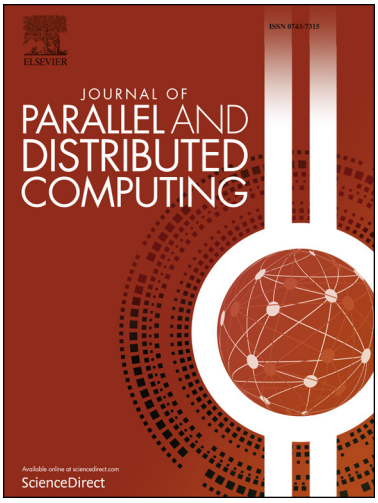
Journal Pre-proof



Cross-Domain Secure Data Sharing using Blockchain for Industrial IoT

Parminder Singh, Mehedi Masud, M. Shamim Hossain and Avinash Kaur

PII: S0743-7315(21)00112-X
DOI: https://doi.org/10.1016/j.jpdc.2021.05.007
Reference: YJPDC 4413

To appear in: *Journal of Parallel and Distributed Computing*

Received date: 1 August 2020
Revised date: 14 March 2021
Accepted date: 18 May 2021

Please cite this article as: P. Singh, M. Masud, M. Shamim Hossain et al., Cross-Domain Secure Data Sharing using Blockchain for Industrial IoT, *Journal of Parallel and Distributed Computing*, doi: https://doi.org/10.1016/j.jpdc.2021.05.007.

Highlights

- A framework for cross-domain secure data sharing in the Industrial Internet of Things.
- A system to manage false reporting and misbehaving using a penalty mechanism.
- A framework for enhancing data integrity through multi-layer signatures.

Cross-Domain Secure Data Sharing using Blockchain for Industrial IoT

Parminder Singh

School of Computer Science and Engineering, Lovely Professional University, India

Mehedi Masud

College of Computers and Information Technology, Taif University, Taif, Saudi Arabia

M Shamim Hossain*

Research Chair of Pervasive and Mobile Computing, King Saud University, Riyadh 11543, Saudi Arabia, and Department of Software Engineering, College of Computer and Information Sciences, King Saud University, Riyadh 11543, Saudi Arabia

Avinash Kaur

School of Computer Science and Engineering, Lovely Professional University, India

[a] *Taif University, KSA*
[b] *Lovely Professional University, India*

Abstract

The Industrial Internet of Things (IIoT) enhances smart manufacturing process that escalates productivity through revolutionary techniques. The manufacturing process is sophisticated and complex because of various IoT domains (e.g. industries). A final product is an outcome of the efforts of several departments from different industries. However, this raises the cross-domain communication's privacy and security issues. Cross-domain data sharing for product manufacturing is a challenging research direction. This paper proposes a centralized cloud-based cross-domain data sharing platform using multiple security gateways. The security gateways use the blockchain to store the information into the centralized cloud. Once the application reported a malicious activity,

*Corresponding author
Email addresses: parminder.16479@lpu.co.in (Parminder Singh), mmasud@tu.edu.sa (Mehedi Masud), mshossain@ksu.edu.sa (M Shamim Hossain), avinash.14557@lpu.co.in (Avinash Kaur)

the centralized cloud verifies the concern from the blockchain. Further, an action is taken against the party that performs malicious activity in the security gateways. The algorithms are designed for authentication and transaction of data. The proposed framework is able the secure data movement among different domains globally. The experiment result demonstrates that the proposed security and privacy framework helps to maintain trust among the industries that collaborate on manufacturing across the domains.

Keywords: Blockchain, Industrial Internet of Things (IIoT), Cross-domain data sharing, Smart contract, Authentication

1. Introduction

The Industrial Internet of Things (IIoT) is emerging as a vital enabling technology in recent days due to the advent of Industry 4.0 [1] and blockchain-based data aggregation [2]. IIoT provides numerous services in manufacturing leveraging the Internet besides connecting only devices. The services are generally offered to preserve privacy within a cloud-based platform [3][4]. In IIoT, inter-connectivity facilitates among devices to collaborate, which significantly increases productivity and efficiency.

IIoT technologies provide a platform to connect devices with a factory domain to facilitate tasks of automating manufacturing. This service substantially increases productivity and minimizes the cost of management. Nevertheless, it is generally challenging to possess a full-fledged product production process within an individual domain since, nowadays, the production process is becoming very sophisticated. Hence, it is a trend to distribute the complete product manufacturing process over numerous domains having a close relationship. Therefore, devices distributed across domains need to share and exchange data for collaboration for the production process using an efficient communication mechanism.

The advancement of communication technology makes tasks easy to connect devices of various domains. Still, it is not a trivial job to establish a secure communication mechanism among the devices in various domains because of

trust and other unsolved security issues. Typically, domains may not trust each other since a domain may not want to expose their sensitive data to others. For example, a factory manager may not permit its devices to be accessed by other devices in outside domains without proper authentication. This research falls within the industrial IoT domain scope that needs to enable trust for the cross-domain communication among entities leveraging recent techniques such as blockchain, machine learning, Ephemeral Elliptic Curve Diffie-Hellman (ECDHE) and Identity-based Signature (IBS), and cloud computing.

This paper proposed a framework with improved trust and accountability by addressing the challenges discussed above in a cross-domain data sharing system. Trust defines the reliability of the platform to receive the desired data. The framework applies a specific penalty to a data provider to gradually build trust in a legally registered data provider if the provider provides incorrect data and performs misconduct to resolve issues. Therefore, the platform gradually develops trustworthiness. The framework manages data requests and controls transactions independently.

A relaxed assumption is considered where a data source may not be a trusted node in the proposed system. Its activities are regulated using a penalty-applying approach for malicious activities. The target data nodes are also regulated to refrain them from doing malicious activities and harming the data source and or the system. Hence, during data sharing through transactions, both the source and target nodes must follow their corresponding areas' policy and rules. The security entryways of the system verify the authenticity and impose action accordingly. The transactions are stored in the blockchain to verify [5, 6], which mainly provides a solution for handling the challenge of anonymous malicious actions of the entities. In the blockchain, each transaction is recorded with the entry consists of the entity and the timestamp to conduct the auditing.

There is a centralized cloud in the system that acts as a bridge with the receiver of data and security gateway. Each security gateway is responsible for a particular area and connects all the data providers in that area to provide a platform for a relaxed trust environment among the data nodes. In relaxed

trust, the data provider sends data to ensure whether the provided data is right or wrong. Therefore, to support reliable data sharing in this kind of platform, we propose a mechanism to produce the malicious misbehaviour report and corresponding penalty process.

1.1. Contributions

The main contributions of this article are as follows.

