Scalable and Secure Gradient Smart Dempster Shafer Reputation for Development of Smart Cities

Senthilselvi Ayothi
SRMIST: SRM Institute of Science and Technology
Shiny Duela Johnson
SRMIST: SRM Institute of Science and Technology
Ramesh Sekaran
Velagapudi Ramakrishna Siddhartha Engineering College
Senthil Pandi Sankareshwaran
Mohamed Sathak Engineering College
Manikandan Ramachandran
Sastra Deemed University
Vidhyacharan Bhaskar (meetvidhyacharan@yahoo.com)
San Francisco State University https://orcid.org/0000-0003-3820-2081

Research Article

Keywords: Blockchain, Gradient, Smart Load Balancer, Dempster Shafer Reputation

Posted Date: April 15th, 2021

DOI: https://doi.org/10.21203/rs.3.rs-397726/v1

SCALABLE AND SECURE GRADIENT SMART DEMPSTER SHAFER REPUTATION FOR DEVELOPMENT OF SMART CITIES

Senthilselvi Ayothi
Department of Computer Science and Engineering,
SRM Institute of Science and Technology Ramapuram Campus,
Chennai, India.
Email: mailmeselvi@yahoo.co.in

Shiny Duela Johnson
Department of Computer Science and Engineering,
SRM Institute of Science and Technology Ramapuram Campus,
Chennai, India.
Email: shiny.duela@gmail.com

Ramesh Sekaran
Department of Information Technology,
Velagapudi Ramakrishna Siddhartha Engineering College,
Vijayawada, Andhra Pradesh, India -520007
Email:sramsaran1989@gmail.com

Senthil Pandi Sankareshwaran
Department of Computer Science and Engineering,
Mohamed Sathak A. J. College of Engineering,
Chennai, INDIA.
E-mail: mailtosenthil.ks@gmail.com

Manikandan Ramachandran
School of Computing,
SASTRA Deemed University,
Tamil Nadu, India.
Email:srmanimt75@gmail.com

Vidhyacharan Bhaskar
Dept. of Electrical and Computer Engineering,
San Francisco State University,
San Francisco, CA 94132, USA.
Email:vcharan@gmail.com

Abstract

Over the last decade, blockchain has been considered an encouraging solution to secure distributed ledgers. Moreover, with the introduction of a pseudonymous payment method without a centralized database or authoritative person, blockchain has also evolved as the future generation for online payment system. However, with the eruption of a large scale database, scalability has also become a demanding issue. In addition to the obstacle mentioned above, challenges like security and scalability stop accelerated adjustments for the development of smart cities. Without directing this essential scalability and privacy issue, such an encouraging method may not help develop smart cities. This paper bestows a measure to analyze both scalability and security aspects of existing blockchain methods with applications of smart city networks. The proposed method is known as Gradient Smart Load Balancer and Blockchain Dempster Shafer Reputation (GSLB-BDSR).

Gradient Smart Load Balancer is designed so that even though with the increase in the number of participating sensors, the load is said to balance by applying gradient function, therefore ensuring scalability. Next, to cover the security aspect, with the aid of scalable blocks in the blockchain network, a Blockchain Dempster Shafer Reputation model is proposed. Evaluation outcomes of proposed security solutions outperform conventional solutions.

Keywords: Blockchain, Gradient, Smart Load Balancer, Dempster Shafer Reputation.

1. Introduction

Tasks and smart home characters are continually progressing due to contemporary Information and Communication Technology (ICT) and the Internet of Things (IoT). With the constant growth globally and with the anticipated overall population exponentially increasing, smart cities have a tendency. According to the home's network arrangement, users explore numerous keep an eye on and manage themselves based on the user settings. However, this shift has generated a smart home circumstance. The formation creates significant security susceptibilities, as several devices in smart homes include centralized networks.

In [1], a Trustworthy Privacy-Preserving Secured Framework (TP2SF) was designed. TP2SF framework consisted of three modules. They were the trustworthiness module, two-level

privacy module, and intrusion detection module. With these three structure module, accuracy, detection rate and precision were found to be improved significantly.

But, few challenges are identified with enhanced IoT nodes, time is taken in file uploading, and block mining enhances. In the future, we improve this work by various load balancing criteria to enhance network performance. Gradient Smart Load Balancer model is designed to aid gradient function to ascertain load condition to address issues in this work. It organizes block gradient surface separately in two different layers. Therefore it ensures scalability via throughput and latency time even with the increase in participating IoT devices.

The contribution of gateways in smart homes is outstanding, but its centralized organization dispenses numerous security susceptibilities. A blockchain-based smart home gateway network was proposed in [2] via three layers to address these security susceptibilities, comprising of device, gateway, and cloud layers. To start with, initially, the blockchain framework was utilized in the gateway layer. The security response time and accuracy were found to be improved. Despite improvement observed inaccuracy, additional computational complexity was incurred due to the increasing number of IoT devices, therefore compromising security. In our work, a Blockchain Dempster Shafer Reputation model is proposed to address this issue with the aid of trust and reputation measured via the Dempster Shafer proposition, ensuring security via accuracy and precision.

The inspiration for work is to resolve the scalability and security of transactions in implementing blockchain computing-based solutions in the smart city. Blockchain with cloud computing environment is the next evolution in the smart city environment, and several countries identify services beyond existing scalability and security-based solutions. Smart cities generate numerous IoT data streams that assist in transforming prevailing standard computing-based results in significant results. Hence, a novel method for smart city permits numerous and frequent streams of human and environment collective contextual data to benefit scalable and secured computing-based applications. Contribution of work enumerated as:

- This article offers related work performed to indicate requisite foundations of IoT, blockchain and smart city architecture in circumstances of IoT.

- GSLB-BDSR method shows various domains of smart city network, namely IoT Fridge activity, IoT Garage Door activity, IoT GPS tracker activity, IoT Modbus activity, IoT Motion Light activity, IoT Thermostat activity and IoT Weather activity to construct scalable and secured computing-based applications.

- Technologies that make it possible for the GSLB-BDSR method to work in a smart city.

- The opportunities and challenges which arise in executing the GSLB-BDSR method. We describe the need for scalability and security to deploy the smart city in a blockchain network, the concerns of precision, accuracy, throughput and latency time in addressing scalability and security concerns.

The residual structure of the article is ordered as below. Related works of blockchain-based security and scalability method for smart cities are offered in Section 2. GSLB-BDSRmethod for the deployment of smart cities in IoT is described in Section 3. Section 4 estimates throughput, accuracy precision, and latency time and scrutinizes the recital parameters of the GSLB-BDSR method with a detailed experimental setting for fair comparison among GSLB-BDSR and state-of-the-art methods. Lastly, Section 5 concludes the work.

2. Related Works

A comprehensive and systematic review in distributing loads among different nodes was proposed in [3]. The insurgence of the IoT is metamorphosing several notions, therefore making them smart. It has transfigured numerous areas of real-life—critical notions of this kind of revolution are Smart City. Though several cities are found to be transformed digitally, still there are found to be several hurdles making the system a more cumbersome process. In [4], areas, where blockchain is utilized are highlighted with the inclusion and advantages of utilizing blockchain in a smart city.

A blockchain-based smart home gateway network was proposed in [5] with the aid of the blockchain method provided measures for potential attacks on the gateway of smart homes. In

addition to protecting transparency and ensuring security for each smart sensor activity, a novel secure wireless mechanism utilizing Blockchain technology was proposed [6]. A review of security and privacy concerning the development of the smart city was investigated in [7].

In [8], a smart city network architecture using the cognitive model, ensuring scalability and flexibility were designed.

Present-day evolutions in IoT has validated gathering, processing and different forms of data analysis with data about personal to create necessary knowledge, making more productive services [9] for stakeholders. However, additional security and privacy issue occur due to the tremendous scale of IoT networks. In [10], a novel privacy preservation blockchain called TrustChain eliminating the delay and ensuring privacy was provided. Yet another study on the convergence of blockchain and Artificial Intelligence was proposed in [11].

