2021 IEEE 23rd Int Conf on High Performance Computing & Communications; 7th Int Conf on Data Science & Systems; 19th Int Conf on Smart City; 7th Int Conf on Dependability in Sensor, Cloud & Big Data Systems & Application

2021 IEEE 23rd Int Conf on High Performance Computing & Communications; 7th Int Conf on Data Science & Systems; 19th Int Conf on Smart City;
7th Int Conf on Dependability in Sensor, Cloud & Big Data Systems & Application (HPCC/DSS/SmartCity/DependSys) | 978-1-6654-9457-1/21/$31.00 ©2021 IEEE | DOI: 10.1109/HPCC-DSS-SMARTCITY-DEPENDSYS53884.2021.00174

Transparency-privacy Trade-off in Blockchain-Based Supply Chain in Industrial Internet of Things

Muhammad Islam
Swinburne University of Technology
Melbourne, Australia
Email: islam.m1991@gmail.com

Mubashir Husain Rehmani
Munster Technological University
Cork, Ireland
Email: mshrehmani@gmail.com

Jinjun Chen
Swinburne University of Technology
Melbourne, Australia
Email: jinjun.chen@gmail.com

***Abstract*—The integration of blockchain and Industrial Internet of Things (IIoT) results in a new model of supply chain in which blockchain provides common platform to record the data whereas IIoT facilitates connectivity of the devices. The temperproof record, traceability, and verification of each step (transparency) from manufacturing to final availability of the product is made possible through blockchain which results in a transparent supply chain. However, the high-level transparency also increases the risk of disclosure of business-related and personal information (minimum privacy) such as business secrets, intellectual property, and special incentives to adversaries. Consequently, a trade-off between transparency and privacy is established. Therefore, this work proposes a blockchain-based supply chain management in the context of IIoT known as SM-IIoT which discusses this transparency-privacy trade-off. Furthermore, the trade-off problem is turned into a Game in which the participants act as players whereas the transparency and privacy leakage are the payoff and loss, respectively. Consequently, the players compete to maximize their payoffs but minimize their individual losses due to privacy leakage. Nash equilibrium gives the solution for the Game which optimizes the payoffs of the players (e.g., maximum transparency and minimum privacy leakage). The scenario is implemented through Hyperledger fabric (HF) blockchain. Moreover, the results suggested that the proposed SM-IIoT outperforms the game theory based privacy preserving analysis approach in big data (GB-PPABD) in terms of transparency. Furthermore, the comparison with other similar works revealed that SM-IIoT owns the key attributes of the supply chain including transparency-privacy trade-off, fairness, and competitive behavior modeling of the participants.**

***Index Terms*—IIoT, Blockchain, Privacy, Transparency, Trade-off, Supply chain, Industrial data sharing, Game Theory.**

I. Introduction

Blockchain is a distributed data structure with the features of transparency, security, and immutability due to which it has been adopted in various domains including health, Internet of Things (IoT), Industrial IoT (IIoT), smart grids, smart cities, and communication networks [1], [2]. The integration of blockchain and IIoT enables a consortium of supply chain (such as manufacturer, distributor, and retailer) where the blockchain provides the common platform to record and share different operations (manufacture, transport, and distribute) across the network and IIoT provides the connectivity of various industrial devices [3]–[5]. Most importantly, blockchain facilitates tracking of the origin of source, i.e., from manufacturing to market availability for valuable products such as food items, electronic equipment, and jewelry across the supply chain through granting access to all information related to products. The food industry and agriculture are practical examples of traceable supply chains.

TABLE I: Calculation of transparency across the supply chain.

No. of items sold	Privacy	Transparency
100	Minimum	3/3 = 1
100	Medium	2/3 = 0.66
100	Maximum	1/3 = 0.33

The transparency of data is to measure the degree to which the participants can see or access the origin or sequence of operations performed on the data. However, in a semi-trusted environment of supply chain, a 100% transparency will result in disclosure of sensitive information such as business plans, intellectual property, incentives, and financial status to adversaries and business rivals which is not acceptable in practical scenarios [6]. The reason is that each participant in the supply chain has its private data (incentives, intellectual property, business secrets) which is not always shared with the rest of the network. For example, Table I shows calculation of transparency and privacy for a supply chain consisting of manufacturer, distributor and retailer. In this example, the data such as number of items sold is shared between them and transparency is taken as: $\frac{\text{No. of participants allowed to see it}}{\text{Total No. of participants}}$. For instance, 3/3 = 1 means that all operations are visible to all participants of the supply chain. As a result, the privacy is minimum.

Consequently, it is evident from Table I that a trade-off between transparency and privacy is established, i.e., when the privacy is maximum then the transparency is minimum (least of calculated values) and vice versa. As a result, increasing the visibility of operations performed by individual participants of supply chain will increase the risk of their privacy disclosure to their rivals or adversaries in the same network. Here, we discuss privacy with differential privacy technique because it is accepted as a *de facto* standard for privacy definition [7]. Applying differential privacy to data decreases the accuracy or utility of data. The privacy level is defined by a parameter called differential privacy budget ϵ. Previously, privacy-utility trade-off problem is heavily discussed in literature [8]. For example, Table II shows the privacy-utility trade-off for sales data. Here, the privacy is equivalent to the value of ϵ, whereas utility or accuracy of data is defined

978-1-6654-9457-1/21/$31.00 ©2021 IEEE
DOI 10.1109/HPCC-DSS-SmartCity-DependSys53884.2021.00174

TABLE II: Perturbation through Laplace mechanism for sales data.

No. of items sold	Privacy (equivalent to ϵ)	Utility (Accuracy)
100	0.1	89.22%
100	0.25	95.7%
100	0.5	98.32%
100	1	99%

as (1-relative error)*100. Furthermore, the relative error is defined as: $\frac{|\text{actual No. of items sold-perturbed No. of items sold}|}{\text{actual No. of items sold}}$. Table II shows that increasing the ϵ increases the accuracy or utility of the data and vice versa.