1. This research designed a blockchain-based framework for cross-domain secure data sharing, transactions, and malicious behaviour reporting in industrial IoT.
2. The framework incorporated the Ephemeral Elliptic Curve Diffie-Hellman (ECDHE) and Identity-based Signature (IBS) for authentication and key agreements.
3. A penalty mechanism is proposed using smart-contracts to overcome false reporting and misbehaving situation from a data-provider using a centralized cloud.
4. Multi-layer signatures are used to strengthened data integrity. A centralized security gateway is applied as a middleware for a security check of signatures.

1.2. Article Organization

The organization of the article as follows: Section 2 discusses the related works. Section 3 presents the problem formulation, and Section 4 described the data-sharing system. Section 5 presents the performance evaluation. Finally, Section 6 defines the conclusion of the paper.

2. Related Work

With IoT's advancement, the industrial IoT (IIoT) is getting more attention in the industry and academic domain. However, privacy threats and security vulnerabilities in industrial IoT are growing due to a lack of proper security

technology. Due to the decentralized approach, collaborative and P2P-based industrial IoT is motivated to use blockchain technology for cross-domain communication and sharing information, ensuring security and vulnerabilities requirements.

Zhao et. al [7] discussed the mechanism to integrate blockchain and IIoT from the perspective of industrial requirements and proposed a blockchain-enabled IIoT framework to develop trust among the components in IIoT. The authors also developed a smart contract solution to store and process data of interaction among the IIoT model components.

Vlacheas et al. [8] proposed an intelligent Knowledge-as-a-Service (iKaaS) framework for sharing data across different clouds. The framework employs a centralized cloud that gathers data from several local cloud systems located in several countries. However, the framework does not focus on security and privacy matters concerning data exchange personal data across clouds.

Hidano et al. [9] developed a secure access gateway model that can infer the rules between two countries during personal data exchange. The mechanism takes care of privacy by controlling the application's access permissions using a flexible, controlled mechanism. The model needs a privacy certificate authority (CA) for each country. The authority acts as an administrative agency and is accountable for governing country regulations to manage personal data. For communication and interpretation of the regulation between two countries, the regulation is inferred between an application running in one country and the cloud that exists in another country using (i) privacy certificate issued by the CA where the application exists and (ii) the security policy configured by the privacy CA in the country where the local cloud exists. Unfortunately, the model lacks to support configuring access permissions for the applications that exist in the city, union, or area.

Hidano et al. [10] resolved the security problem mentioned before by proposing a hierarchical model consisting of multiple CAs. The model supports the iKaaS platform to support different regulations for personal data within the common region. Yet, the model does not support data exchange accountability

and trust among the various participants. It is very important to ensure strict security and privacy policy to maintain in trans-border data sharing systems.

Authors [11] uses IoT-sensing to share healthcare information[12, 13], among them tackling cross-boundary barrier using cloud computing. Moreover, the authors also proposed an urban healthcare big data framework to deal with healthcare service providers for sharing data over the cloud.

Hörandner et al. [14] presented a framework for sharing data in the cloud by applying proxy re-encryption and retractable signatures to overcome barriers of privacy and security. Mainly the authors developed multi-factor authentication systems to solve the existing security vulnerabilities in the cloud platforms.

Authors in [15] presented the prospects and issues to implement blockchain technology [16] in cross-border business. The research mainly focuses on exploring the application of blockchain technology in cross-border supply chain business.

Blockchains use the concept of a distributed database that records constantly increasing blocks that are secured from altering and amendment using a sequence of transactions. These transactions are verified by the miners solving critical puzzles. The accountability of the platforms is ensured by the concept of smart contract [17]. The blockchain platform's accountability is ensured by a Smart contract [18]. Smart contract-oriented services in blockchain remove the burden of a trusted third party, where each transaction stores a list of miners who are permitted to approve the transaction. In general, the possessor of the data related to the transaction decides this.

Authors in [19] proposed a framework that combines IoT platforms and blockchain with the Hyperledger Fabric framework as the blockchain back-end for secure and decentralized IoT data sharing. Blockchain is utilized for storing access control policies and making access control decisions. The framework used identity-based encryption to provide for cryptography-enforced access control.

Authors in [20] proposed a cross-domain authentication process in an IoT environment using blockchain. The process is based on the PBFT algorithm. A smart contract implements the authentication process. An encrypted key

sharing method is used to authenticate and share to ensure the security of authentication data.

Authors in [21] proposed a decentralized access control framework using Blockchain for the Internet of Things (IoT). Hierarchical based smart contracts are used to perform permission assignment and access control for cross-domain user/IoT devices. The mechanism used Proof-of-Authenticity/Integrity (PoAI) mechanism for authentication in order to search and retrieve user/IoT device platform hashes.

3. Problem Formulation

This section presents the scenario of data-sharing among various domains working in collaboration in the IIoT environment.

3.1. Application Scenarios

The advancement of sensors and actuators opens many opportunities for IIoT to connect multiple manufacturing domains. The high-level view of application scenarios is shown in Figure 1. The two business partners have operated two manufacturing units.

The production line of each factory is equipped with sensors, actuators, and other smart devices. The manufacturing of the product is being monitored at each stage through sensing devices. This data can be used further to make decisions to optimize manufacturing. The manufacturing units are shown in Figure 1 are working on the same product. Therefore, extensive communication is required between these plants. Thus, a robust authentication and data sharing mechanism is required for the secure transmission of data.

3.2. Security Threats

Single manufacturing units are more interconnected and open. This is a cost-efficient and highly productive scenario. However, when we consider multiple domains, the security and privacy issues raised that need to resolve seriously.

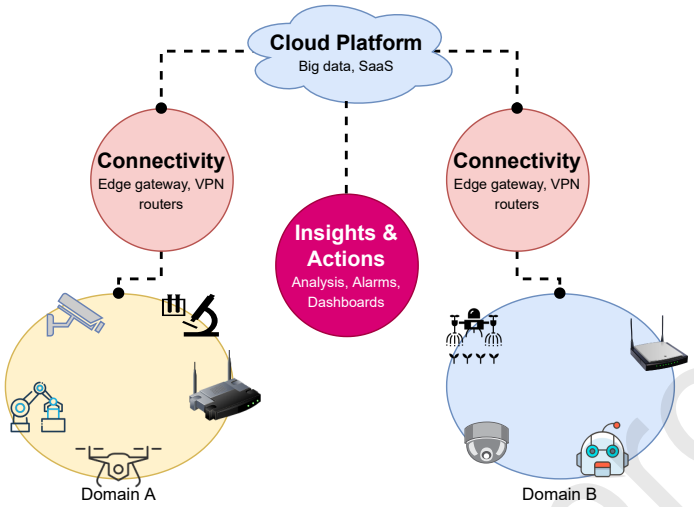


Figure 1: High-level view of application scenario

IIoT devices are prone to cyber-attacks because they are connected to the Internet. The attackers are using the eavesdropping attack to collect the sensing data to communicate over the internet [22]. In an impersonation attack, an attacker tries to impersonate as a legitimate user to cheat IIoT devices to collect the sensor's data [23][24]. Although, the man-in-middle attack forging different messages to the receiver collected from the sender. Therefore, these attacks lead to data leakage. There many other threats to the availability, integrity, privacy, and security of IIoT services [25].