A blockchain-based security solution was introduced in [12] for Industry 4.0-based applications. A comprehensive review of blockchain involving industrial aspects was made in [13]. Another experimental study involving the impact of blockchain in the smart city was proposed in [14]. A conceptual framework that includes three dimensions, namely, human, technology and organization, was presented in [15].

Next-generation smart cities are countenance of the concurrence of these developments. An enormous amount of data is produced by the mass crowd and IoT devices daily. These data have to be processed and acknowledged securely and cognitively. In [16], a blockchain-based infrastructure was designed using artificial intelligence, therefore supporting secured smart city services. Another fine-grained access control mechanism for smart healthcare using hash calculation was proposed in [17], therefore contributing to security.

A privacy-preserving strategy via Healthchain with Blockchain technology ensured security, privacy, scalability and integrity concerning smart healthcare data was discussed in [18]. Concepts of blockchain, smart city and file system utilized for smart cities were investigated [19]. Yet another blockchain-based loan system push-pulls mooring effects was proposed in [20].

So far, researchers estimated numerous use cases of blockchain. But, small-scale research is performed on the blockchain concept in smart cities. Several authors have simulated their graphs in esteem to scrutinize sensitivity, specificity structure. This work aims to present a smart city environment with blockchain and calculate graphs on various parameters in security and scalability via blockchain.

3. Gradient Smart Load Balancer and Blockchain Dempster Shafer Reputation

Blockchain is a distributed network, shares and stores data between sensors in IoT devices participating in the communications. As far IoT-driven smart cities are concerned, data created by sensors in IoT devices are stored in a distributed blockchain ledger. With this, data centralization and reliability is said to be ensured. However, with the increase in participating IoT nodes, both security and scalability remain a significant factor to be analyzed. Scalability is influenced by numerous factors, like, throughput (i.e., maximum throughput or the maximum rate of how many transactions can be confirmed by the network), latency time (i.e., how quickly transactions are confirmed).

The main contribution of this work is concentrating on how different scalability influence the security of proof-of-work blockchain and what improvements in regards to an increased number of transactions per second and latency they bring. In this work, a method called GSLB-BDSR for smart cities is proposed that provides security and scalability using blockchain for the development of smart cities. Here, only after the validation of each transaction between sensors in IoT devices execution is performed, hence contributing to both security and scalability to a greater extent. A blockchain network model is designed, followed by which the scalability and security models are elaborated in detail.

3.1 Network model

Blockchain applied for smart cities development is a critical part of data transmission authentication necessitating confidentiality among devices and sensors. Smart Cities possess a centralized network form; it has been applied in recent years as centralized to the distributed

network via utilizing blockchain at the cloud layer. Smart city gateway presented based on designed blockchain with three layers. It consists of a device layer, gateway layer and cloud layer [2]. Figure 1 given below shows the network model used in our work.

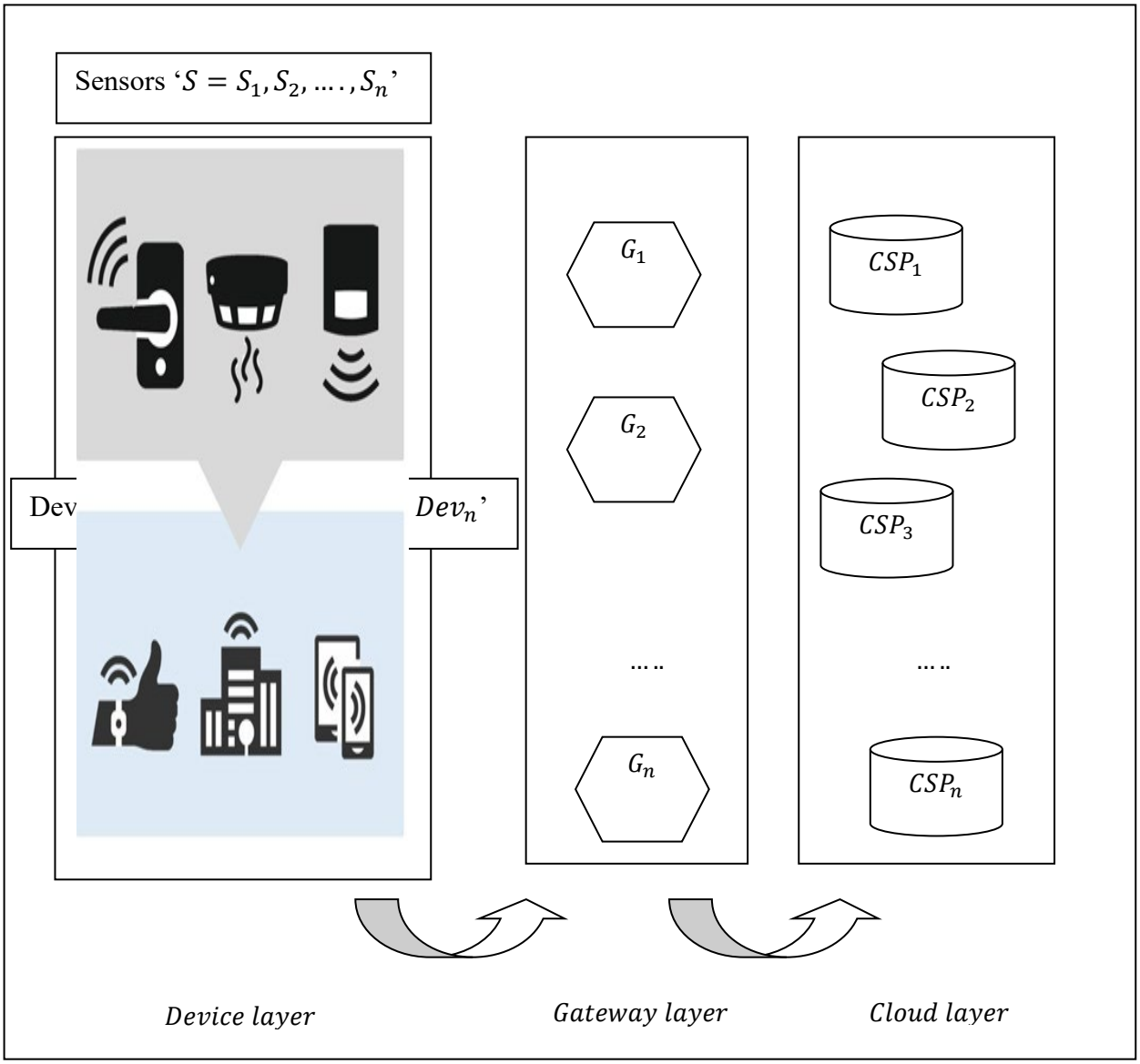

Fig. 1 Overview of the network model

As shown in the above figure, the first layer, also referred to as a device layer '$DLayer$' comprises sensors '$S = S_1, S_2, \ldots, S_n$' and devices '$Dev = Dev_1, Dev_2, \ldots, Dev_n$' and monitor data '$D = D_1, D_2, \ldots, D_n$' in a smart city environment via numerous heterogeneous IoTs configured in a smart city. It is mathematically stated as given below.

$$DLayer = \begin{matrix} & Dev_1 & Dev_2 & \ldots & Dev_n \\ S_1 \\ S_2 \\ \ldots \\ S_n \end{matrix} \begin{bmatrix} D_{11} & D_{12} & \ldots & D_{1n} \\ D_{21} & D_{22} & \ldots & D_{2n} \\ \ldots & \ldots & \ldots & \ldots \\ D_{n1} & D_{n2} & \ldots & D_{nn} \end{bmatrix} \quad (1)$$

The second layer utilized in our work refers to the gateway layer '$GLayer$' that stores data. '$D_{11}, \ldots . D_{1n,} D_{21}, \ldots . . D_{2n}, D_{n1}, \ldots, D_{nn}$' (i.e., IoT Fridge, IoT Garage, IoT GPS Tracker, IoT Modbus, IoT Motion Light, IoT Thermostat, IoT Weather) created by Device Layer '$DLayer$' and offers to users as required. It is mathematically expressed as given below.

$$GLayer = \sum_{i=1,\ldots m; j=1,\ldots n} D_{ij}(IoT_f), D_{ij}(IoT_G), D_{ij}(IoT_{GPS}), D_{ij}(IoT_{MBus}), D_{ij}(IoT_{MLight}), D_{ij}(IoT_T), D_{ij}(IoT_W) \quad (2)$$

Finally, the cloud layer registers ID 'ID' for gateway '$GLayer$' and data processed by every gateway '$DLayer$' in the corresponding blockchain and formulated as given below.

$$CLayer = ID(GLayer) \quad (3)$$

3.2 Gradient Smart Load Balancer model

With enhanced IoT nodes for the development of smart cities, the time consumed in block mining moderately rises, compromising scalability. Gradient Smart Load Balancer (GSLB) is designed which enhance the performance of blockchain network to address this issue. Figure 2 shows the Proximity Administration and Block Gradient Surface block diagram used in Gradient Smart Load Balancer.

