≤ $u_{id}$ .length ()) Do
    If ($L_t$ .$u_{id}$ [ i ] == $u_{id}^{j}$ ) && (i ≤ $L_t$ .length () ) Do J=j+1
    A= $u_{id}^{count[j]}$
    If (k ≤ j) Do k =k+1
        $u_k$ . Follow (A)
    Else Do b = gene Block (A)
        $u_{id}$ .Del(k )
    End if
End if
End
```

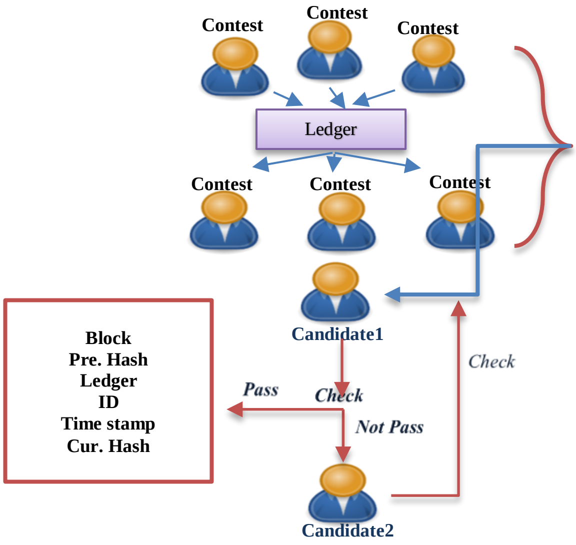

Figure 7. The proposed protocol

As mentioned previously, the proposed system is aimed at improving data security and storing sensitive data. Figure 7 shows the technology for storing sensitive data and who can see this data. This technology is divided into a category that has the power to grant the owner of the package the rights to access the visitors, and the second category verifies their identities.

In the proposed model, it is assumed that the visitor is "B" and the owner of the data package is "A". According to the visitor's status and depending on the proposed system that will verify the number of blocks, if the number of blocks owned by the visitor is large, then they will not be considered an attacker, or vice versa. The work stages begin to check if "B" as a new user in the system wants to access sensitive information; in that case, the identity of the user will first be verified and they must agree to synchronize all data and reveal the blocks that they own. In the event that the synchronization is incomplete, this means that this user does not have sufficient computing power, then the system will reject it, otherwise, it will be allowed to access the data. One of the basic steps in the system is to encrypt user privacy, as every transaction will be encrypted depending on the data distribution criterion.

### 3.2.3. Privacy-preserving mechanism

In conventional blockchain technology, the data is clear; therefore, blockchain is incapable of guaranteeing user privacy as every blockchain network may check the systems' total ledger. If an attacker hacks into blockchain through a users' computer, all the ledgers are visible. Thus, it is essential to encrypt user behaviours to ensure privacy in a blockchain-based architecture.

The method of user interaction is as shown in: when User#1 sends a message M to User#2: (1) User#1 will sign to User#2 the content using signature algorithm; (2) User#1 will transmit to User#2 the ciphertext c. (3) User#2 receives the ciphertext" c" and a private key is used to decrypt it (4) User#2 will see the message. Figure 8 presents the message sending procedure.

At this point, the message must be encrypted whilst noting that homomorphic encryption enhances the elliptic-curve cryptography (ECC) algorithm. In addition, a message is split into parts as n to improve the algorithms' security. Subsequently, the ECC (SHECC) has lower encryption and decryption time than the ECC. Moreover, because SHECC divides the message in n at random, no part carries all this message, which enhances the systems' security.