In literature, the third party CA is introduced to bridge the trust of domains. However, the CA has failed throughout the world due to operational errors and compromising nature [26]. Many of CA's reap the benefit by sharing loopholes with attackers.

4. Research Methodology

In this section, we discuss the proposed framework, along with the role of each component.

The proposed framework is designed to promote the collaboration of cross-

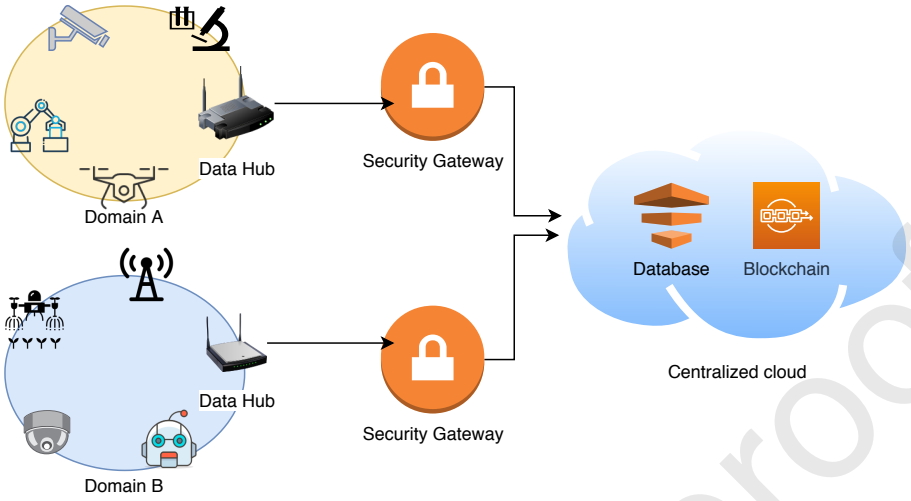


Figure 2: Cross-domain authentication and data sharing framework

domain and cross-border data sharing. The proposed framework is shown in Figure 2. On top of the proposed framework, we deployed the centralized cloud as a knowledge base to provide the data to various applications. The security gateways are applied to provide the security and privacy of a specific region. The proposed framework promotes the production process through the inter-countries manufacturing process. The proposed framework promotes the comparative study of different countries and multiple-scale analysis. As countries or state governing bodies might have different rules for sharing personal data, the security gateways applied in different regions handle this concern. The role of various components is as follows.

- Cloud: Data request is accepted through central cloud servers and performs the action accordingly. The security gateways are connected with cloud servers across the globe. Any organization can report the misbehaviour; the blockchain-inspired system deployed here verifies and punishes the false reporting or misbehaving entity.

- Security Gateway: The cloud passes the request to the security gateways, and further security gateways pass the same request to data hubs. These

gateways play a vital role to identify the misbehaving entities in the network. The cloud is further attached to the security gateways. The data exchange between the data hub and cloud performed through the security gateways. The governing rules decided by each domain are deployed in security gateways. This helps to control the personal data within and outside the countries. Data owners are usually unaware of the security concerns, so these gateways help provide privacy control.

A token-based mechanism is designed to access the data. Once the application request from the storage hub, a token is generated by the security gateway. The token has a certain expiry time, and the application can access the data any number of times till the token is not expired. The authentication mechanism and membership certificate have been verified as per the rules of organizations and countries while issuing the token to the application. The gateway is responsible for issuing the token after verification of security protocols to access the data.

- Data Hub: The various organization are deployed the smart devices equipped with IoT devices. The data collected through sensing devices moved to the cloud through data hubs. It also helps to identify the IoT device with malicious behaviour.

- Blockchain: The cloud servers deploy and maintain the blockchain. The blockchain is used to store every action as a transaction performed on data storage, update, and retrieval through security gateways. The verification of malicious activities can be performed by cross verify the blockchain transaction. The proposed technique works with a permissioned blockchain, where authorized miners verify each transaction.

  Smart contracts help to record the transactions. Even the cloud needs to verify itself before recording the transactions on the cloud servers. The Blockchain network provides the verified account to record the transaction. Once the account is verified, permission is granted to store the transaction in the block. Smart contracts also help to audit the specific transaction.

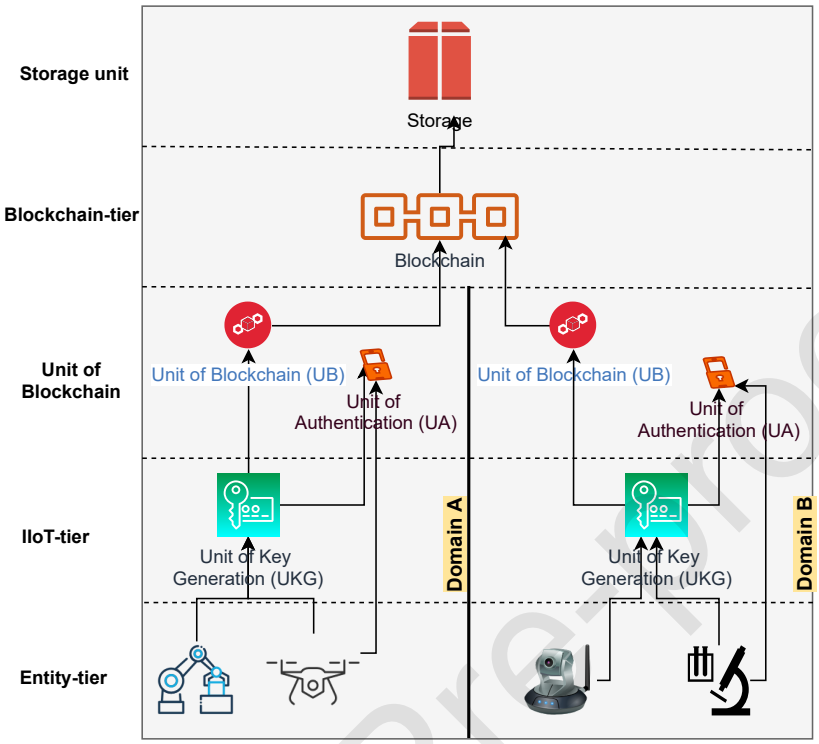


Figure 3: Multi-tier cross-domain authentication process

The transaction can be checked with hash-id. The proposed model will analyze the misbehaviour and generate the report.