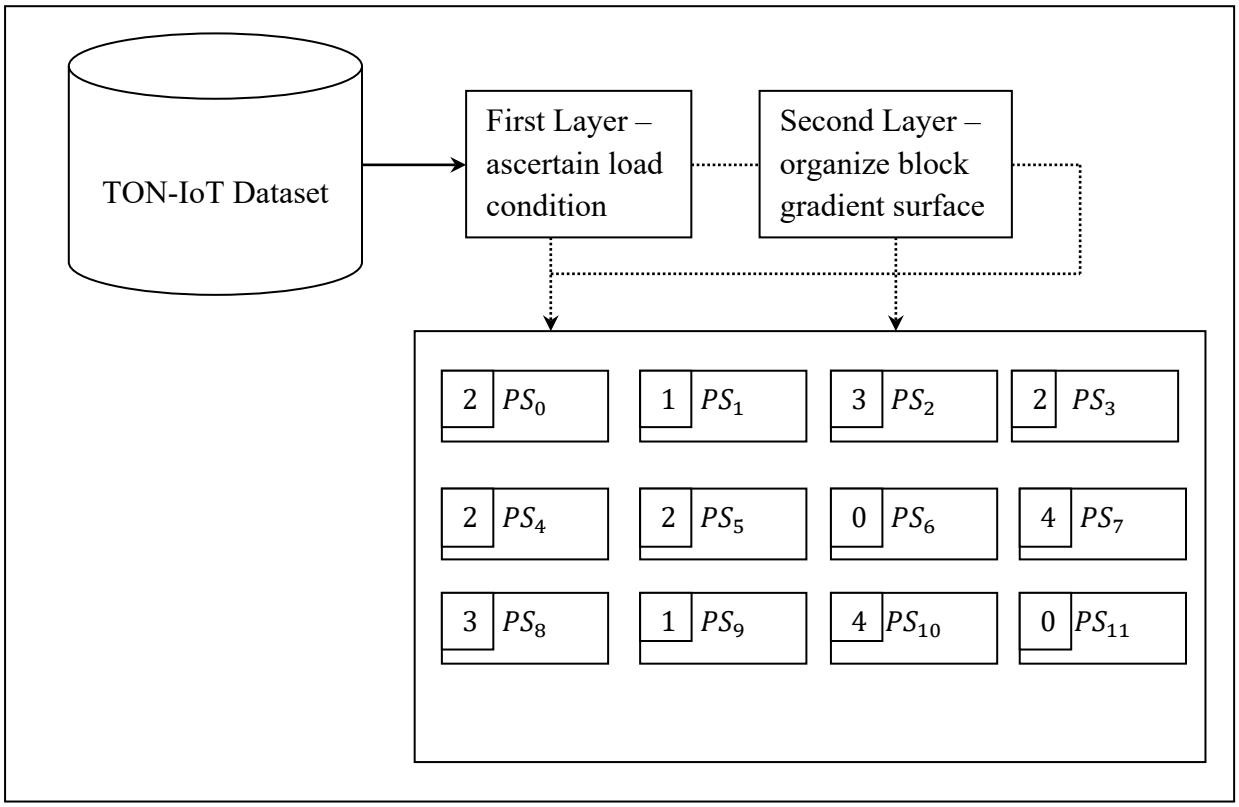

Fig. 2 Block diagram of Proximity Administration and Block Gradient Surface

As an example, the figure depicts a Proximity Administration and Block Gradient Surface system with a 4 x 3 rectangular configuration and assumes that sensors 'S_6' and 'S_{11}' are lightly loaded. As shown in the above figure, the GSLB uses a two-layered load balancing algorithm. The first layer let each block ascertain its loading condition. The time differing load state of a block may be light, average, or dense. Hence, if a block is light, more load is said to be given to the block in the blockchain network, on the other hand, if a block is dense, then some of the load has to be freed, or else, the blocks in the blockchain network is said to be average and left as it is.

The gradient blockchain surface 'GBS' of a blockchain network is the group of the closeness of all sensors represented in the form of blocks in the blockchain network, represented as '$GBS = WB_1, WB_2, \ldots, WB_n$', the workload of all the consecutive blocks. The distance 'Dis' between two sensors in the form of blocks 'S_i' and 'S' of a blockchain network is the distance of the shortest trajectory between the path. 'S_i' and 'S_j'. The breadth of a blockchain network 'BN'

is the most considerable distance between any two blocks of 'N', and this is mathematically expressed as given below.

$$Breadth(N) = \max\left\{Dis_{S_i,S_j}, forallS_i, S_j inN\right\} \quad (4)$$

The gate of a sensor in the form of a block. 'S_i' then represents a binary function. 'G_i'. Here, the gate is open if the block in the blockchain network is lightly loaded, and on the other hand, it is closed. It is defined as given below.

$$G_i = 0, ifGateS_i isopen \quad (5)$$

$$G_i = WB_{max}, ifGateS_i isclosed;\ WB_{max} = Breadth(N) + 1 \quad (6)$$

The second layer of the Gradient Smart Load Balancer step is to organize a gradient surface to smooth task migrations between blocks in the blockchain network. The heap value of all proximities then denotes the gradient surface. The proximity of a sensor in the form of a block. 'S_i', 'WS_i', represent the minimum distance between the block and a lightly loaded sensor in the blockchain network. On the other hand, if there is no sensor in the form of a block in the blockchain network, 'WS_i' is defined as 'WS_{max}' and this is represented as given below.

$$WS_i = \min\left\{Dis_{S_i,S_k}, overkwhereG_k = 0; ifthereexistsaksuchthatG_k = 0\right\} \quad (7)$$

$$or$$

$$WS_i = WS_{max}, iff forallk, G_k = WS_{max} \quad (8)$$

From the above equations (7) and (8), the proximity of a light sensor is denoted as zero. In contrast, its instantaneous adjacent sensor's proximity represents that these sensors in the respective blocks are one hop away from a light block. The proximity of the adjacents' adjacent is two, etc. The pseudo-code representation of Gradient Smart Load Balancer is given below.

Algorithm: Gradient Smart Load Balancer
Input: IoT devices '$Dev = Dev_1, Dev_2, \dots, Dev_n$', blocks '$B = B_1, B_2, \dots, B_n$', gradient

blockchain surface 'GBS',
Output: Computationally efficient block gradient surface approximation
1: **Begin** 2: **For** each subset of IoT device. 'Dev_i' with transactions T' 3: **For** each sensors '$S = S_1, S_2, \ldots, S_n$' 4: Evaluate the breadth of a blockchain network 'BN' using equation (4) 5: Evaluate block gate using equation (5) and (6) 6: For smooth task migrations between blocks 7: Evaluate (7) and (8) 8: **End for** 9: **Return** block gradient surface approximation (BA) 10: **End for** 11: **End for** 12: **End**

As given in the Gradient Smart Load Balancer algorithm, the objective remains in improving the scalability with the increase in participating IoT devices. It is achieved by designing a two-layered Gradient Load Balancer for smart cities. In the first layer, load conditions are ascertained, and accordingly, in the second layer, block gradient surface for each sensor are organized on time, therefore ensuring scalability.