It is evident from Table II that the privacy-utility trade-off discussed in literature balances the trade-off between privacy and utility in the context of data sharing/publishing. However, the effect of transparency on privacy, i.e., transparency-privacy trade-off has not been considered so far. Moreover, Table I shows that increasing the transparency significantly impacts the privacy which raises the question that *what is the highest level of transparency which simultaneously protects the privacy of individual participants, and which is acceptable to all stakeholders in blockchain-based supply chain in the context of IIoT?* Therefore, in this work, we investigate the transparency-privacy trade-off problem to answer the above question. Hyperledger fabric blockchain is adopted to automate the transactions and contracts through its chaincode (smart contract) between supply chain participants [9].

Our contributions in this work are summarized as follows. We develop a blockchain-based supply chain model in the context of IIoT using HF blockchain which is called SM-IIoT. Differential privacy is integrated into the chaincode (smart contract) to guarantee privacy preservation. Finally, the trade-off problem is turned into a Game between semi-trusted supply chain participants. In our game model, participants of supply chain act as players whereas the transparency and privacy leakage are considered as payoff and loss, respectively. Furthermore, we evaluate the Nash equilibrium for the game which optimizes the payoff for each player. Moreover, the proposed SM-IIoT is compared with the traditional privacy-utility trade-off approach of [8], and other similar works to reveal its novelty in terms of transparency and other key attributes of the supply chain, respectively.

The rest of the paper is organized according to the following sequence: in Section II, a literature review of previous works in the related domain is presented. In Section III, we present the proposed model SM-IIoT in detail. Similarly, Section IV presents the evaluation and simulation results. Finally, Section V concludes this work.

II. Related Work

In [10], a blockchain-based food supply chain is proposed which is called TrustChain. TrustChain consists of three layers which are data, blockchain, and application. A reputation module is integrated into blockchain which evaluates scores based on the authenticity of data and entities in the blockchain. In this way, it avoids false information generation and improves trust across the supply chain. Furthermore, it was found that TrustChain achieves trustworthiness through the incorporated reputation module while keeping the throughput and latency at the same level. In [11], a new blockchain-based framework for recording of product-related data over different stages of its life cycle is proposed which is called carbon footprint chain (CFC). CFC enables tracking of carbon footprint through the fine-grained collection of product-related data at all stages. In CFC, the whole supply chain is divided into private clusters which represent individual stages of the product's life cycle. Furthermore, through evaluation, authors showed that CFC achieves high throughput, and minimum transaction processing time as compared to traditional blockchain network.

Similarly, a lightweight blockchain-enabled RFID-based authentication protocol (LBRAPS) for supply chain management has been proposed in [12]. LBRAPS is basically a blend of AI, mobile edge computing (MEC), blockchain, and RFID technologies. The proposed model consists of blockchain nodes which read RFID tags as the product moves from manufacturing to consumption stage. In this way, each stage of the product's life cycle is verified and authenticated. Moreover, it was found that the protocol resists many privacy attacks and achieves high efficiency in terms of communication and computation. In [13], a new consensus mechanism for blockchain-based food supply chain (FSC) scenario has been proposed which is known as Proof of Object (PoO). PoO suits the supply chain scenario because it is based on the proof of physical object to win the mining race rather than a computation task in PoW which is virtual. RFID tagging has been adopted to read a food package and record is flow across the supply chain. Similarly, in [14]–[16], blockchain has been adopted to increase the transparency, enable privacy preservation, and share data to incentivize each other in the context of IIoT. Apart from this, in large-scale sensor networks such as industrial environment, accurate real-time data is needed to control various processes (i.e., in manufacturing and designing) [17]. However, cloud computing has several challenging problems such as service composition [18], [19], minimum transparency, and security.

It is evident from the existing literature that the main focus of these works is on transparency, privacy, provenance, security, and verification. However, the transparency-privacy trade-off problem has not been discussed so far. Furthermore, in a consortium of supply chain participants, each participant needs different privacy level which results in a semi-trusted environment. Consequently, it is challenging to adopt the existing blockchain without solving the transparency-privacy trade-off problem.

III. Proposed Work: SM-IIoT

This Section presents the proposed work (SM-IIoT) in detail.

A. Preliminaries

1) Game Theory: Game theory provides a framework to model the interactions and decision-making process between