- Application: The application works at the organization level to request the data from the cloud and reporting malicious behaviour.

4.1. Cross-domain Authentication

In each domain, authentication is the coordination process of three tiers. Figure 3 shows the process of cross-domain authentication process of Domain A entity T_i^A with Domain B entity T_j^B. Three domain Units of Key Generation (UKG), Unit of Authentication (UA), and Unit of Blockchain (UB) are coordinating with each other for the authentication process.

Ephemeral Elliptic Curve Diffie-Hellman (ECDHE) is employed in this paper for the establishment of the key. Whereas Identity-based Signature (IBS) is used

for the authentication mechanism. ECDHE shared the public key and keep the private key for security purposes. Private keys are very crucial for the session key and, this must not be shared on the Internet. Once the session is over, these keys are discarded. The exchange entities can further not able to use the same session to communicate and exchange the data. The main reason to adopt the ECDHE is that it is relatively fast. As compared to DHE, the ECDHE has a smaller message. Furthermore, ECDHE is known for its biodiversity. Once, the ECDHE has been deployed on the cloud servers, it works for all the versions. For example, fossilization has overcome whether someone uses IE 6 or 7.

1. IIoT-tier: The entity tier contains the IIoT devices. These devices have the facility to act as a sensor or actuator. The authentication of these devices is performed through the UKG unit. The IIoT devices put a request for the private key to the UKG unit.
2. Entity-tier: The entity-tier in the proposed system consists of UKG and IIoT devices. The private keys and requests are managed by the UKG specifically for the IIoT devices. Further, the devices received the private keys generated through the UKG unit. The authentication process is completed with the coordination of UA and UB tiers also.
3. Unit of Blockchain (UB): A centralized record needs to maintain with the consortium blockchain. It is employed to store the domain-oriented data in an encapsulated way. The separate server is used for the consortium blockchain to reduce the workload of the UKG server.
4. Unit of Authentication (UA): The authentication mechanism realized with the IBS scheme. Generally, this process has two sub-parts: Signature-Generation and verification. These processes are fine-grained and required more computation. The centralized cloud is an overall manager, and responsible for the monitoring and control. UA acts as a request representative for the generation of signature and verification processes. The workload of UKG is divided into the UB and UA.
5. Blockchain-tier: The consortium blockchain is employed in this tier. The

administrative information of various domains has been encapsulated in the blocks. This information is further used in the cross-domain authentication process and shared as per the requirement.

There may be numerous parameters and their corresponding values need to store for the domain-specific authentication process. So, the required information is stored in the blockchain.

6. Storage unit: The domain's public key list for the entities, public key of domain, names of domain are stored separately on the centralized cloud unit. The JSON file is used to store all the information. The file is hashed to protect the information, and this hash is stored in the blockchain.

A man-in-the-middle attack can affect the ECDHE when the public key received cannot be validated for authenticated sources. To avoid the man-in-the-middle attack, the public key is sent via the message integration process. The authenticated private key signed the public key.

4.2. Data-Sharing Mechanism

In this section, we discussed the proposed data sharing mechanism. The data-sharing mechanism is divided into two steps: data access and accountability. The process of data sharing is shown in Figure 4.

4.2.1. Data Access

Once the authentication is successful, the next step is to perform the access to data. Following steps are involved in data access:

1. A request is put to the centralized cloud by the user to access the specific region data.
2. The database module records the request. Further, the centralized cloud moves the request to the regional security gateway.
3. The security gateways are employed to analyze the smart-contract to decide to entertain the request or reject it.
4. A combination of data and signature is generated and sent to the security gateways.

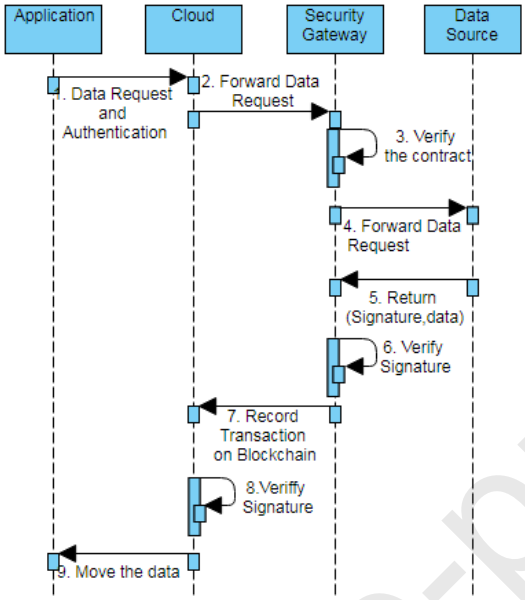


Figure 4: Data sharing process

5. Once the signature is verified the security gateway further performs its signatures and forwards the new combination to the centralized cloud.
6. The transaction details are stored in the blockchain as per Algorithm 1. Initially the status is set to false (line no. 1). The authentication status is verified from the security gateways. The user account is passed as a parameter (line no. 2). The authentication status is checked whether it is true or false. If the status is true then the metadata is stored and set the global status as true. Otherwise, discard the transaction due to unauthorization (line no. 3-8). If the status is true, then perform the authentication of the user account from the centralized cloud. If authentication status is true then send the block at blockchain and its metadata to centralized cloud storage. This function returns the Block Id after a successful record of the transaction (line no. 19). If the authentication is failed at any point it sends the null and halts the smart contract.
7. After verification is completed, the centralized cloud communicates the

requested information to the user.

4.2.2. Accountability Mechanism

Once the transaction has been stored in the blockchain. The next vital step in cross-domain authentication is to analyze the transaction for malicious behavior. The domain-level policies are stored in the native smart contract, and the global policies are stored in the imported smart contract. The accountability mechanism is consist of the following steps:

1. The application is equipped with the features to report any misbehavior. The user-owned this application can report any issue. This request further uploads to the cloud. The smart contract in the cloud is verified for the misbehavior complaint.
2. The blockchain transactions of reported users are verified and prepare an audit report.
3. The native smart contract takes consideration of reported misbehavior to properly justifying the accountability. The imported smart contract deploys in the central cloud. This further verifies the smart contract against the issue raised by the user.
4. Once the verification of native and imported smart contracts performed in the central cloud, the blockchain transaction are verified as per the proposed model.
5. The misbehavior reported by the user could be proven true or false. In case, if the issue raised is true then the domain or region has to bear liability in terms of punishment as per the smart contracts. The decided penalty has been recorded in the database as per Figure 5.
6. Furthermore, the security gateways of all the regions are also informed about the penalty of misbehaving domain/region.
7. The security gateway further analyzes the received report. If the report belongs to itself, then it sends the report to the data hub performed malicious activity.