3.3 Blockchain Dempster Shafer Reputation model

In this work, a model for evaluating the reputation and trust values are obtained according to the transaction history and rating information. In our work, blockchain-based transaction history is maintained. Our proposed Blockchain Dempster Shafer Reputation model does not parse all the previous transaction to minimise the computational time and overhead incurred. Instead, it only utilizes a small cache of fundamental values without deteriorating user experience. We evaluate our model using the synthetic statistics of all IoT records. The purpose of using synthetic statistics of all IoT records is to validate the time in calculation with a large amount of data (i.e., ensuring scalability) and test the transaction query (i.e., the response and

latency for parsing a large amount of blockchain data). Figure 3, given below, shows the architecture of the Blockchain Dempster Shafer Reputation model.

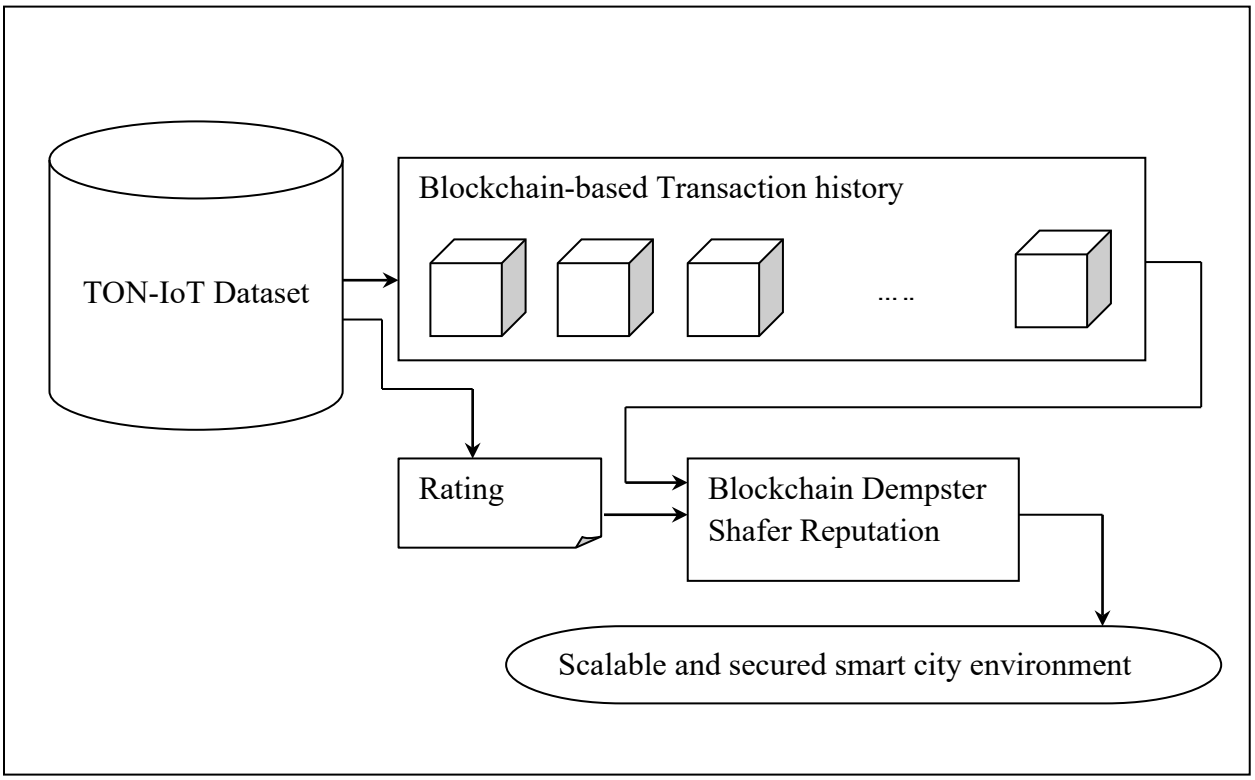

Fig. 3 Architecture of Blockchain Dempster Shafer Reputation model

As shown in the above figure, with rating information obtained according to each transaction for the respective sensor 'S', trustworthiness among IoT devices 'Dev' is said to be ensured. It is first accomplished by designing an access control mechanism for each transaction. For each transaction corresponding to the respective sensor 'S', initially, an asymmetric key pairs '$(Priv_k, Pub_k)$' are said to be generated. The private key, '$Priv_k$' is utilized to sign transaction actions for respective sensor 'S' to be performed in the blockchain network whereas public key, 'Pub_k' is employed as transaction identification to resolve the transaction. Hence, public key 'Pub_k' for corresponding sensor 'S' is sent to the blockchain network via entry-level transaction as below.

$$T_{entry} = [r_i, Pub_k, t_i, Sig_i] \tag{9}$$

From the above equation (9), entry-level transaction. 'T_{entry}' is derived based on the random number, 'r_i', public key 'Pub_k', timestamp, 't_i' and the signature of the issuer, 'Sig_i' respectively. The entry-level transaction, 'T_{entry}' is next validated in the blockchain network where the transaction signing is said to occur and is then forwarded to the blockchain network via the updated transaction as given below.

$$T_{updated} = \left[(r_i, Pub_k, t_i, Sig_i), \{r_j, t_j, Sig_j(t_i, Sig_i, r_j, t_j)\}\right] \quad (10)$$

From the above equation (10), the updated transaction, '$T_{updated}$' is generated based on the random number, 'r_j', time, 't_j' when the entry was granted and, 'Sig_j' being the issuer signature, respectively. Upon a successful update of the transaction, the newly generated transaction becomes part of a block in the blockchain. Every transaction in the blockchain network can include a public key, 'Pub_k' from '$T_{updated}$' to list of identification keys, with 't_j'. The new transaction is then said to be included in the blockchain network, which then accesses the blockchain's complete content and creates transactions.

Upon transaction selection for each IoT device, each cloud service provider preserves the information of monitored transactions with IoT devices. IoT device's public key is included in to trust table, and the transaction is attributed to the initial Reputation Score, 'RS_i'. Based on the Reputation Score for each transaction, IoT devices are categorized into a standard device, 'Dev_{nor}' or malicious device, 'Dev_{mal}' respectively. A new IoT device attains a more excellent reputation score, more significant than threshold trust value, '$Trust_{th}$' of the blockchain network, '$RS_i > Trust_{th}$' to start.

Therefore, an IoT device with a transaction must have sufficed reputation, '$RS_i > Trust_{th}$' to resume as a candidate in the blockchain network. With the reputation score and trust aid, security is ensured through Dempster Shafer and hence referred to as the Blockchain Dempster Shafer Reputation model. In the Blockchain Dempster Shafer Reputation model, all cloud service providers independently issue voting transaction for the IoT devices with '$RS < Trust_{th}$' and is mathematically expressed as given below.

$$T_v = \left(r_k, Pub_{k(mal_{dev})}, Pub_{k(CSP)}, t_k, Sig_k\right) \quad (11)$$

From the above equation (11), the voting transaction, 'T_v', for each IoT device is arrived based on the random number, 'r_k', the public key of the malicious IoT device, '$Pub_{k(mal_{dev})}$', a public key of the cloud service provider, '$Pub_{k(CSP)}$', time, 't_k' and the issuer signature, 'Sig_k'. Dempster Shafer-based reputation is utilized that integrate evidence from different sources (i.e., cloud service providers). It arrives at a degree of belief (represented by belief function) takes every available evidence (obtained from all cloud service providers) to evaluate the trustworthy of IoT device. Then, the possible set of conclusions 'Θ' is given below.

$$\Theta = \{T_{v1}, T_{v2}, T_{v3}, \ldots\ldots T_{vn}\} \quad (12)$$

From the above equation (12), 'Θ' refers to the possible set of conclusions arrived at for each IoT device's transaction whereas, 'T_{vi}' is said to be mutually exclusive. Then, the set of all possible subsets of 'Θ' is mathematically expressed as given below.

$$\Theta = \left\{T_{vi}, T_{vj}, T_{vk}\right\} = \left\{\emptyset, T_{vi}, T_{vj}, T_{vk}, \left(T_{vi}, T_{vj}\right), (T_{vi}, T_{vk}), \left(T_{vj}, T_{vk}\right), \left(T_{vi}, T_{vj}, T_{vk}\right)\right\} \quad (13)$$

From the above equation (13), '$\emptyset$' refers to the empty set possessing '0' probability as one of the outcomes obtained from the cloud service provider has to be true. Each of the other outcomes in the possible subsets has a probability of either '0' or '1'. Then, belief in an IoT device, 'Dev_i' refers to the sum of the masses that are subsets of IoT device, 'Dev_i' respectively and is mathematically expressed as given below.

$$Be(Dev_i) = M(V_i) + M\left(V_j\right) + M(V_k) + M\left(V_i, V_j\right) + M\left(V_j, V_k\right) + M(V_i, V_k) + M\left(V_i, V_j, V_k\right) \quad (14)$$

The pseudo-code representation of Blockchain Dempster Shafer-based Reputation for a secured blockchain with smart city networks is given below.