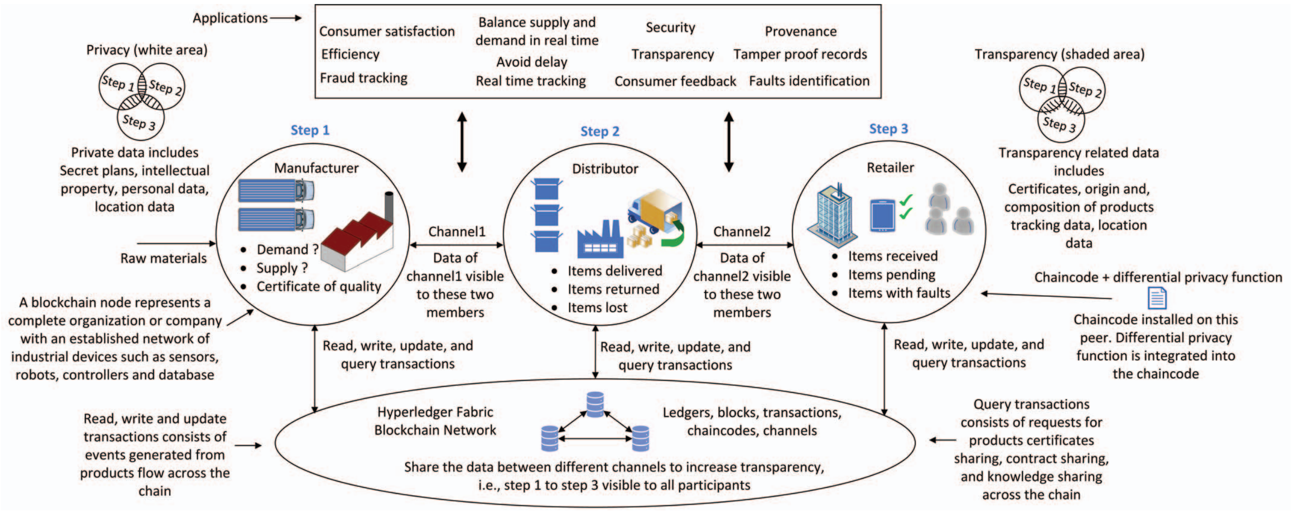

Applications
Consumer satisfaction
Efficiency
Fraud tracking
Balance supply and demand in real time
Avoid delay
Real time tracking
Security
Transparency
Consumer feedback
Provenance
Tamper proof records
Faults identification
Privacy (white area)
Step 1
Step 2
Step 3
Private data includes Secret plans, intellectual property, personal data, location data
Raw materials
A blockchain node represents a complete organization or company with an established network of industrial devices such as sensors, robots, controllers and database
Read, write and update transactions consists of events generated from products flow across the chain
Step 1
Manufacturer
Demand ?
Supply ?
Certificate of quality
Channel1
Data of channel1 visible to these two members
Step 2
Distributor
Items delivered
Items returned
Items lost
Channel2
Data of channel2 visible to these two members
Step 3
Retailer
Items received
Items pending
Items with faults
Transparency (shaded area)
Step 1
Step 2
Step 3
Transparency related data includes Certificates, origin and, composition of products tracking data, location data
Chaincode + differential privacy function
Chaincode installed on this peer. Differential privacy function is integrated into the chaincode
Read, write, update, and query transactions
Read, write, update, and query transactions
Read, write, update, and query transactions
Hyperledger Fabric Blockchain Network
Ledgers, blocks, transactions, chaincodes, channels
Share the data between different channels to increase transparency, i.e., step 1 to step 3 visible to all participants
Query transactions consists of requests for products certificates sharing, contract sharing, and knowledge sharing across the chain

Fig. 1: Demonstration of increasing the transparency through data sharing between different channels in blockchain-based supply chain (SM-IIoT).

the players involving in conflicting interests over the outcome of a decision process [20]. Furthermore, games can be divided into two broad categories known as cooperative and non-cooperative games.

In cooperative games, the players have a common goal which is achieved through utilization of individual contributions. Therefore, this type is also called coalition games or group-oriented games. In non-cooperative games, the players do not coordinate and nor have a common goal. Consequently, each player takes decision in order to increase only its own outcome. In this work, we adopt non-cooperative game model. The reason is that the players in supply chain are rational and tries to increase transparency (payoff) while decrease their individual privacy leakage (loss). As a result, non-cooperative game model is suitable to analyze the interaction between players and find the optimized decisions. Our proposed non-cooperative game model is presented in Section III-C.

2) Differential Privacy: Differential privacy has been accepted as a *de facto* standard for privacy definition [7]. In differential privacy, a calibrated noise is added to the true value of data before sharing/publishing. As a result, the data receiver extracts the required knowledge from the shared data while the true value is hidden. In this way, the privacy of the data holder is protected. According to [7], differential privacy can be defined as following:

Definition 1: *A randomized algorithm Z satisfies ϵ-differential privacy if for all datasets D_1, D_2 which differs in at most one record, and for all $O \subset Range(Z)$, the following inequality holds [7]:*

$$P[Z(D_1) \in O] \leq e^{\epsilon} \times P[(Z(D_2) \in O] \quad \text{(by [7])} \qquad (1)$$

Here, Range (Z) denotes the range of all possible outputs of algorithm Z. ϵ is known as differential privacy budget which satisfies $\epsilon > 0$. Moreover, a greater value of ϵ represents less privacy while a smaller value represents high privacy.

We adopt differential privacy model for privacy preservation because it gives a mathematical definition of privacy, and it considers an adversary with strong background information. Consequently, any dataset which satisfies differential privacy guarantees privacy preservation.

B. System model of SM-IIoT

The proposed system model consists of a supply chain scenario based on HF blockchain network as shown in Fig. 1. In the proposed scenario, a general supply chain model is considered which consists of manufacturer, distributor, and retailer. The detail of various components and data sharing is given below.

1) Composition of system model of SM-IIoT:

a) Node: Each node in the chain represents a full organization or company which has various Industrial devices equipped with sensors (e.g., RFID sensor, temperature senor, and location sensor) connected through wireless media. The node is capable of recording the data, i.e., blocks of data.

b) Channel: It represents a sub-network which limits the visibility of transactions to members of the channel [9]. Furthermore, transactions in each channel in HF are maintained in a separate ledgers which are only accessible to its members.

c) Transaction: It consists of various types of transactions in HF including financial, query, read, write, and update transactions. Furthermore, the query transaction is used to request data recorded on the ledger of a different channel.

d) Chaincode: The smart contract of HF is known as chaincode [9]. Moreover, it automates interaction between various nodes of the blockchain through the implementation of read, write, query and update operations on the blockchain ledger.

e) Differential privacy function: It consists of a function which implements differential privacy using Laplace mechanism [8]. Furthermore, the function is installed on the peer as part of the chaincode.

2) Data Sharing in SM-IIoT: In the proposed scenario, the data consists of two types which are data of the same HF channel and data from a different HF channel. To increase the transparency, the data between different channels is shared through query transactions. Moreover, we only consider sharing of statistical data such as number of products sold or received and discounts rates as private information of the node. The reason is that its disclosure to competitors results in heavy loss and significant effect on the business interests of rivals. Furthermore, it is to be noted that private information can be extended in the same fashion to include other sensitive data such as secret plans, intellectual property etc. Therefore, query transaction consists of a statistical query such as what is the total number of items sold? The node tries to protect its sensitive information while contributing to transparency of the supply chain.