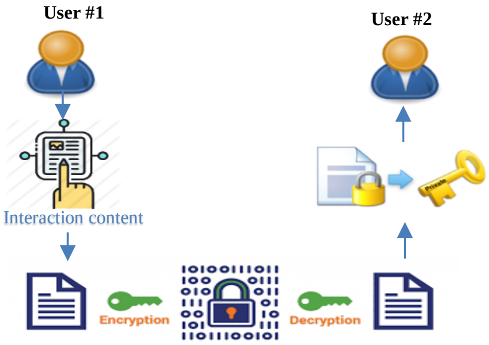

Figure 8. User-communication method

After some time, the user#1-user#2 interaction is encrypted into an ECC-encrypted transaction and transmitted to the generation block. The ECC encryption algorithm was selected because is an asymmetrical algorithm for encryption, therefore attackers cannot crack it during transmission. Additionally, the ECC algorithm provides a shorter output and takes less time, which allows users to save additional data in limited HD space, compared with Rivest–Shamir–Adleman (RSA) and ZK-SNARk algorithms.

## 4. EXPERIMENTS AND DISCUSSION OF RESULTS

The aim of this section is to confirm that the model effectively achieves the required performance. To analyse the models' performance, information about user behaviours for big data in Twitter and Weibo are necessary. In general, fully symmetric encryption (FHE) is very time-consuming, especially when the size of the data is very large, however, traditional blockchain technology facilitates faster searches due to the search mechanism. Figure 9 demonstrates how both our model and a traditional blockchain system are memorized when a user saves the data identified on the computer. Through experiments, our model with SHECC has shown that large amounts of memory are saved. The memory used in SHECC is only 80% of ECCs and 30% of RSA specifically. This means that our model only needs 1/30 of the ECC memory required by the traditional approach. Following the testing of several significant performance levels of the model and a traditional blockchain system, the impact on user systems was also examined. To assess the impacts of our model and conventional blockchain system three different computers were used. Additionally, three hosts were adopted in the system configurations in our experiments: (Host1, Host2, and Host3). Each host has the following properties:

- Host1 has CPU i7-4720HQ (4 cores, 8 threads, 2.6 GHz), HD = 1 TB and memory = 8 GB
- Host2 has CPU i7-6700K (4 cores, 8 threads, 4 GHz), HD = 1 TB and memory = 8 GB
- Host3 has CPU i7-7700K (4 cores, 8 threads, 4.2 GHz), HD = 1 TB and memory = 16 GB

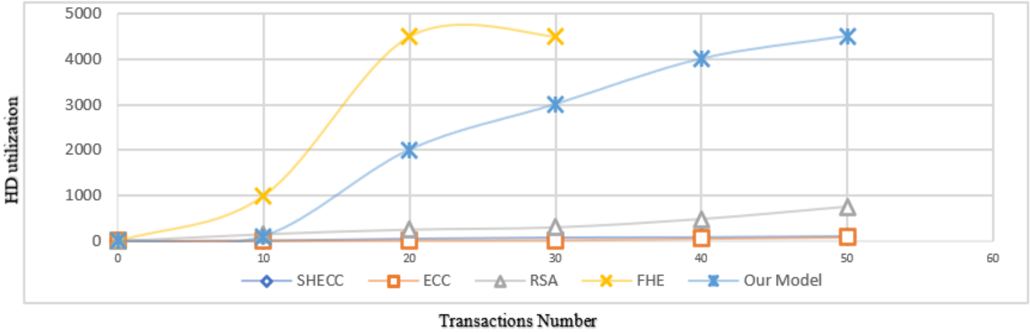

Figure 9. The use of HD space

In terms of memory utilization and storage capacity, the storage of identical data in both systems was applied (the blockchain system and the proposed system). The experiments focused on election Ability and data synchronization ability between the traditional blockchain system and our model. Computers used by most social media users perform similarly to Host1 and Host2 after testing important performance levels, and the final results are shown in Table 2.

The experiment tested the impact of the confirmation of communication process on CPUs with different numbers of blocks and proof of stake and proof of work. The terminals' results are shown in Figure 10. Our confirmation of communication process in social networks was found to be most effective and delivered the best performance when compared with proof of work and proof of stake.