Algorithm: A Blockchain Dempster Shafer-based Reputation calculator for evaluating the trustworthiness of IoT devices in smart city
Input: random number, 'r_i', public key 'Pub_k', timestamp, 't_i' issuer signature, 'Sig_i', IoT devices '$Dev = Dev_1, Dev_2, \dots, Dev_n$'
Output: Accurate and secured blocks
1: **Initialize** Reputation Score, 'RS_i', threshold trust value, '$Trust_{th}$'
2: **Begin**
3: **For** each subset of IoT device, 'Dev_i' with transactions T'
4: **For** each sensors '$S = S_1, S_2, \dots., S_n$'
5: Evaluate entry-level transaction, 'T_{entry}' as in equation (9)
6: Validate entry-level transaction as in equation (10) and update accordingly
7: Issue voting transaction as in equation (11)
8: Evaluate possible set of conclusions as in equation (12)
9: Evaluate the set of all possible subsets of 'Θ' as in equation (13)
10: Measure belief as in equation (14)
11: **If** '$Be(Dev_i) > Trust_{th}$'
12: **Then,** '$RS_i \rightarrow RS_i + 1$'
13: Device 'Dev_i' is a normal and honest transaction
14: **End if**
15: **If** '$Be(Dev_i) < Trust_{th}$'
16: **Then,** '$RS_i \rightarrow RS_i - 1$'
17: Device 'Dev_i' is a malicious and dishonest transaction
18: **End if**
19: **End for**
20: **End**

As given in the above Blockchain Dempster Shafer-based Reputation algorithm, the objective remains to ensure the security aspect using blockchain to develop smart cities. To achieve this objective, for each subset of IoT device with numerous transactions, the entry-level transactions are first validated, followed by which voting transactions are issued. Next, a possible set of conclusions and subsets are obtained, and accordingly, belief is measured for each

transaction. Finally, according to the belief value and the reputation score, the validity of each device is obtained. With this, the security faster adaptations of IoT-driven smart cities are said to be ensured.

4. Experimental results and Discussion

Experimental analysis of GSLB-BDSR is conducted in CloudSim and Java programming language with IoT-based datasets ToNIoT [21], [22]. The results of GSLB-BDSR are compared with [1] and [2] for in-depth analysis of latency time, throughput, security response time, accuracy. A prototype has been implemented to examine the viability and performance of the method. The configuration utilized for analyzing the simulation is an intel core i7-4790@3.60GHz processor, 4GB RAM.

4.1 Dataset description

The TON_IoT datasets are the new generations of IoT datasets for measuring the effectiveness of several cybersecurity applications. Datasets have been referred to as ToN_IoT, includes heterogeneous data sources taken from telemetry datasets of IoT, **O**perating systems datasets of Windows 7 and 10 with Ubuntu 14 and 18 TLS and **N**etwork traffic datasets. Moreover, datasets are attained from a realistic and large-scale network in detailed presented at IoT Lab of UNSW Canberra Cyber, School of Engineering and Information technology (SEIT), UNSW Canberra @ the Australian Defense Force Academy (ADFA). Besides, datasets were attained in a parallel processing manner for obtaining numerous regular and cyber-attack events. It included raw datasets, processed datasets, train test datasets, description stats, and security events ground-truth data set.

4.2 Performance analysis of throughput, accuracy and precision

The first essential and significant metric of consideration for scalable and secured development of smart cities is accuracy. The higher the accuracy rate, the large numbers of IoT devices tasks are being accessed, and more significant events are noted from IoT networks. Accuracy 'Acc' refers to the percentage ratio of correctly identified instances for sustainable

smart cities by leveraging blockchain and reputation model to the total number of observations in the test case. It takes both a valid positive rate, 'TP' and an actual negative rate, 'TN', into account for measuring the accuracy. It is mathematically expressed as given below.

$$Acc = \frac{TP+TN}{TN+FN+TP+FP} * 100 \quad (15)$$

From the above equation (15), the accuracy rate 'Acc' is measured based on the actual positive rate 'TP', actual negative rate 'TN', false-positive rate 'FP' and the false-negative rate 'FN'. It is calculated in percentage (%). Second parameter is precision. It refers to the percentage ratio of malicious activities detected to the total number of observations measured as an attack. The precision rate is mathematically expressed as given below.

$$P = \frac{TP}{TP+FP} * 100 \quad (16)$$

From the above equation (16), the precision rate 'P', is measured based on the actual positive rate 'TP' and the false positive rate 'FP'. It is calculated in percentage (%). Throughput is utilized to increase the efficiency of the method. '$Throughput$' refers to the number of transactions confirmed by the blockchain network to the time that the sensors spend in the operational level for smart cities from the initiation to the ending process. It is mathematically expressed as given below.

$$Throughput = \frac{T_i}{time_{init \rightarrow end}} * 100 \quad (17)$$

From equation (17), throughput '$Throughput$', is calculated with the number of transactions 'T_i' to time between the start of operation and end of the operation, '$time_{init \rightarrow end}$'. It is calculated in percentage (%). Table 1 below shows the throughput, accuracy, and precision of three different methods: GSLB-BDSR, TP2SF [1], and Blockchain-based smart home gateway network [2]. From table 1, the performance of the GSLB-BDSR method using the ToN_IoT dataset illustrates improved throughput, accuracy and precision.

Table 1 Throughput, accuracy and precision results obtained using GSLB-BDSR, TP2SF [1] and Blockchain-based smart home gateway network [2] on ToN_IoT test dataset

Parameters	Methods		
	GSLB-BDSR	TP2SF	Blockchain-based smart home gateway network
Throughput (%)	91.35	88.25	86
Accuracy (%)	98.35	97.71	95.25
Precision (%)	90.15	87.55	84.15

As given in the above table, the ToN-IoT dataset comprises both the regular and attack instances involving unbalanced frequencies. Hence, to evaluate the security and scalability aspects, the performance of the GSLB-BDSR method, the throughput, accuracy, and precision results are calculated.

Figure 4 shows the graphical representation of throughput, accuracy and precision concerning 5000 transactions carried out at different timestamps for measuring the security and scalability for the development of smart cities. From the figure, it is inferred that the three parameters, throughput, accuracy, and precision, are better using GSLB-BDSR than two existing methods, TP2SF [1] and Blockchain-based smart home gateway network [2] on the ToN_IoT test dataset.