To protect the sensitive information, the node uses differential privacy function of the chaincode, i.e., the query is evaluated, and a perturbed response is generated which is then returned to the requesting participant. Therefore, the overall transparency in the proposed scenario, is to increase the visibility or access of the data of the same as well as different HF channel.

C. Game Model of SM-IIoT

The participants in the supply chain shown in Fig. 1 are interested to increase the transparency of operations across the supply chain in order to satisfy consumers, improve the quality, and reduce frauds through tracking. However, the disclosure of operations by individual participants can leak sensitive information to competitors and adversaries. Consequently, each participant is rational to maximize the transparency but minimize the disclosure or leakage of its own sensitive information. Therefore, game theoretic model is suitable to analyze such kind of supply chain. We consider z such nodes or participants in the supply chain model for our analysis and develop game between two of them. The game consists of a single round (non-iterative game) in which the players constitute a competition to select strategies so that their payoffs are maximized. We first define transparancy and privacy leakage with their mathematical representations and then we define our game model. We adopt the definition of blockchain transparency from [1] and formulate its mathematical form as following:

Definition 2: *In a supply chain of z nodes, if q is the number of nodes which can see or allowed to see all the operations across the supply chain then the transparency **T** is given as following:*

$$\mathbf{T} = q/z \tag{2}$$

Here, **T** denotes the transparency of supply chain. Furthermore, for given z nodes, higher q will give more transparency and vis versa. In the considered scenario, transparency refers to the accessibility/visibility of overall supply chain operations including transactions, certificate sharing, composition of products and delivery locations etc. Furthermore, it is strongly related to channels in HF, i.e., if two participants are on the same channel then the transparency is maximum whereas participants in different channel has minimum transparency. Since, we propose two player game model (as discussed in the start of this Section), therefore, the range of **T** can be identified, i.e, if both participants are on the same channel, then both can see the supply chain operations and hence $\frac{q}{z} = 1$ otherwise, only one of them will see the operations and hence, $\frac{q}{z} = 0.5$. Consequently, the range of **T** is Range(**T**) ∈ [0.5, 1]. Therefore, 0.5 represents minimum transparency whereas 1 represents the maximum transparency.

In the proposed scenario, guarantee of privacy protection of sensitive information is achieved through differential privacy. Therefore, we adopt the definition of privacy from [21] and modify it to formulate the definition of privacy leakage of a node in supply chain as following:

Definition 3: *The differential privacy leakage of a supply chain participant can be represented as a monotonically increasing function in privacy budget ϵ. let C be real number such that $C > 0$ then the privacy leakage **P** can be denoted as following:*

$$\mathbf{P} = C\epsilon \qquad \text{(by [21])} \tag{3}$$

Here, $\epsilon > 0$, **P** denotes the privacy leakage of a supply chain participant, and C is real number which represents weight constant for privacy defined by each participant. More specifically, the data owner (a supply chain participant in our scenario) which needs strict privacy, i.e., they don't want to take risk of privacy leakage and prefer privacy protection over transparency will use comparatively high value of C. Consequently, for same value of ϵ in equation 3, the value of **P** will be comparatively high for the participant with the high value of C, i.e., the privacy leakage will be high. Therefore, the participants select the privacy weight C according to their preferences. Furthermore, the privacy leakage is maximum (**P** = 1) when the ϵ value exceeds the maximum allowed differential privacy budget ϵ_{max} for a participant, i.e., beyond that maximum value of ϵ, data is no more differentially private because the noise added is negligible. Therefore, from equation 3, $C = \frac{1}{\epsilon_{max}}$. For example, for typical large value of ϵ_{max} = 3, $C = \frac{1}{3}$. As a result, ϵ_{max} = 3 gives maximum privacy leakage. Furthermore, the privacy leakages of two players will be $C_1\epsilon_1$, and $C_2\epsilon_2$. Here, C_1 and C_2 are weight constants whereas ϵ_1 and ϵ_2 are differential privacy budgets for both players.

1) Non-Cooperative Game for SM-IIoT: In this Section, the formulation of our non-cooperative game model is presented. We describe our game model as follows:

a) Players: Two supply chain participants, i.e, distributor and retailer are the players (any two of the nodes can be selected as players) of the non-cooperative game as shown in Fig. 1. Distributor is represented as p_1 and retailer is represented as p_2.

b) Strategies: The strategies for p_1 and p_2 consist of the set of values for differential privacy budget ϵ. In the considered system model, for both p_1 and p_2, $\epsilon_{j_i} \in \{0.1, 0.5, 1\}$ whereas $j \in \{p_1, p_2\}$ and $i \in \{1, 2, 3\}$.

c) Payoffs: The payoff for each player is given as the difference of transparency **T** and privacy leakage **P**. The reason is that the transparency is considered as gain whereas the privacy leakage is the loss or cost for each player. According to *definitions* 2 and 3, the payoff $U_1(\epsilon_{1_i}, \epsilon_{2_j})$ of p_1 is given as $U_1(\epsilon_{1_i}, \epsilon_{2_j}) = \frac{q}{z} + C_2\epsilon_{2_j} - C_1\epsilon_{1_i}$. In $U_1(\epsilon_{1_i}, \epsilon_{2_j})$, the term $\frac{q}{z}$ represents the overall visibility of transactions between two channel members, term $C_2\epsilon_{2_j}$ denotes the privacy leakage of p_2 and $C_1\epsilon_{1_i}$ represents the privacy leakage (loss) for p_1. Similarly, for p_2, payoff is given as $U_2(\epsilon_{1_i}, \epsilon_{2_j}) = \frac{q}{z} + C_1\epsilon_{1_i} - C_2\epsilon_{2_j}$. Here, the terms definitions are same as for $U_1(\epsilon_{1_i}, \epsilon_{2_j})$.