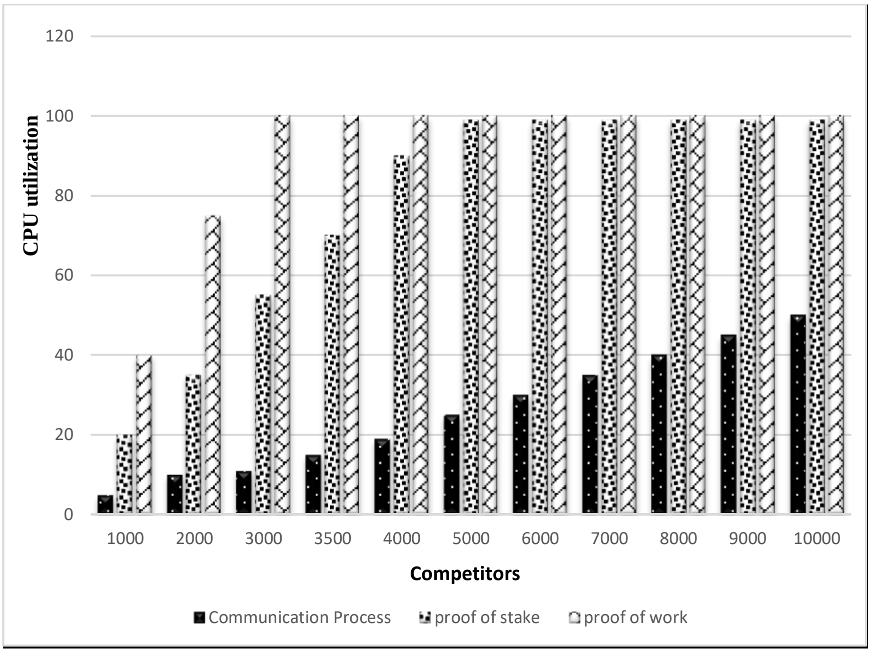

Figure 10. CPU utilization of communication process, proof of work, and proof of stake

Table 2. The tolerance in the traditional blockchain system and the proposed model

| Host name | Total ledger size | Traditional blockchain system | | Our model | |
|---|---|---|---|---|---|
| | | Data synchronization ability | Election ability | Data synchronization ability | Election ability |
| Host1 | 16 | * | * | * | * |
| Host2 | 16 | * | * | * | * |
| Host1 | 64 | * | * | * | * |
| Host2 | 64 | * | * | * | * |
| Host1 | 128 | * | * | * | |
| Host2 | 128 | * | * | * | |
| Host1 | 256 | * | * | | |
| Host2 | 256 | * | * | | |
| Host1 | 512 | * | * | | |
| Host2 | 512 | * | * | | |

To ensure the performance of the proposed model, the proposed protocol must have perfect for Byzantine fault tolerance, especially with the large numbers of users in social networks. A malicious or bad node aimed to affix itself in the consensus chain was generated so as to evaluate the Byzantine fault tolerance. This was subsequently compared to the Byzantine fault tolerance in both proof of work and proof of stake. The suggested number of users for the network was 5,000 subscribers, and the results showed that the proposed model may face a Byzantine fault tolerance for a small number of users, so it is possible to trust the model in most cases compared to the others. Table 3 presents the testing results. In Big Data environments, our model was also compared to some other techniques of protection of privacy so as to measure the communication costs of our model with the K-means cluster [22]. The dimensions of a transaction show that our model is less expensive than the cluster K-means.