Algorithm 1 Transaction using blockchain

Input: Metadata (MD)

Output: Block (B_{id})

Status $\leftarrow$ $false$
Auth_status $\leftarrow$ Security_Gateway(User_Account)
if Auth_status == $true$ **then**
    F_MD $\leftarrow$ MD ▷ MD is transaction metadata
    Status $\leftarrow$ $true$
else
    DISCARD ▷ Due to unauthorized blockchain, discard the transaction
end if
if Status == $true$ **then**
    Auth_status $\leftarrow$ Centralized_Cloud(User_Account)
    if Auth_status == $true$ **then**
        Centralized_BlockChain $\leftarrow$ B_{id}
        if B_{id} <> $NULL$ **then**
            Centralized_CloudStorage $\leftarrow$ Metadata
        end if
    else
        return -1
    end if
    return the Block B_{id} ▷ send the block
else
    return NULL ▷ Halt the smart contract
end if

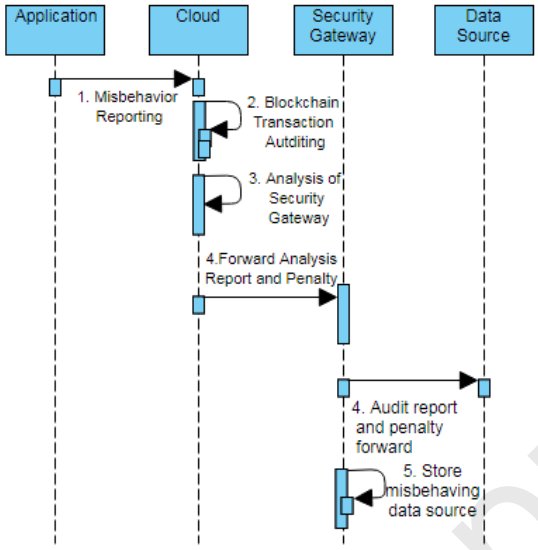


Figure 5: Accountability process using smart contracts

8. If the audit report finds that the reported misbehavior activity is false, then the penalty is imposed on the reported user. Furthermore, the request has been put on to refurbish the smart contracts as per Algorithm 2.

As per Algorithm 2, once the application is registered on the proposed system, an application id is generated represents with AP_{id}. Further, AP_{id} has to pass the test certification test to receive the certificate of membership CF, here *time* represents the time stamp. The application request region is denoted with $RG_{AP_{id}}$, whereas $RG_{Dhub_{id}}$ presents the region of data hub. The database module is the centralized cloud that received the event e_{req} for request data. If the request is similar above the threshold then give the response. In case, if request and response are below the threshold value then the penalty will be calculated and return. Otherwise, revoke the request by updating time-variant $T_{variant}$ by paying the decided amount.

Algorithm 2 Penalty scheme using smart contract

Input: e_{req}, $RG_{AP_{id}}$, $RG_{Dhub_{id}}$
Output: $Penalty$, e_{res}
$R_{AP} \leftarrow$ Verification(APP_{id})
if $R_{AP} == true$ **then**
    CF $\leftarrow$ Issue_Certificate(AP,$time$)
    if CF $==$ *reasonable* **then**
        $e_{res} \leftarrow$ Data_Request($e_{req}, RG_{AP_{id}}, RG_{Dhub_{id}}, CF_{id}$)
        if Request_Status(e_{res},$e_{req} \geq \theta$) ▷ θ defines the threshold value **then**
            return e_{res}
        else
            $P \leftarrow$ Discard_request(e_{req}) ▷ Decide the penalty on discarding request
            return Penalty P
        end if
        Update $time$ by paying desired amount $AMT(AP_{id})$
    end if
else
    return -1
end if

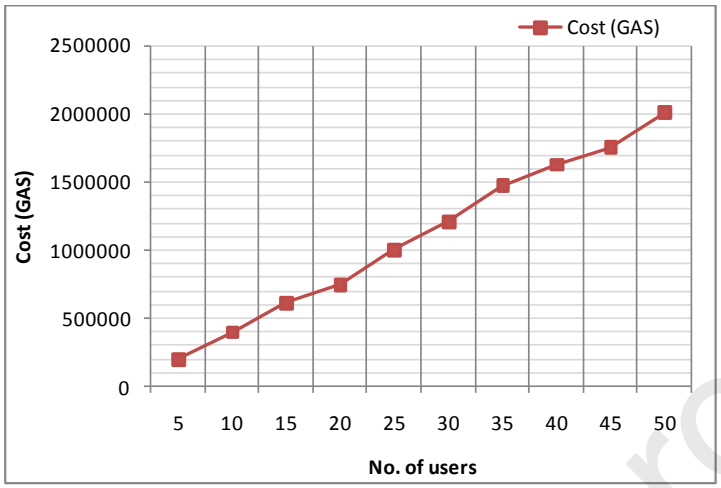


Figure 6: Transaction cost of Block-id generation

5. Performance Evaluation

The evaluation of the proposed system is performed by Java 1.8 code in Windows 7 PC with an i5 processor and 16GB RAM. The implementation of signatures is performed with ECDHE and Identity-based Signature (IBS) implements device identity.

5.1. Cost to Generate the Block-id in Blockchain

During the period of transaction, an isolated block-id generation cost is taken for checking the performance. The transaction number of users increases by one in Figure 6. As the number of users increases so does the graph. It depicts a linear relationship 0.20051 million amount of gas is taken by the transaction for 5 users, and 2.0063 million gas is taken by 50 users in the test. The amount of gas increases with the user 35. So there is an assumption that network stability impacts the transaction. The faster the network is less amount of gas is required for the transaction.

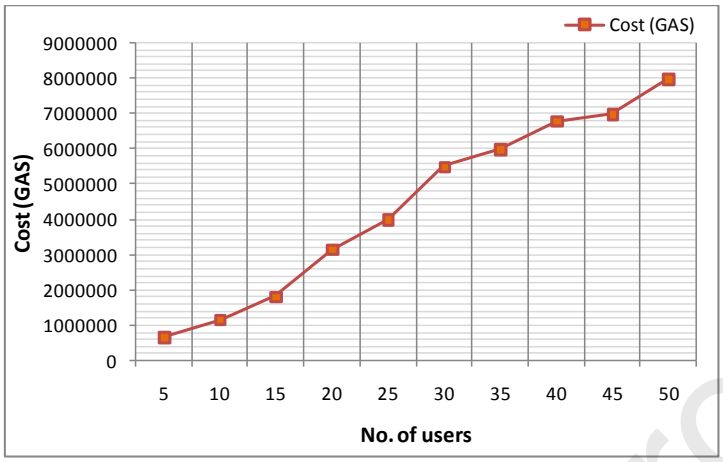


Figure 7: Transaction cost without Block-id generation

5.2. Cost of Transaction Without Generation of Block-id

In each transaction, the amount of gas is calculated for finishing the transaction of data. The amount of gas taken by the five users for transactions is 0.65 million. There is linearity in Figure 7 until user 25, after that a different form is shown. Also, an important role is played by network stability in the gas fee. The network stability is reformed after user 16 for obtaining better performance. The graph is stable between 40 and 45 users. The stability reason is related to network stability. 8 million gas cost is used by the user 50 for finishing, which is in linear stage with other users.