TABLE III: Best response strategies of players on the same channel at equilibrium state of the game.

p_1/p_2 strategy ϵ	0.1	0.5	1
0.1	**(0.99, 1.01)**	(1.07, 0.93)	(1.17, 0.83)
0.5	(0.87, 1.13)	(0.95, 1.05)	(1.05, 0.95)
1	(0.72, 1.28)	(0.8, 1.2)	(0.9, 1.1)

TABLE IV: Best response strategies of players on different channels at equilibrium state of the game.

p_1/p_2 strategy ϵ	0.1	0.5	1
0.1	**(0.49, 0.51)**	(0.57, 0.43)	(0.67, 0.33)
0.5	(0.37, 0.63)	(0.45, 0.55)	(0.55, 0.45)
1	(0.22, 0.78)	(0.3, 0.7)	(0.4, 0.6)

2) Game Analysis and Nash Equilibrium: In the game analysis, we prove the existence of Nash equilibrium, which is the solution of the game, i.e., the Nash equilibrium consists of strategies profile having one strategy for each player of the game which gives maximum payoff for each player given that other player does not change its strategy [20]. In the proposed scenario, a Nash equilibrium of the game means that all supply chain participants are satisfied, i.e., it fulfills the needs for improved transparency and privacy protection. To prove that the proposed game has a pure strategy Nash equilibrium, the payoffs of both players need to satisfy the following two conditions [8], [20], i.e., for p_1, $\frac{\partial^2 U_1}{\partial^2 \epsilon_{1_i}} \le 0$ and $\frac{\partial^2 U_1}{\partial \epsilon_{1_i} \partial \epsilon_{2_j}} \ge 0$. Similarly, for p_2, the conditions are $\frac{\partial^2 U_2}{\partial^2 \epsilon_{2_j}} \le 0$ and $\frac{\partial^2 U_2}{\partial \epsilon_{2_j} \partial \epsilon_{1_i}} \ge 0$. We prove both conditions for p_1 as following.

$$\frac{\partial U_1}{\partial \epsilon_{1_i}} = -C_1 \quad \text{(first order partial derivative of } U_1\text{)} \tag{4}$$

$$\frac{\partial^2 U_1}{\partial^2 \epsilon_{1_i}} = 0 \quad \text{(second order partial derivative of } U_1\text{)} \tag{5}$$

Similarly, taking the partial derivative of the result in equation 4 with respect to ϵ_{2_j} yields:

$$\frac{\partial^2 U_1}{\partial \epsilon_{2_j} \partial \epsilon_{1_i}} = 0 \qquad \text{(Since, } C_1 \text{ is a constant)} \tag{6}$$

Therefore, the above result of equation 6 completes the proof of second condition for the existence of at least one pure Nash equilibrium. In the same fashion, both conditions are verified for p_2 as following.

$$\frac{\partial U_2}{\partial \epsilon_{2_j}} = -C_2 \quad \text{(first order partial derivative of } U_2\text{)} \tag{7}$$

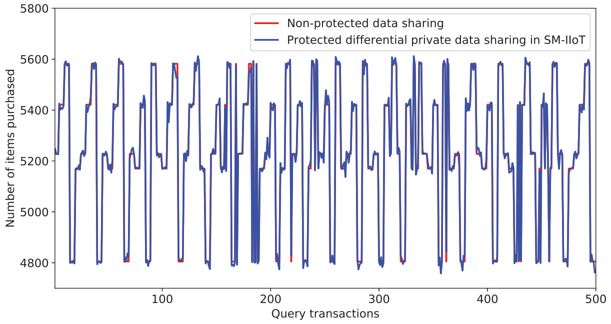


Fig. 2: Privacy preservation of shared data for best strategies $(\epsilon_1^*, \epsilon_2^*)$ = (0.1, 0.1) of the players in SM-IIoT.

$$\frac{\partial^2 U_2}{\partial^2 \epsilon_{2_j}} = 0 \quad \text{(second order partial derivative of } U_2\text{)} \tag{8}$$

Similarly, taking the partial derivative of the result in equation 7 with respect to ϵ_{1_i} yields:

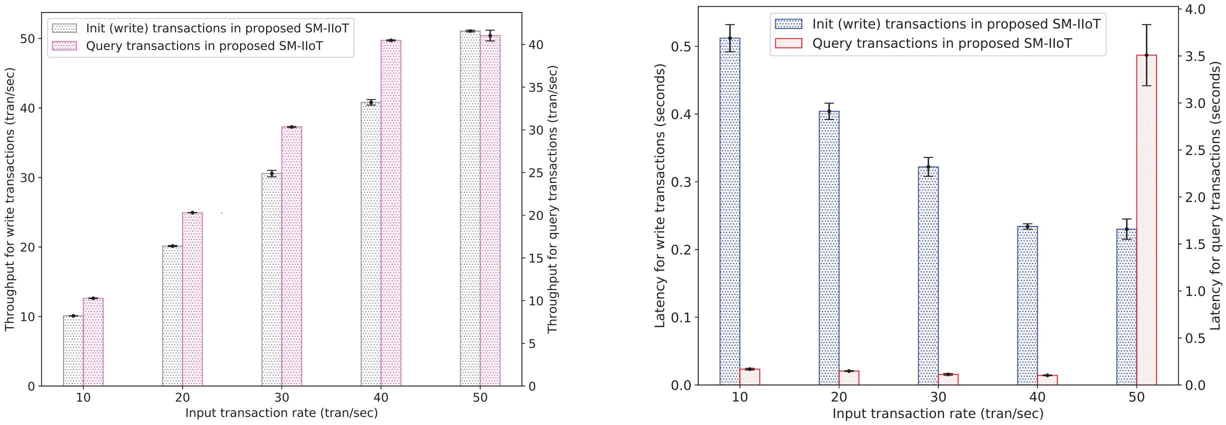
$$\frac{\partial^2 U_2}{\partial \epsilon_{1_i} \partial \epsilon_{2_j}} = 0 \qquad \text{(Since, } C_2 \text{ is a constant)} \tag{9}$$

Hence, the outcome of equation 9 completes the proof. In this way, the pure strategy profile which results in Nash equilibrium is represented as a pair $(\epsilon_{1_i}^*, \epsilon_{2_j}^*)$ where $\epsilon_{1_i}^* = BR_1(\epsilon_{2_j}^*)$ and $\epsilon_{2_j}^* = BR_2(\epsilon_{1_i}^*)$, and BR stands for *Best Response*.