Table 3. Evaluate Byzantine fault tolerance

| Number of | Consensus protocol | | |
|---|---|---|---|
| users | Our Protocol | Proof of work | Proof of stake |
| 100 | ✓ | × | × |
| 250 | ✓ | × | × |
| 500 | ✓ | × | × |
| 1000 | ✓ | × | × |
| 1500 | ✓ | × | × |
| 2000 | ✓ | × | × |
| 2500 | × | × | × |
| 3000 | × | × | × |
| 3500 | × | × | × |
| 4000 | × | × | × |
| 4500 | × | × | × |
| 5000 | × | × | × |

## 5. CONCLUSION

In recent years, many studies have agreed that a peer-to-peer system is generated by combining the blockchain and the IoT, where peers interact in an auditable and unreliable manner. However, few of the proposed solutions have dealt with leveraging this technology in order to keep users' IoT big data private from a comprehensive perspective. In this paper, blockchain technology was employed to secure the privacy of users in big data settings, and a customer power processing data storage approach was implemented to address the abovementioned smart city challenges. For this reason, a blockchain-based model has been proposed to protect the big data of users' applications in smart cities with privacy-preserving security. Our model prioritised managing blockchain size so as to maintain computational capacity and database storage where sensitive user information is protected, and non-sensitive information is excluded and sent to the primary system. Our model is composed of three algorithms: an algorithm for allocating data for every user, a data search algorithm, and an algorithm for the confirmation of the communication process. The experiment proved that the proposed protocol for blockchain has excellent Byzantine fault tolerance and comparisons with previous studies showed that the algorithms effectively meet the performance requirements.

## REFERENCES

[1] A. Nayyar, R. Rameshwar, and A. Solanki, *Internet of Things (IoT) and the Digital Business Environment: A Standpoint Inclusive Cyber Space, Cyber Crimes, and Cybersecurity*, 1st Edition. 2020.

[2] N. Chaabouni, M. Mosbah, A. Zemmari, C. Sauvignac, and P. Faruki, “Network intrusion detection for IoT security based on learning techniques,” *IEEE Communications Surveys and Tutorials*, vol. 21, no. 3, pp. 2671–2701, 2019, doi: 10.1109/COMST.2019.2896380.

[3] W. T. Wang, Y. S. Wang, and E. R. Liu, “The stickiness intention of group-buying websites: The integration of the commitment–trust theory and e-commerce success model,” *Information and Management*, vol. 53, no. 5, pp. 625–642, Jul. 2016, doi: 10.1016/j.im.2016.01.006.

[4] T. Jung et al., “AccountTrade: Accountable protocols for big data trading against dishonest consumers,” in *Proceedings - IEEE INFOCOM*, May 2017, pp. 1–9, doi: 10.1109/INFOCOM.2017.8057004.

[5] F. Liang, W. Yu, D. An, Q. Yang, X. Fu, and W. Zhao, “A survey on big data market: pricing, trading and protection,” *IEEE Access*, vol. 6, pp. 15132–15154, 2018, doi: 10.1109/ACCESS.2018.2806881.

[6] Y. I. Alzoubi, A. Al-Ahmad, and A. Jaradat, “Fog computing security and privacy issues, open challenges, and blockchain solution: An overview,” *International Journal of Electrical and Computer Engineering*, vol. 11, no. 6, pp. 5081–5088, Dec. 2021, doi: 10.11591/ijece.v11i6.pp5081-5088.

[7] S. K. Funde and G. Swain, “Security aware information classification in health care big data,” *International Journal of Electrical and Computer Engineering*, vol. 11, no. 5, pp. 4439–4448, Oct. 2021, doi: 10.11591/ijece.v11i5.pp4439-4448.

[8] *An overview of the IoT Security Market Report 2017-2022*,” IoT Analytics 2017, Accessed: May 15, 2020. [Online]. Available: https://iiot-world.com/reports/an-overview-of-the-iot-security-market-report-2017-2022/#wpcf7-f7856-o1

[9] IESE Insight, “New York, London and Paris Firmly Established as the Smartest Cities,” *Iese*, 2018. http://www.ieseinsight.com/doc.aspx?id=2124&ar=&idi=2&idioma=2. (Accessed on 26 June 2020).

[10] A. H. Ali, M. N. Abbod, M. K. Khaleel, M. A. Mohammed, and T. Sutikno, “Large scale data analysis using MLlib,” *TELKOMNIKA (Telecommunication Computing Electronics and Control)*, vol. 19, no. 5, pp. 1735–1746, Oct. 2021, doi: 10.12928/TELKOMNIKA.v19i5.21059.

[11] A. M.-Balleste, P. P.-Martinez, and A. Solanas, “The pursuit of citizens' privacy: A privacy-aware smart city is possible,” *IEEE Communications Magazine*, vol. 51, no. 6, pp. 136–141, Jun. 2013, doi: 10.1109/MCOM.2013.6525606.