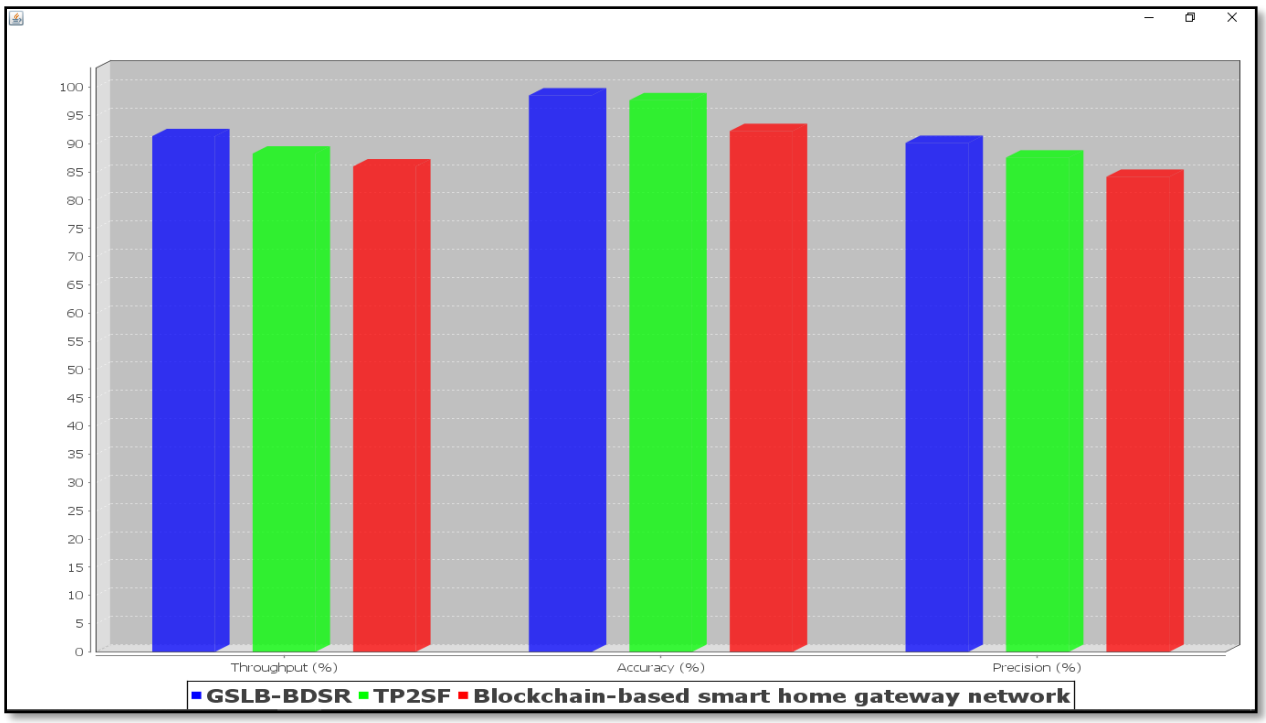

Fig. 4 Measurement of throughput, accuracy and precision with the variation in the number of transactions

First, throughput refers to the rate of transactions confirmed by the blockchain network. Maximum throughput or maximum rate of transactions ensured by the blockchain network ensures the efficiency of the method. The throughput improvement using the GSLB-BDSR method is due to applying the Gradient Smart Load Balancer model. By applying this model, only after ascertaining the load condition in the first layer, the organization gets proceeds. With this significant number of transactions are said to be processed in the blockchain network. The throughput using the GSLB-BDSR method is enhanced by 4% and 3% compared to [1] and [2].

In the second set of experiments, accuracy is shown. Accuracy refers to the correct identification of instances (i.e., regular instances to be identified as usual and malicious instances identified as malicious). The IoT features considered for experimentation were collected from IoT Fridge activity, IoT Garage Door activity, IoT GPS tracker activity, IoT Modbus activity, IoT Motion Light activity, IoT Thermostat activity and IoT Weather activity, a total number of 5000 transactions obtained at different timestamps. From the graphical representation, it is inferred that the accuracy is better using the GSLB-BDSR method than [1] and [2].

The reason behind the improvement was due to the application of the Gradient Smart Load Balancer algorithm. The gradient block surface was organized only after ascertaining the load put in the blockchain network by applying this algorithm. The scalability was improved, and the rate of transactions accurately addressed involving different IoT due to the binary function applied, therefore ensuring smooth task migrations between blocks in the blockchain network. Due to this, the accuracy using the GSLB-BDSR method was better than 2% compared to [1] and 6% compared to [2].

Finally, we estimated precision to address the scalability aspect for different IoT features. Precision illustrated the number of transactions confirmed based on actual positive and false positive by the cloud service provider via the blockchain network. Also, the precision using the GSLB-BDSR method was better than [1] and [2]. The improvement was due to the application of Proximity Administration and Block Gradient Surface in the GSLB-BDSR method. With this, both the breadth and the proximity factor were considered for the increasing number of participating devices or transactions. The precision was better using the GSLB-BDSR method by 3% compared to [1] and 4% compared to [2], respectively.

4.3 Performance analysis of latency time

Next, to ensure scalability using blockchain for the development of smart cities, latency is highly considered. It refers to the time consumed in confirming the transactions. It is mathematically expressed as given below.

$$Latency_t = \sum_{i=1}^{n} T_i * Time\ [TB] \tag{18}$$

From the above equation (18), latency time, '$Latency_t$' refers to the number of transactions involved in a simulation, 'T_i' and the time consumed in transacting the blocks '$Time\ [TB]$'. It is calculated in milliseconds (ms). Table 1 below shows the latency time of three different methods, GSLB-BDSR, TP2SF [1] and Blockchain-based smart home gateway network [2], respectively. From table 1, the performance of the GSLB-BDSR method using the ToN_IoT dataset shows minimum latency time.

Table 2 Latency time results obtained using GSLB-BDSR, TP2SF [1] and Blockchain-based smart home gateway network [2] on ToN_IoT test dataset

Number of transactions	Latency time (ms)		
	GSLB-BDSR	TP2SF	Blockchain-based smart home gateway network
500	72.5	92.5	102.5
1000	90.15	105.35	125.15
1500	102.35	125.45	155.85
2000	115.45	140.15	180
2500	165.85	190.35	225.15
3000	205.35	225.15	240.35
3500	245.55	260.15	295.15
4000	260	285.55	325.55
4500	285.35	315.5	350.15
5000	305.15	335.55	395.45

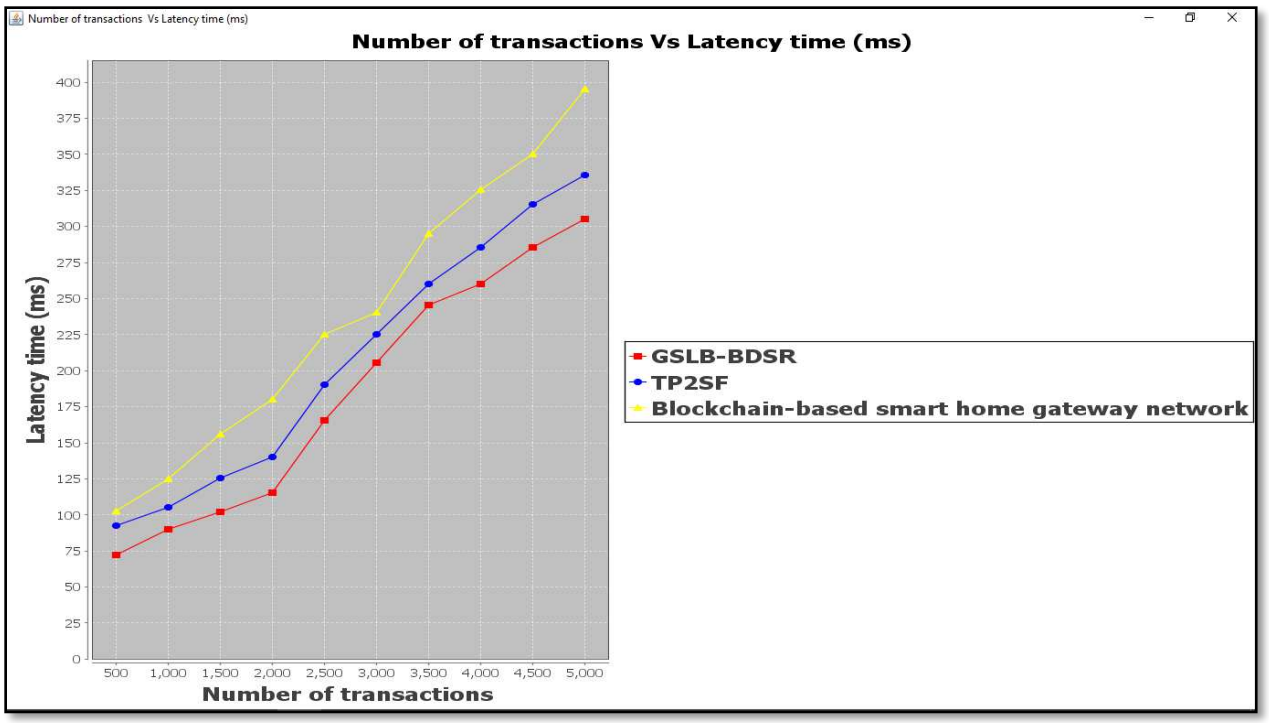

Fig. 5 Measurement of latency time with the variation in the number of transactions