5.3. Total Cost of the Transaction

As depicted in Figure 8, three lines of the graph exist. In the blockchain, the total gas cost is depicted by the purple line. From the analysis, it can be seen that for users 5 in the beginning, without block-id generation, the transaction and total cost have very little difference. However, there exists a low block-id generation cost. 0.8505 million is the total transaction cost where 0.2005 million is block-id generation cost and transaction cost is 0.65 million of gas. According to the 20 users case, 3.9 million total amount of gas is required that is quite sound as compare to the generation cost of block-id. In conclusion, the cost of

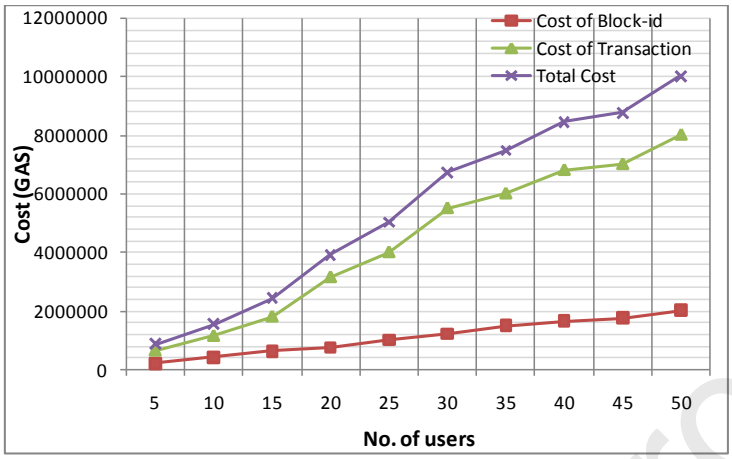


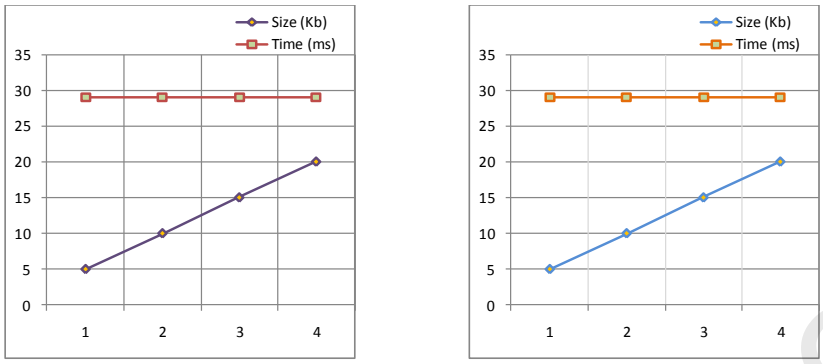
Figure 8: Comparison of various transaction cost in Blockchain

transactions elevates with the number of users. However, in the beginning, the block-id cost of generation is lower for users 5. For 50 users, when there is a transaction between a centralized cloud and a security gateway, the maximum gas amount can be 10 million gas as per the proposed system.

5.4. Signature Evaluation

In our system, ECDHE is used for the generation of signatures. Every exchange needed distinct signatures for each transaction of data for signing and verification. On data request justification, signed data is shared by data hubs with signature. The signature is verified by the security gateway and it ensures that the data is sent from authenticated or trusted data providers. Later, data is again signed by security gateway pair with a centralized cloud. Then the signature is verified by a centralized cloud and the data is sent to the requester of data.

The signature function is analyzed with input size and time. By the program, 5 to 20 kb of data is taken. In Figure 9a, the behavior of the signature id is depicted with the increase in the input size. The graph is parallel and linear to the x-axis, which refers to that with the elevating input size, a similar amount of time is needed by signature. The size of input has no effect on the time taken



(a) Time taken by Single Signature (b) Time taken by Multi-layer Signature

Figure 9: Comparison of time taken by signatures

for signing the program with ECDHE. The behavior of a multilayer signature is depicted in Figure 9b. The graph is similar to Figure 9a that refers to signing twice or multiple times the signature takes time as a single sign.

There is no effect of input size on a multilayer signature. It takes 29 ms for generating a signature in both of the cases. In conclusion, there is no effect of input size on signature generation, although the signatures are done at each layer.

5.5. Comparison with Similar Systems

The related systems are compared with our system based on different parameters as described in Table 1. A fair comparison of these techniques performed. Johnson et al. [27] proposed the Digital Signature Algorithm (DSA) based on elliptic curve analogue known as Elliptic Curve Digital Signature Algorithm (ECDSA). This technique is accepted for various standards such as ISO, ANSI, IEEE, and NIST in 1998, 1999, and 2000 respectively. The proposed technique used the latest robust techniques such as blockchain to enhance cross-domain communication. Shafagh et al. [28] used the cloud as a central unit for data management. The authors used the blockchain for data management and access controls. This technique is not suitable for cross-border data sharing. Our proposed technique has the potential to work with a multi-cloud environment

Parameter	Johnson et al. [27]	Shafagh et al. [28]	Azaria et al. [29]	Shen et al. [30]	Our Work
Blockchain	✗	✓	✓	✓	✓
Smart-contracts	✗	✗	✗	✗	✓
Multi-Cloud Ecosystem	✓	✗	✗	✓	✓
Privacy of Owner	✓	✓	✓	✓	✓
Cross domain/ border Policies	✓	✗	✗	✓	✓
Penalty Scheme	✗	✗	✗	✗	✓
Data Accountability	✗	✓	✗	✓	✓
Trusted Data Reciever/ Provider	✗	✓	✗	✓	✓
Trusted Platform	✓	✓	✓	✗	✗

Table 1: Comparison of existing related system with proposed system

which is much suitable for cross-domain and cross-border secure data sharing. Azaria et al. [29] used the blockchain to store the electronics medical records (EMRs). Data aggregation is used to fetch useful information from the EMRs. In comparison to this technique, our proposed model used the smart-contracts to ensure the authentic exchange of information. If any party responsible for the misbehavior, the penalty is imposed on that party. Shen et al. [30] have worked on secure authentication of devices for the cross-domains. The proposed authentication is robust enough for the authentication mechanism. The proposed model got a lot of inspiration from this paper. We further used the smart contracts and penalty mechanism which ensure the trustworthy participation of various users. The system carrying the feature marked with ✓, and if the feature is not available marked with ✗. The comparison shows that our proposed model has higher advantages over the existing system.