[12] A. Altaf, H. Abbas, F. Iqbal, and A. Derhab, “Trust models of internet of smart things: A survey, open issues, and future directions,” *Journal of Network and Computer Applications*, vol. 137, pp. 93–111, Jul. 2019, doi: 10.1016/j.jnca.2019.02.024.

[13] E. C. Ferrer, “The blockchain: A new framework for robotic swarm systems,” in *Advances in Intelligent Systems and Computing*, vol. 881, 2019, pp. 1037–1058.

[14] G. O. Karame, E. Androulaki, and S. Čapkun, “Double-spending fast payments in Bitcoin,” in *Proceedings of the ACM Conference on Computer and Communications Security*, 2012, pp. 906–917, doi: 10.1145/2382196.2382292.

[15] N. Z. Aitzhan and D. Svetinovic, “Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams,” *IEEE Transactions on Dependable and Secure Computing*, vol. 15, no. 5, pp. 840–852, Sep. 2018, doi: 10.1109/TDSC.2016.2616861.

[16] L. Yuan, I. Alsammak, and W. Itwee, “Research of optimized algorithm about mining frequent closed itemsets,” *International Journal of Computer Science Engineering (IJCSE)*, vol. 5, no. 4, pp. 205–211, 2016.

[17] E. Park, A. P. d. Pobil, and S. J. Kwon, “The role of internet of things (IoT) in smart cities: Technology roadmap-oriented approaches,” *Sustainability (Switzerland)*, vol. 10, no. 5, p. 1388, May 2018, doi: 10.3390/su10051388.

[18] T. Braun, B. C. M. Fung, F. Iqbal, and B. Shah, “Security and privacy challenges in smart cities,” *Sustainable Cities and Society*, vol. 39, pp. 499–507, May 2018, doi: 10.1016/j.scs.2018.02.039.

[19] M. U. Hassan, M. H. Rehmani, and J. Chen, “Privacy preservation in blockchain based IoT systems: Integration issues, prospects, challenges, and future research directions,” *Future Generation Computer Systems*, vol. 97, pp. 512–529, Aug. 2019, doi: 10.1016/j.future.2019.02.060.

[20] K. Gai, J. Guo, L. Zhu, and S. Yu, “Blockchain meets cloud computing: A survey,” *IEEE Communications Surveys and Tutorials*, vol. 22, no. 3, pp. 2009–2030, 2020, doi: 10.1109/COMST.2020.2989392.

[21] S. Aggarwal, R. Chaudhary, G. S. Aujla, N. Kumar, K. K. R. Choo, and A. Y. Zomaya, “Blockchain for smart communities: Applications, challenges and opportunities,” *Journal of Network and Computer Applications*, vol. 144, pp. 13–48, Oct. 2019, doi: 10.1016/j.jnca.2019.06.018.

[22] K. Xing, C. Hu, J. Yu, X. Cheng, and F. Zhang, “Mutual privacy preserving k-means clustering in social participatory sensing,” *IEEE Transactions on Industrial Informatics*, vol. 13, no. 4, pp. 2066–2076, Aug. 2017, doi: 10.1109/TII.2017.2695487.

[23] I. L. H. Alsammak, H. M. A. Sahib, and W. H. Itwee, “An enhanced performance of K-nearest neighbor (K-NN) classifier to meet new big data necessities*,” IOP Conference Series: Materials Science and Engineering*, vol. 928, no. 3, p. 032013, Nov. 2020, doi: 10.1088/1757-899X/928/3/032013.

[24] Y. Yang, X. Zheng, W. Guo, X. Liu, and V. Chang, “Privacy-preserving smart IoT-based healthcare big data storage and self-adaptive access control system,” *Information Sciences*, vol. 479, pp. 567–592, Apr. 2019, doi: 10.1016/j.ins.2018.02.005.