Figure 5 shows the latency time for numerous transactions in the range of 500 to 5000, including different types of IoT features. From the figure, inferences can be made for different numbers of transactions. The latency time is found to be directly proportional to the number of transactions provided as input. In other words, increasing the number of transactions causes an increase in the number of IoT features involved in transacting smart city structure. Conversely, the latency time is also said to be increased. However, with '500' number of transactions to be performed in the blockchain network and the time consumed in transacting single blockchain being '$0.145ms$' using GSLB-BDSR, '$0.185ms$' using [1] and '$0.205ms$' using [2], the overall latency time was observed to be '$72.5ms$', '$92.5ms$' and '$102.5ms$' respectively.

The improvement using GSLB-BDSR is due to the application of the Blockchain Dempster Shafer-based Reputation algorithm. By applying this algorithm, scalability is said to be ensured. In other words, the transactions are quickly confirmed by the cloud provider in the blockchain network. To reduce the latency time, for each subset of IoT device with numerous transactions, validation of the entry-level transactions is first performed. Then the actual voting

transactions are issued. The probable conclusion set and subsets were obtained based on the belief obtained for each transaction. Finally, based on the belief and reputation score, validity was made; this, in turn, reduced the latency time of the GSLB-BDSR method by each device is obtained. The security faster adaptations of 13% compared to [1] and 25% comparison to [2] respectively.

5. Conclusion

An efficient GSLB-BDSR method for building a secure and scalable method using blockchain to develop smart cities is proposed to improve throughput, accuracy, and precision with minimum latency time. In work, the scalability is addressed via throughput, latency time, whereas security is addressed utilizing precision and accuracy. The key objective of GSLB-BDSRmethod is to ensure throughput, precision, accuracy maximization and minimize latency time for a smart city environment. The objective of GSLB-BDSRmethod is attained with the application of Gradient Smart Load Balancer and Blockchain Dempster Shafer-based Reputation algorithm. First, a two-layer modelled was structured to ensure scalability where ascertaining load conditions and organization of each block for numerous transactions were made in a computationally efficient manner. By employing the Blockchain Dempster Shafer-based Reputation algorithm, reputation scores were obtained through Blockchain Dempster Shafer and rating was made accordingly for each transaction. Finally, for each belief factor were obtained and only upon reputation score evaluation, the IoT devices were accessed, ensuring security. The efficiency of the GSLB-BDSR method is estimated in terms of throughput, accuracy, precision and latency time. Simulation results ofGSLB-BDSRmethod present better performance with enhanced scalability and security for smart cities via blockchain than conventional works.

Funding Information

No Funding

Conflict of Interests

On behalf of all authors, the corresponding author states that there is no conflict of interest.

Data Availability statement:

Data sharing not applicable to this article as no datasets were generated or analysed during the current study.

Code Avaliability

Not Applicable.

References

[1] Kumar, P., Gupta, G. P., & Tripathi, R. (2020). TP2SF: A Trustworthy Privacy-Preserving Secured Framework for sustainable smart cities by leveraging blockchain and machine learning. Journal of Systems Architecture, 101954.

[2] Lee, Y., Rathore, S., Park, J. H., & Park, J. H. (2020). A blockchain-based smart home gateway architecture for preventing data forgery. Human-centric Computing and Information Sciences, 10(1), 1-14.

[3] Pourghebleh, B., & Hayyolalam, V. (2019). A comprehensive and systematic review of the load balancing mechanisms in the Internet of Things. Cluster Computing, 1-21.

[4] Ahmed, S., Shah, M. A., & Wakil, K. (2020). Blockchain as a Trust Builder in the Smart City Domain: A Systematic Literature Review. IEEE Access, 8, 92977-92985.

[5] Hoque, M. A., & Davidson, C. (2019). Design and implementation of an IoT-based smart home security system. International Journal of Networked and Distributed Computing, 7(2), 85-92.

[6] Rathee, G., Balasaraswathi, M., Chandran, K. P., Gupta, S. D., & Boopathi, C. S. (2020). A secure IoT sensors communication in industry 4.0 using blockchain technology. Journal of Ambient Intelligence and Humanized Computing, 1-13.

[7] Ismagilova, E., Hughes, L., Rana, N. P., & Dwivedi, Y. K. (2020). Security, privacy and risks within smart cities: Literature review and development of a smart city interaction framework. Information Systems Frontiers, 1-22.

[8] Park, J. H., Salim, M. M., Jo, J. H., Sicato, J. C. S., Rathore, S., & Park, J. H. (2019). CIoT-Net: a scalable cognitive IoT based smart city network architecture. Human-centric Computing and Information Sciences, 9(1), 1-20.

[9] Jayasinghe, U., Lee, G. M., MacDermott, Á., & Rhee, W. S. (2019). TrustChain: A privacy preserving blockchain with edge computing. Wireless Communications and Mobile Computing, 2019.

[10] Syed, T. A., Alzahrani, A., Jan, S., Siddiqui, M. S., Nadeem, A., & Alghamdi, T. (2019). A comparative analysis of blockchain architecture and its applications: Problems and recommendations. IEEE access, 7, 176838-176869.

[11] Singh, S., Sharma, P. K., Yoon, B., Shojafar, M., Cho, G. H., & Ra, I. H. (2020). Convergence of blockchain and artificial intelligence in IoT network for the sustainable smart city. Sustainable Cities and Society, 63, 102364.

[12] Akram, S. V., Malik, P. K., Singh, R., Anita, G., & Tanwar, S. (2020). Adoption of blockchain technology in various realms: Opportunities and challenges. Security and Privacy, 3(5), e109.

[13] Bodkhe, U., Tanwar, S., Parekh, K., Khanpara, P., Tyagi, S., Kumar, N., & Alazab, M. (2020). Blockchain for industry 4.0: A comprehensive review. IEEE Access, 8, 79764-79800.

[14] Khrais, L. T. (2020). IoT and Blockchain in the Development of Smart Cities. Khrais, L.(2020). IoT and Blinternational Journal of advanced computer science and applications, 153-159.

[15] Sun, J., Yan, J., & Zhang, K. Z. (2016). Blockchain-based sharing services: What blockchain technology can contribute to smart cities. Financial Innovation, 2(1), 1-9.

[16] Rahman, M. A., Rashid, M. M., Hossain, M. S., Hassanain, E., Alhamid, M. F., & Guizani, M. (2019). Blockchain and IoT-based cognitive edge framework for sharing economy services in a smart city. IEEE Access, 7, 18611-18621.

[17] Sun, J., Ren, L., Wang, S., & Yao, X. (2020). A blockchain-based framework for electronic medical records sharing with fine-grained access control. Plos one, 15(10), e0239946.

[18] Chenthara, S., Ahmed, K., Wang, H., Whittaker, F., & Chen, Z. (2020). Healthchain: A novel framework on privacy preservation of electronic health records using blockchain technology. Plos one, 15(12), e0243043.

[19] Tiwari, A., & Batra, U. (2021). IPFS enabled blockchain for smart cities. International Journal of Information Technology, 13(1), 201-211.

[20] Sun, W., Dedahanov, A. T., Shin, H. Y., & Li, W. P. (2021). Using extended complexity theory to test SMEs' adoption of Blockchain-based loan system. PloS one, 16(2), e0245964.

[21] Haider, W., Moustafa, N., Keshk, M., Fernandez, A., Choo, K. K. R., & Wahab, A. (2020). FGMC-HADS: Fuzzy Gaussian mixture-based correntropy models for detecting zero-day attacks from linux systems. Computers & Security, 96, 101906.