IV. Performance Evaluation

The performance of proposed SM-IIoT is evaluated by simulating a blockchain-based supply chain scenario using HF blockchain. Furthermore, to witness the superiority of our proposed SM-IIoT, we compare it with the state-of-the-art works in two ways. Firstly, it is compared with the game theory based privacy preserving analysis approach in big data (GB-PPABD) of [8] to witness its superiority in terms of transparency consideration. Secondly, it is compared with the similar works of [13]–[16] to witness its superiority in terms of transparency-privacy trade-off, fairness, and competitive behavior modeling of participants.

The software setup includes Fabric software under test (SUT)



(a) Throughput

(b) Latency

Fig. 3: Throughput and Latency vs input transactions rate in SM-IIoT. The results are within 95% of confidence interval.

```
Algorithm 1: Algorithm to compute Nash equilibrium
  Input: Players $p_1$, $p_2$, privacy weight constants $C_1$, $C_2$,
    privacy loss $\mathbf{P} = C_j \epsilon_j$, strategies $\epsilon_{j_i}$, maximum privacy
    budget $\epsilon_{max}$, total nodes in the network $z$, nodes allowed
    to see the contents (data) $q$
  Output: Optimal strategies (Nash equilibrium) $(\epsilon^*_{1_i}, \epsilon^*_{2_j})$
  Initialization: Iterations = True, $\epsilon_{j_i} \in \{0.1, 0.5, 1\}$,
    $i \in \{1, 2, 3\}$, $j \in \{p_1, p_2\}$, $C_j \leftarrow \frac{1}{\epsilon_{max_j}}$, $q$, $z$
  Repeat
  Select strategies $\epsilon_{1_i} \leftarrow \{0.1, 0.5, 1\}$, $\epsilon_{2_i} \leftarrow \{0.1, 0.5, 1\}$
  Calculate the payoffs (Section III-C1) $U_1$, and $U_2$
  Populate the matrix (as given in Tables III, and IV)
  Execute row and column elimination (on the matrix)
  Until $(\epsilon^*_{1_i}, \epsilon^*_{2_j}) \leftarrow (\epsilon_{1_i}, \epsilon_{2_j})$
  Output: $(\epsilon^*_{1_i}, \epsilon^*_{2_j})$
```

with SDK version 1.4.11 and Ubuntu-18 64-bit operating system whereas Caliper version 0.4.0 is used for evaluation of SUT [22]. Similarly, the hardware setup includes Intel(R)Core (TM) i5-8250U CPU @ 1.6 GHz processor with 8 GB of installed physical memory. The differential privacy budget is taken according to $\epsilon_{j_i} \in \{0.1, 0.5, 1\}$. The solution of the game (that is Nash equilibrium) is evaluated to identify best strategies $(\epsilon^*_{1_i}, \epsilon^*_{2_j})$ for both players. Other evaluation parameters include privacy preservation, throughput and latency of transactions.

A. *Best response strategies*

The payoffs for both players are evaluated using the configured setting with weights $C_1 = 0.3$, $C_2 = 0.2$ for p_1 and p_2, respectively. The values of weights are not fixed and can be changed accordingly for any node of the network. In the evaluation, we consider different weights for players and the evaluation for equal weights are not included. Furthermore, $z = 2$, $q \in \{1, 2\}$ is configured. Here, the value of q depends on whether p_1, p_2 are on the same channel. The payoffs are calculated, and the results are inserted into a matrix. p_1 is represented as the row player whereas the p_2 is represented as the column player in the matrix. Finally, the dominant strategy row and column elimination method is used to find the $(\epsilon^*_{1_i}, \epsilon^*_{2_j})$ [20]. The results are given in Tables III and IV. The values highlighted with bold fonts (e.g., (0.99, 1.01) and (0.49, 0.51)) in Tables III and IV represent the maximum payoffs using best response strategies $(\epsilon^*_{1_i}, \epsilon^*_{2_j})$ for both players. As a result, these strategies optimize the payoffs, i.e., transparency **T** under the constraint of differential privacy for both players. Furthermore, the maximum payoffs in Table III, i.e., (0.99, 1.01) are greater than in Table IV, i.e., (0.49, 0.51) because in Table IV, the players are on different channels for which $\frac{q}{z} = 0.5$ rather than 1. The mathematical steps to execute the game are given in algorithm 1.

B. *Privacy preservation in SM-IIoT*

The comparison of protected and unprotected data sharing is evaluated by taking $\epsilon = 0.1$. The reason is that $\epsilon = 0.1$ results in high value of payoffs for both players as shown in Tables III and IV. Furthermore, a total of 500 write transactions were sent to initialize the ledger. Similarly, 500 query transactions were sent in order to share data between two blockchain nodes. The results are presented in Fig. 2. It demonstrates that the beneficial knowledge has been retained in the shared data (minor difference in actual and perturb curves) while the privacy protection equivalent to $\epsilon = 0.1$ is guaranteed in the proposed SM-IIoT. As a result, at the equilibrium state of the game, the players get maximum payoffs and achieve high transparency for minimum privacy leakage.