[25] I. L. H. Alsammak, “A proposed algorithm for prediction HIV by using data mining technology,” *Journal of University of Babylon for Pure and Applied Sciences*, 2019, [Online]. Available: https://www.journalofbabylon.com/index.php/JUBPAS/article/view/2486.

[26] Y. Yang, X. Zheng, X. Liu, S. Zhong, and V. Chang, “Cross-domain dynamic anonymous authenticated group key management with symptom-matching for e-health social system,” *Future Generation Computer Systems*, vol. 84, pp. 160–176, Jul. 2018, doi: 10.1016/j.future.2017.06.025.

[27] S. Q. Ren *et al*., “Secure searching on cloud storage enhanced by homomorphic indexing,” *Future Generation Computer Systems*, vol. 65, pp. 102–110, Dec. 2016, doi: 10.1016/j.future.2016.03.013.

[28] G. Sun *et al*., “Efficient location privacy algorithm for internet of things (IoT) services and applications,” *Journal of Network and Computer Applications*, vol. 89, pp. 3–13, Jul. 2017, doi: 10.1016/j.jnca.2016.10.011.

[29] F. Gao, L. Zhu, M. Shen, K. Sharif, Z. Wan, and K. Ren, “A blockchain-based privacy-preserving payment mechanism for vehicle-to-grid networks,” *IEEE Network*, vol. 32, no. 6, pp. 184–192, Nov. 2018, doi: 10.1109/MNET.2018.1700269.

[30] D. Liao, H. Li, G. Sun, M. Zhang, and V. Chang, “Location and trajectory privacy preservation in 5G-Enabled vehicle social network services,” *Journal of Network and Computer Applications*, vol. 110, pp. 108–118, May 2018, doi: 10.1016/j.jnca.2018.02.002.

[31] K. Christidis and M. Devetsikiotis, “Blockchains and smart contracts for the internet of things,” *IEEE Access*, vol. 4, pp. 2292–2303, 2016, doi: 10.1109/ACCESS.2016.2566339.

[32] P. K. D. Pramanik, G. Pareek, and A. Nayyar, “Security and privacy in remote healthcare: Issues, solutions, and standards,” in *Telemedicine Technologies: Big Data, Deep Learning, Robotics, Mobile and Remote Applications for Global Healthcare*, Elsevier, 2019, pp. 201–225.

[33] F. Alam Khan, M. Asif, A. Ahmad, M. Alharbi, and H. Aljuaid, “Blockchain technology, improvement suggestions, security challenges on smart grid and its application in healthcare for sustainable development,” *Sustainable Cities and Society*, vol. 55, p. 102018, Apr. 2020, doi: 10.1016/j.scs.2020.102018.

[34] S. E. Bibri, “The IoT for smart sustainable cities of the future: An analytical framework for sensor-based big data applications for environmental sustainability,” *Sustainable Cities and Society*, vol. 38, pp. 230–253, Apr. 2018, doi: 10.1016/j.scs.2017.12.034.

[35] J. H. Park and J. H. Park, “Blockchain security in cloud computing: Use cases, challenges, and solutions,” *Symmetry*, vol. 9, no. 8, p. 164, Aug. 2017, doi: 10.3390/sym9080164.

[36] X. Li, P. Jiang, T. Chen, X. Luo, and Q. Wen, “A survey on the security of blockchain systems,” *Future Generation Computer Systems*, vol. 107, pp. 841–853, Jun. 2020, doi: 10.1016/j.future.2017.08.020.

[37] A. Prashanth Joshi, M. Han, and Y. Wang, “A survey on security and privacy issues of blockchain technology,” *Mathematical Foundations of Computing*, vol. 1, no. 2, pp. 121–147, 2018, doi: 10.3934/mfc.2018007.

[38] Y. Liu, F. R. Yu, X. Li, H. Ji, and V. C. M. Leung, “Blockchain and machine learning for communications and networking systems,” *IEEE Communications Surveys and Tutorials*, vol. 22, no. 2, pp. 1392–1431, 2020, doi: 10.1109/COMST.2020.2975911.