6. Conclusion

In this research, a data-sharing platform is proposed for cross-domain data utilization. The centralized cloud is leveraged by a platform that is responsible for collecting requested data from providers of data working in different regions. On a global blockchain, the transaction is to be recorded by the data provider while providing the data. In case of any kind of misbehavior in applications, the transaction can be audited by a centralized cloud. Also, the misbehaving application or data provider can be penalized using smart contracts. For the misbehavior, the data receiver or sender, or any of the participating entities can be punished. The device authentication is strengthened with Ephemeral Elliptic Curve Diffie-Hellman (ECDHE) and Identity-based Signature (IBS). Hence, this research provides an accountable cross-domain platform for data sharing where the data provider is not fully trusted while requesting access to data. The searchability is yet to be investigated on encrypted data through the platform. Our future work will be a prototyping platform introduced for data receivers, data providers for large-scale data.

Acknowledgement

The authors are grateful to the Deanship of Scientific Research at King Saud University, Riyadh, Saudi Arabia, for funding this work through the Vice Deanship of Scientific Research Chairs: Research Chair of Pervasive and Mobile Computing.

References

[1] H. Lasi, P. Fettke, H.-G. Kemper, T. Feld, M. Hoffmann, Industry 4.0, Business & information systems engineering 6 (4) (2014) 239–242.

[2] H. Lin, et al., A blockchain-based secure data aggregation strategy using 6g-enabled nib for industrial applications, IEEE Transactions on Industrial Informatics (2020) 1–1doi:10.1109/TII.2020.3035006.

[3] M. Shen, B. Ma, L. Zhu, X. Du, K. Xu, Secure phrase search for intelligent processing of encrypted data in cloud-based iot, IEEE Internet of Things Journal 6 (2) (2018) 1998–2008.

[4] M. S. Hossain, G. Muhammad, W. Abdul, B. Song, B. Gupta, Cloud-assisted secure video transmission and sharing framework for smart cities, Future Generation Computer Systems 83 (2018) 596 – 606.

[5] G. D. Hunt, L. Koved, Auditing certified blockchain checkpoints, uS Patent 10,460,289 (Oct. 29 2019).

[6] M. A. Rahman, et al., Blockchain-based mobile edge computing framework for secure therapy applications, IEEE Access 6 (2018) 72469–72478.

[7] S. Zhao, S. Li, Y. Yao, Blockchain enabled industrial internet of things technology, IEEE Transactions on Computational Social Systems 6 (6) (2019) 1442–1453.

[8] P. Vlacheas, V. Stavroulaki, A. Georgakopoulos, D. Kelaidonis, A. Biswas, K. Moessner, Y. Miyake, S. Kiyomoto, K. Yamada, K. Hashimoto, An

overview and main benefits of an intelligent knowledge-as-a-service platform, in: WWRF 34th Meeting, 2015.

[9] S. Hidano, S. Kiyomoto, Y. Murakami, P. Vlacheas, K. Moessner, Design of a security gateway for ikaas platform, in: International Conference on Cloud Computing, Springer, 2015, pp. 323–333.

[10] S. Hidano, A. Biswas, S. Kiyomoto, Hierarchical privacy cas for cross-border transfer of personal data, Research Briefs on Information & Communication Technology Evolution (ReBICTE) 2 (2) (2016) 1–12.

[11] J. J. Seddon, W. L. Currie, Cloud computing and trans-border health data: Unpacking us and eu healthcare regulation and compliance, Health policy and technology 2 (4) (2013) 229–241.

[12] S. U. Amin, et al., Cognitive smart healthcare for pathology detection and monitoring, IEEE Access 7 (2019) 10745–10753.

[13] M. S. Hossain, Cloud-supported cyber–physical localization framework for patients monitoring, IEEE Systems Journal 11 (1) (2017) 118–127.

[14] F. Hörandner, S. Krenn, A. Migliavacca, F. Thiemer, B. Zwattendorfer, Credential: a framework for privacy-preserving cloud-based data sharing, in: 2016 11th International Conference on Availability, Reliability and Security (ARES), IEEE, 2016, pp. 742–749.

[15] Y. Chang, E. Iakovou, W. Shi, Blockchain in global supply chains and cross border trade: a critical synthesis of the state-of-the-art, challenges and opportunities, International Journal of Production Research 58 (7) (2020) 2082–2099.

[16] M. A. Rahman, et al., Blockchain and iot-based cognitive edge framework for sharing economy services in a smart city, IEEE Access 7 (2019) 18611–18621.

[17] M. Yang, T. Zhu, K. Liang, W. Zhou, R. H. Deng, A blockchain-based location privacy-preserving crowdsensing system, Future Generation Computer Systems 94 (2019) 408–418.

[18] S. Dhupkar, N. Mehta, H. Singh, T. S. McGuire, Collateral management with blockchain and smart contracts apparatuses, methods and systems, uS Patent App. 16/125,608 (Jan. 3 2019).

[19] H. T. T. Truong, M. Almeida, G. Karame, C. Soriente, Towards secure and decentralized sharing of iot data, in: 2019 IEEE International Conference on Blockchain (Blockchain), 2019, pp. 176–183. doi:10.1109/Blockchain.2019.00031.

[20] D. Li, J. Yu, X. Gao, N. Al-Nabhan, Research on multidomain authentication of iot based on cross-chain technology, Security and Communication Networks 2020 (2020) 6679022. doi:10.1155/2020/6679022.
URL https://doi.org/10.1155/2020/6679022

[21] G. Ali, N. Ahmad, Y. Cao, S. Khan, H. Cruickshank, E. A. Qazi, A. Ali, xdbauth: Blockchain based cross domain authentication and authorization framework for internet of things, IEEE Access 8 (2020) 58800–58816. doi:10.1109/ACCESS.2020.2982542.

[22] X. Li, J. Xu, H.-N. Dai, Q. Zhao, C. F. Cheang, Q. Wang, On modeling eavesdropping attacks in wireless networks, Journal of Computational Science 11 (2015) 196–204.

[23] A. K. Sangaiah, et al., Energy-aware green adversary model for cyberphysical security in industrial system, IEEE Transactions on Industrial Informatics 16 (5) (2020) 3322–3329.