C. *Throughput and Latency of transactions in SM-IIoT*

The throughput and latency of transactions in the blockchain network were evaluated by varying the input transactions rate

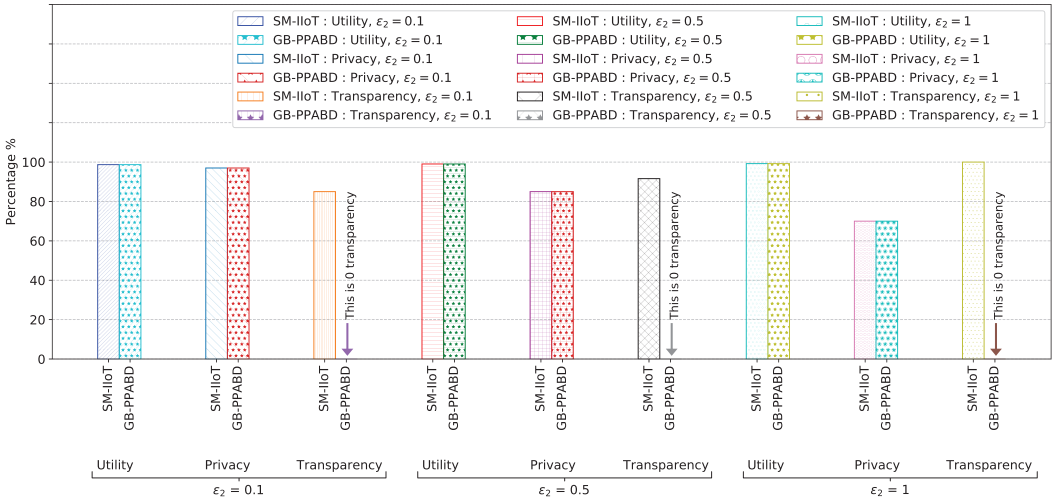


Fig. 4: Comparison of utility, privacy and transparency trade-off for SM-IIoT and GB-PPABD.

from 10 tran/sec to 50 tran/sec. Two types of transactions were considered which are write and query transactions. The results are presented in Fig. 3. The throughput is increasing for both write and query transactions with increase in the input transactions rate as shown in Fig. 3a. The reason is that the range of input transaction rate (10-50 tran/sec) lies within the processing capacity of the blockchain network (SUT) due to which more input transactions result in high throughput. Similarly, the latency of both types of transactions shows a decrease until the input transaction rate of 40 tran/sec whereas beyond this point, the latency for query transactions shows sudden increase as depicted in Fig. 3b. The reason is that the maximum capacity of transaction processing of query transactions is reached until 40 tran/sec due to which further increase causes increase in the latency.

D. *Comparison of SM-IIoT with GB-PPABD of [8]*

It is evident from the results of Tables III and IV that the players get maximum payoffs at the equilibrium state of the game. In the proposed case, the payoff is transparency on the cost of privacy leakage (i.e., as evident from the mathematical form of U_1 and U_2). Therefore, maximum payoff means high transparency on the cost of less privacy leakage (i.e., transparency-privacy trade-off). In the proposed scenario of two blockchain participants (game players p_1 and p_2), the transparency-privacy trade-off is evaluated for the proposed approach SM-IIoT and GB-PPABD of [8]. Here, transparency, privacy and utility were compared in which transparency for p_1 was calculated using $\frac{q}{z} + C_2\epsilon_{2_j}$, privacy was evaluated as (1-$C_1\epsilon_{1_i}$), and utility was evaluated as (1-average relative error in the perturbed query responses) by varying the privacy budget of p_2 according to $\epsilon_{2_j} \in \{0.1, 0.5, 1\}$. Furthermore, to represent the transparency in percentage, relative value was taken which is $\frac{\text{transparency}}{\text{maximum transparency}}$ over the range of privacy budget. The results are demonstrated in Fig. 4.

It is evident from Fig. 4 that the proposed approach has the same level of utility and privacy as compared to GB-PPABD in which the utility has increased from 98.71% for $\epsilon_2 = 0.1$ to 99.23% for $\epsilon_2 = 1$. Similarly, the privacy has decreased from 97% for $\epsilon_2 = 0.1$ to 70% for $\epsilon_2 = 1$. The reason is that both approaches use differential privacy for perturbation with Laplace mechanism. However, in terms of transparency, the proposed SM-IIoT outperforms the GB-PPABD for all values of ϵ_2 as shown in Fig. 4. The transparency for SM-IIoT is always higher than GB-PPABD, i.e., zero. The reason is that SM-IIoT considers the transparency and visibility of block contents associated with blockchain participants in the channel. Conversely, GB-PPABD did not consider the transparency and visibility of block contents in the channel. Therefore, the transparency value is zero over the range of privacy budget. Furthermore, the transparency for SM-IIoT has increased from 85% for $\epsilon_2 = 0.1$ to 100% for $\epsilon_2 = 1$ because increasing the privacy budget ϵ_2 of p_2 increases the chances of p_1 to get exact private data of p_2. It is also evident from Fig. 4 that the achieved transparency through SM-IIoT did not impact the privacy and utility of the system. i.e., the privacy and utility for SM-IIoT and GB-PPABD are on the same level.

E. *Comparison of SM-IIoT with state-of-the-art mechanisms*

In this Section, SM-IIoT is compared with four state-of-the-art mechanisms which are blockchain empowered collaborative architecture for data sharing between multiple parties (BCA-MP) [14], distributed k-means clustering (DKC)

TABLE V: Comparison of SM-IIoT with the state-of-the-art mechanisms over key attributes of supply chain.

Attributes/state-of-the-art	(BCA-MP) [14]	DKC [15]	BC-RFID [13]	DRL [16]	SM-IIoT (our approach)
Transparency-privacy trade-off	×	×	×	×	✓
Optimal strategy selection	×	×	×	×	✓
Competitive behavior modeling	✓	✓	✓	✓	✓
Private data sharing	✓	✓	×	✓	✓
Accuracy or utility of data	✓	✓	×	×	✓
Fairness	×	×	×	✓	✓

[15], blockchain-based RFID (BC-RFID) [13], and Ethereum blockchain and deep reinforcement learning (DRL) [16]. All these mechanisms have adopted blockchain to enable a smart and secure supply chain model in the context of IIoT. Furthermore, the comparison is performed in terms of six key attributes of the supply chain network which are i) transparency-privacy trade-off ii) optimal strategy selection ii) competitive behavior modeling, iv) private data sharing, v) accuracy or utility of data, and vi) fairness.