[39] I. L. H. Alsammak, A. H. Mohammed, and N. S. Nasir, “E-learning and COVID-19: predicting student academic performance using data mining algorithms,” *Webology*, vol. 19, no. 1, pp. 3419–3432, Jan. 2022, doi: 10.14704/web/v19i1/web19225.

[40] W. Li, W. Meng, L.-F. Kwok, and H. H. S. IP, “Enhancing collaborative intrusion detection networks against insider attacks using supervised intrusion sensitivity-based trust management model,” *Journal of Network and Computer Applications*, vol. 77, pp. 135–145, Jan. 2017, doi: 10.1016/j.jnca.2016.09.014.

[41] W. Li, S. Tug, W. Meng, and Y. Wang, “Designing collaborative blockchained signature-based intrusion detection in IoT environments,” *Future Generation Computer Systems*, vol. 96, pp. 481–489, Jul. 2019, doi: 10.1016/j.future.2019.02.064.

[42] S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system,” *SSRN Electronic Journal*, 2020, doi: 10.2139/ssrn.3977007.

[43] G. Liang, S. R. Weller, F. Luo, J. Zhao, and Z. Y. Dong, “Distributed blockchain-based data protection framework for modern power systems against cyber attacks,” *IEEE Transactions on Smart Grid*, vol. 10, no. 3, pp. 3162–3173, May 2019, doi: 10.1109/TSG.2018.2819663.

[44] K. S. Adewole, N. B. Anuar, A. Kamsin, K. D. Varathan, and S. A. Razak, “Malicious accounts: Dark of the social networks,” *Journal of Network and Computer Applications*, vol. 79, pp. 41–67, Feb. 2017, doi: 10.1016/j.jnca.2016.11.030.

[45] M. Al-Qurishi, M. S. Hossain, M. Alrubaian, S. M. M. Rahman, and A. Alamri, “Leveraging analysis of user behavior to identify malicious activities in large-scale social networks,” *IEEE Transactions on Industrial Informatics*, vol. 14, no. 2, pp. 799–813, Feb. 2018, doi: 10.1109/TII.2017.2753202.

## BIOGRAPHIES OF AUTHORS

**Ihab L. Hussein Alsammak** He received his computer Science degree from the College of Scince, University of Kerbala, (Iraq); his MSc degree in Data Mining from the Huazhong University of Science and Technology (China); His research interests focus on control and cooperative decision-making in swarms of self-organising drones aimed at fighting fires autonomously. He is currently a PhD student at Universiti Tenaga Nasional (UNITEN). He can be contacted at email: ehablaith@gmail.com.

**Mohammed F. Alomari** He received his computer Science degree from the College of Scince, University of wasit, (Iraq); his MSc degree in Telecommunication from the Utara University Malaysia (Malaysia); His research interests focus on IoT and wireless sensor network in intelligent transportation systems. He is currently a PhD student at Universiti Tenaga Nasional (UNITEN). He can be contacted at email: mohammedict1@gmail.com.

**Intedhar Shakir Nasir** She received BSc in Statistics, Baghdad University, College of Administration and Economics, Baghdad, Iraq in 1990. Then she earned High Diploma in Computer Qualification from Iraqi Commission for Computer and Informatics-Institute of Postgraduate studies in Informatics, Baghdad, Iraq, in 2003. Later she graduated her M.Sc. in Computer Science from DR. Babasaheb Ambedkar Marthwada University-Aurangabad. Maharashtra (India), 2010.She is currently works as lecturer at the Department of Family and Community Medicine, College of Medicine, University of Kerbala. She can be contacted at email: intedhar.shakir@uokerbala.edu.iq.

**Wasan H. Itwee** She received his computer Science degree from the College of Scince, University of Kerbala, (Iraq); her MSc degree in Data Mining from the Huazhong University of Science and Technology (China); Her research interests focus on control and cooperative decision-making in swarms of self-organising drones aimed at fighting fires autonomously. She can be contacted at email: wassan_iraq@yahoo.com.