[24] M. S. Hossain, G. Muhammad, Cloud-assisted industrial internet of things (iiot) – enabled framework for health monitoring, Computer Networks 101 (2016) 192 – 202.

[25] M. J. Covington, R. Carskadden, Threat implications of the internet of things, in: 2013 5th International Conference on Cyber Conflict (CYCON 2013), IEEE, 2013, pp. 1–12.

[26] S. Matsumoto, R. M. Reischuk, Ikp: Turning a pki around with decentralized automated incentives, in: 2017 IEEE Symposium on Security and Privacy (SP), IEEE, 2017, pp. 410–426.

[27] D. Johnson, A. Menezes, S. Vanstone, The elliptic curve digital signature algorithm (ecdsa), International journal of information security 1 (1) (2001) 36–63.

[28] H. Shafagh, L. Burkhalter, A. Hithnawi, S. Duquennoy, Towards blockchain-based auditable storage and sharing of iot data, in: Proceedings of the 2017 on Cloud Computing Security Workshop, 2017, pp. 45–50.

[29] A. Azaria, A. Ekblaw, T. Vieira, A. Lippman, Medrec: Using blockchain for medical data access and permission management, in: 2016 2nd International Conference on Open and Big Data (OBD), IEEE, 2016, pp. 25–30.

[30] M. Shen, H. Liu, L. Zhu, K. Xu, H. Yu, X. Du, M. Guizani, Blockchain-assisted secure device authentication for cross-domain industrial iot, IEEE Journal on Selected Areas in Communications 38 (5) (2020) 942–954.

Author biographies

Dr. Parminder Singh works as an Associate Professor with the School of Computer Science and Engineering, Lovely Professional University. He received his Ph.D. from Lovely Professional University, India, in 2019. He has published more than 40 articles in refereed journals, conferences, and book chapters and holds one patent. His research interests include machine learning, deep learning, blockchain, and cloud/fog/edge computing.

Prof. Mehedi Masud is with the Department of Computer Science at Taif University, Taif, Kingdom of Saudi Arabia. He received a Ph.D. in Computer Science from the University of Ottawa, Canada. His research interests include machine learning, distributed algorithms, data security, formal methods, and health analytics. He has authored and co-authored around 70 publications, including refereed IEEE/ACM/Springer/Elsevier journals, conference papers, books, and book chapters.

M. Shamim Hossain is currently a Professor with the Department of Software Engineering, College of Computer and Information Sciences, King Saud University, Riyadh, Saudi Arabia. He is also an adjunct professor with the School of Electrical Engineering and Computer Science, University of Ottawa, ON, Canada. He received his Ph.D. in Electrical and Computer Engineering from the University of Ottawa, ON, Canada in 2009. His research interests are on cloud networking, smart environment (smart city, smart health), AI, deep learning, edge computing, Internet of Things (IoT), multimedia for health care, and multimedia big data. He has authored and coauthored more than 300 publications including refereed journals, conference papers, books, and book chapters. Recently, he co-edited a book on "Connected Health in Smart Cities", published by Springer. He has served as the cochair, general chair, workshop chair, publication chair, and TPC in several IEEE and ACM conferences. He is the chair of IEEE Special Interest Group on Artificial Intelligence (AI) for Health with IEEE ComSoc eHealth Technical Committee. Currently, he is the Co-Chair of the special session "AI- Enabled technologies for smart health monitoring", to be held with IEEE I2MTC 2021. He is also the Co-Chair of the 1st IEEE GLOBECOM 2021 Workshop on Edge-AI and IoT for Connected Health. He was the co-chair of the 3rd IEEE ICME Workshop on Multimedia Services and Tools for smart-health (MUST-SH 2020). He is a recipient of a number of awards, including the Best Conference Paper Award and the 2016 ACM Transactions on Multimedia Computing, Communications and Applica-

tions (TOMM) Nicolas D. Georganas Best Paper Award, the 2019 King Saud University Scientific Excellence Award (Research Quality), and the Research in Excellence Award from the College of Computer and Information Sciences (CCIS), King Saud University (3 times in a row). He is on the editorial board of the IEEE Transactions on Multimedia, IEEE Multimedia, IEEE Network, IEEE Wireless Communications, IEEE Access, Journal of Network and Computer Applications (Elsevier), International Journal of Multimedia Tools and Applications (Springer), Human-centric Computing and Information Sciences (Springer), Games for Health Journal, and International Journal of Information Technology, Communications and Convergence (Inderscience). He also presently serves as a lead guest editor of IEEE Network, ACM Transactions on Internet Technology, ACM Transactions on Multimedia Computing, Communications, and Applications (TOMM) and Multimedia systems Journal. Previously, he served as a guest editor of IEEE Communications Magazine, IEEE Network, IEEE Transactions on Information Technology in Biomedicine (currently JBHI), IEEE Transactions on Cloud Computing, International Journal of Multimedia Tools and Applications (Springer), Cluster Computing (Springer), Future Generation Computer Systems (Elsevier), Computers and Electrical Engineering (Elsevier), Sensors (MDPI), and International Journal of Distributed Sensor Networks. He is a senior member of both the IEEE, and ACM. He is an IEEE ComSoc Distinguished Lecturer (DL).

Dr. Avinash Kaur is an Associate Professor in the Department of Computer Science and Engineering of Lovely Professional University. She received her Ph.D. in Computer Science and Engineering from Lovely Professional University, India. Her research interests includes cloud computing, fog computing, IoT, and data mining. She has more than 30 publications in reputable journals, conference papers, and book chapters.

Author declaration

1. Conflict of Interest

Potential conflict of interest exists:

We wish to draw the attention of the Editor to the following facts, which may be considered as potential conflicts of interest, and to significant financial contributions to this work:

The nature of potential conflict of interest is described below:

☒No conflict of interest exists.

We wish to confirm that there are no known conflicts of interest associated with this publication and there has been no significant financial support for this work that could have influenced its outcome.

. Authorship

☒We confirm that the manuscript has been read and approved by all named authors.

☒We confirm that the order of authors listed in the manuscript has been approved by all named authors.

We all agree with all of the above.

Parminder Singh

Mehedi Masud

M Shamim Hossain

Avinash Kaur

Authors Statement

Parminder Singh: Conceptualization, Methodology, Formal analysis, Writing—original draft preparation. Mehedi Masud.: Conceptualization, Formal analysis, Investigation, Results interpretation, original draft preparation. Avinash Kaur: Investigation, Software, Validation, Writing—review and editing, Funding acquisition. M. Shamim Hossain: Methodology, Visualization, Results interpretation, Supervision, Writing—review and editing. All authors have read and agreed to the published version of the manuscript.