The comparison over six key attributes is summarized in Table V. It is evident from the results that the proposed SM-IIoT outperforms other state-of-the-art mechanisms. The reason is that SM-IIoT owns all the required key attributes of the supply chain network as compared to others. None of the previous mechanisms possesses all the key attributes of the supply chain network which witnesses the superiority of the proposed mechanism SM-IIoT.

V. Conclusion

In this work, we presented a game theoretic approach to solve the transparency-privacy trade-off problem in blockchain-based supply chain in the context of IIoT which is called SM-IIoT. First, a blockchain-based (HF) supply chain scenario is presented and then the trade-off problem is turned into a non-cooperative game. The players are considered as rational in achieving transparency across the supply chain at the cost of their privacy leakage. Furthermore, it was found that a pure Nash equilibrium exists in the game which gives the solution by identifying the maximum payoffs of the players. The proposed SM-IIoT outperforms the GB-PPABD approach by considering the transparency along with privacy and utility of data. Moreover, the comparison with other similar works revealed that the proposed SM-IIoT owns all the key attributes of the supply chain.

References

[1] M. S. Ali, M. Vecchio, M. Pincheira, K. Dolui, F. Antonelli, and M. H. Rehmani, "Applications of blockchains in the internet of things: A comprehensive survey," *IEEE Communications Surveys and Tutorials*, vol. 21, no. 2, pp. 1676–1717, 2019.

[2] M. H. Rehmani, *Blockchain Systems and Communication Networks: From Concepts to Implementation*, 1st ed., ser. Textbooks in Telecommunication Engineering. Springer Nature Switzerland AG, Jul. 2021.

[3] S. E. Chang and Y. Chen, "When blockchain meets supply chain: A systematic literature review on current development and potential applications," *IEEE Access*, vol. 8, pp. 62 478–62 494, 2020.

[4] V. Hassija, V. Chamola, V. Gupta, S. Jain, and N. Guizani, "A survey on supply chain security: Application areas, security threats, and solution architectures," *IEEE Internet of Things Journal*, vol. 8, no. 8, pp. 6222–6246, 2021.

[5] W. Lin, X. Huang, H. Fang, V. Wang, Y. Hua, J. Wang, H. Yin, D. Yi, and L. Yau, "Blockchain technology in current agricultural systems: From techniques to applications," *IEEE Access*, vol. 8, pp. 143 920–143 937, 2020.

[6] N. Kshetri, "Cryptocurrencies: Transparency versus privacy [cybertrust]," *Computer*, vol. 51, no. 11, pp. 99–111, 2018.

[7] C. Dwork, "Differential privacy," in *Automata, Languages and Programming*, M. Bugliesi, B. Preneel, V. Sassone, and I. Wegener, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2006, pp. 1–12.

[8] X. Wu, T. Wu, M. Khan, Q. Ni, and W. Dou, "Game theory based correlated privacy preserving analysis in big data," *IEEE Transactions on Big Data*, pp. 1–1, 2017.

[9] "Hyperledger-fabricdocs documentation," https://hyperledger-fabric.readthedocs.io/en/release-2.2/, accessed: 2021-06-05.

[10] S. Malik, V. Dedeoglu, S. S. Kanhere, and R. Jurdak, "Trustchain: Trust management in blockchain and iot supported supply chains," in *IEEE International Conference on Blockchain (Blockchain)*. IEEE, 2019, pp. 184–193.

[11] D. Shakhbulatov, A. Arora, Z. Dong, and R. Rojas-Cessa, "Blockchain implementation for analysis of carbon footprint across food supply chain," in *IEEE International Conference on Blockchain (Blockchain)*, 2019, pp. 546–551.

[12] S. Jangirala, A. K. Das, and A. V. Vasilakos, "Designing secure lightweight blockchain-enabled rfid-based authentication protocol for supply chains in 5g mobile edge computing environment," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 11, pp. 7081–7093, 2020.

[13] S. Mondal, K. P. Wijewardena, S. Karuppuswami, N. Kriti, D. Kumar, and P. Chahal, "Blockchain inspired rfid-based information architecture for food supply chain," *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 5803–5813, 2019.

[14] Y. Lu, X. Huang, Y. Dai, S. Maharjan, and Y. Zhang, "Blockchain and federated learning for privacy-preserved data sharing in industrial iot," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 6, pp. 4177–4186, 2019.

[15] B. Jia, X. Zhang, J. Liu, Y. Zhang, K. Huang, and Y. Liang, "Blockchain-enabled federated learning data protection aggregation scheme with differential privacy and homomorphic encryption in iiot," *IEEE Transactions on Industrial Informatics*, 2021.

[16] C. H. Liu, Q. Lin, and S. Wen, "Blockchain-enabled data collection and sharing for industrial iot with deep reinforcement learning," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 6, pp. 3516–3526, 2018.

[17] D. Puthal, S. Nepal, R. Ranjan, and J. Chen, "Dlsef: A dynamic key-length-based efficient real-time security verification model for big data stream," *ACM Transactions on Embedded Computing Systems (TECS) 16 (2), Article 51*, 2017.

[18] L. Qi, W. Dou, and J. Chen, "Weighted principal component analysis-based service selection method for multimedia services in cloud," *Computing, 98: 195-214*, 2016.

[19] L. Qi, W. Dou, X. Zhang, and J. Chen, "A qos-aware composition method supporting cross-platform service invocation in cloud environment," *Journal of Computer and System Sciences, 78(5): 1316-1329*, 2012.

[20] Z. Han, D. Niyato, W. Saad, T. Basar, and A. Hjorungnes, *Game Theory in Wireless and Communication Networks: Theory, Models, and Applications*. Cambridge University Press, 2011.

[21] B. Pejo, Q. Tang, and G. Biczok, "Together or alone: The price of privacy in collaborative learning," *Proceedings on Privacy Enhancing Technologies*, vol. 2019, no. 2, pp. 47–65, 2019.

[22] "Hyperledger caliper," https://www.hyperledger.org/use/caliper, accessed on: 2021-06-17.