[22] N. Moustafa, http://dx.doi.org/10.21227/fesz-dm97, Feb 2019

Figures

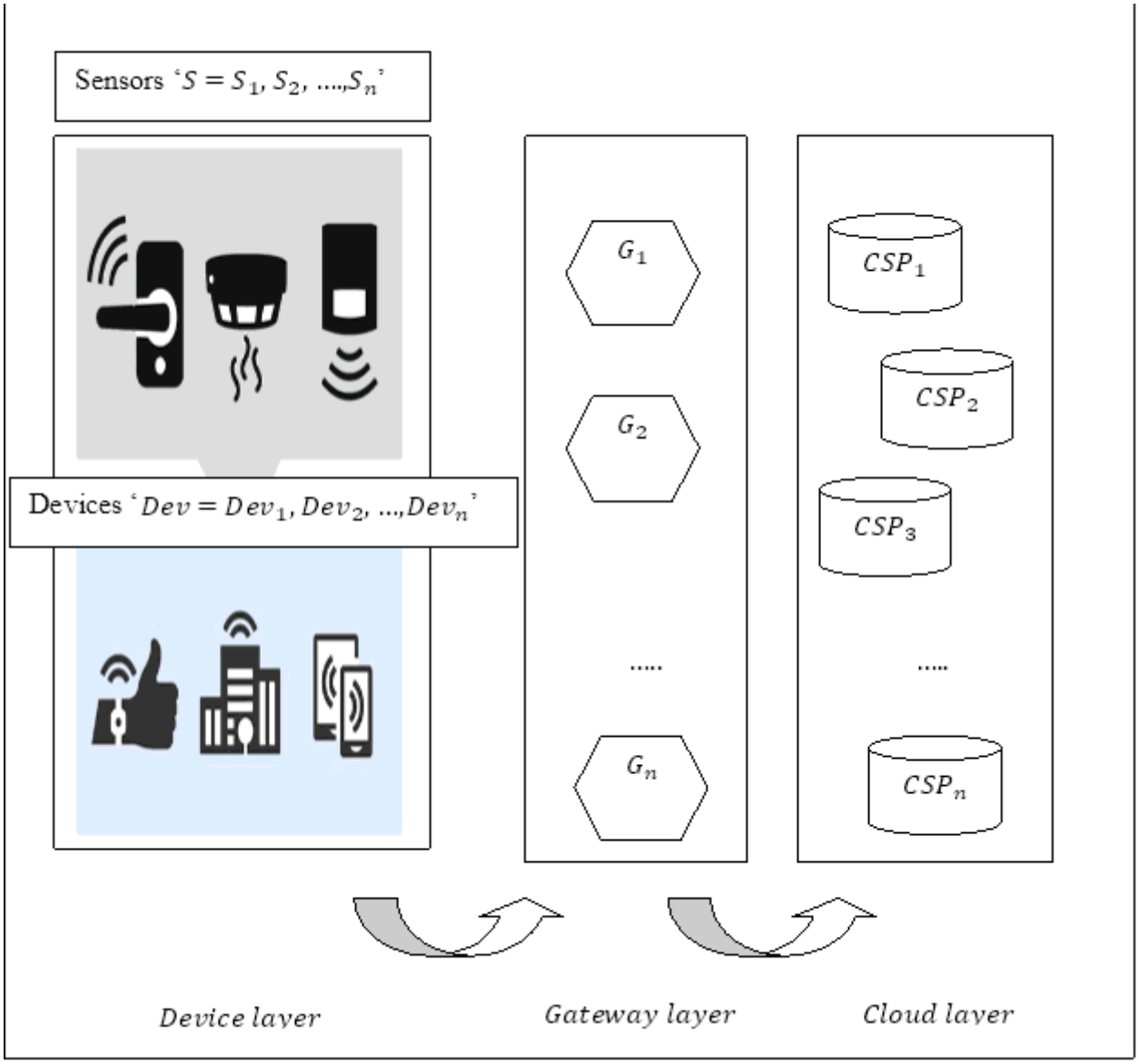

Figure 1

Overview of the network model

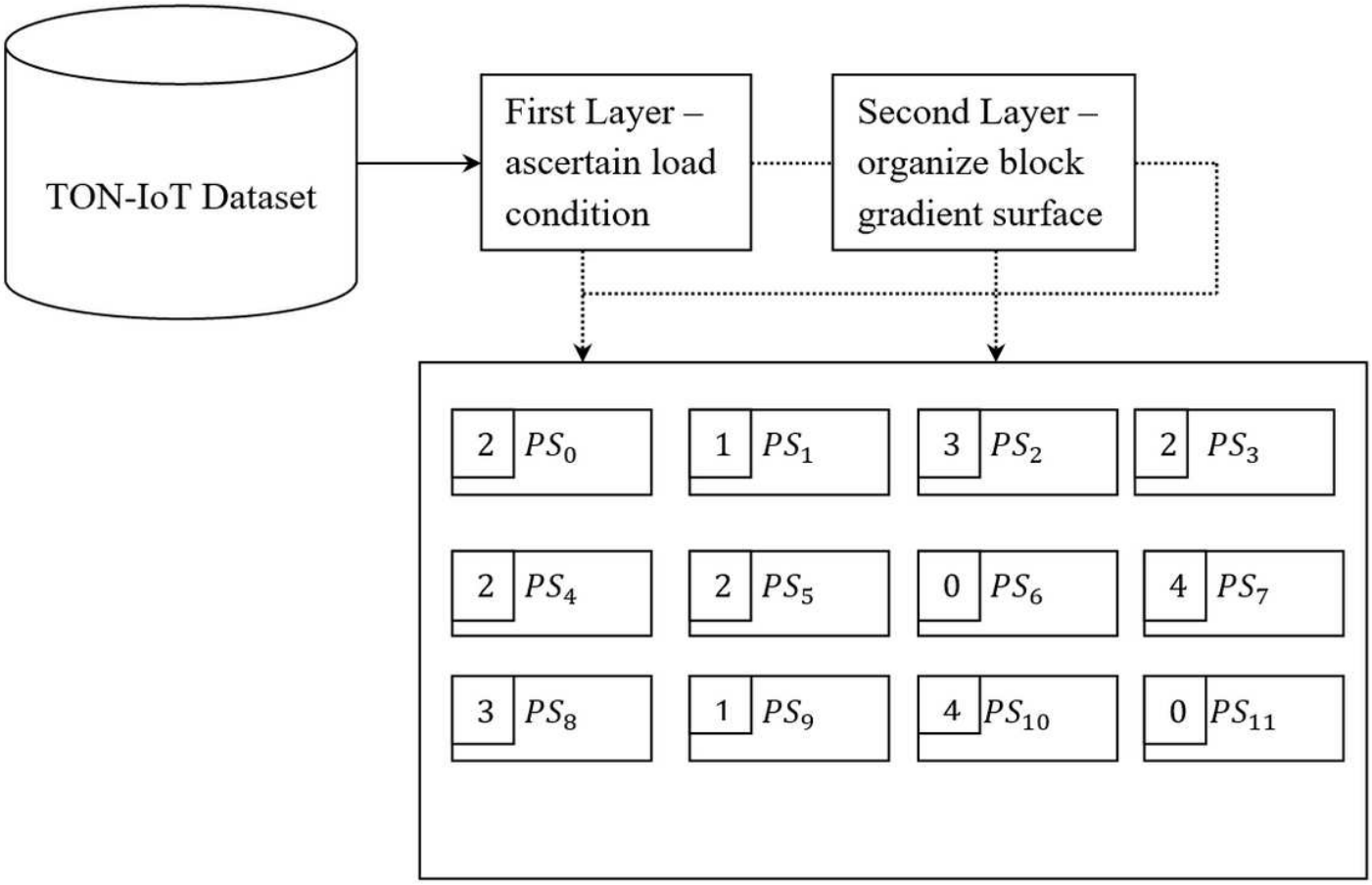

Figure 2

Block diagram of Proximity Administration and Block Gradient Surface

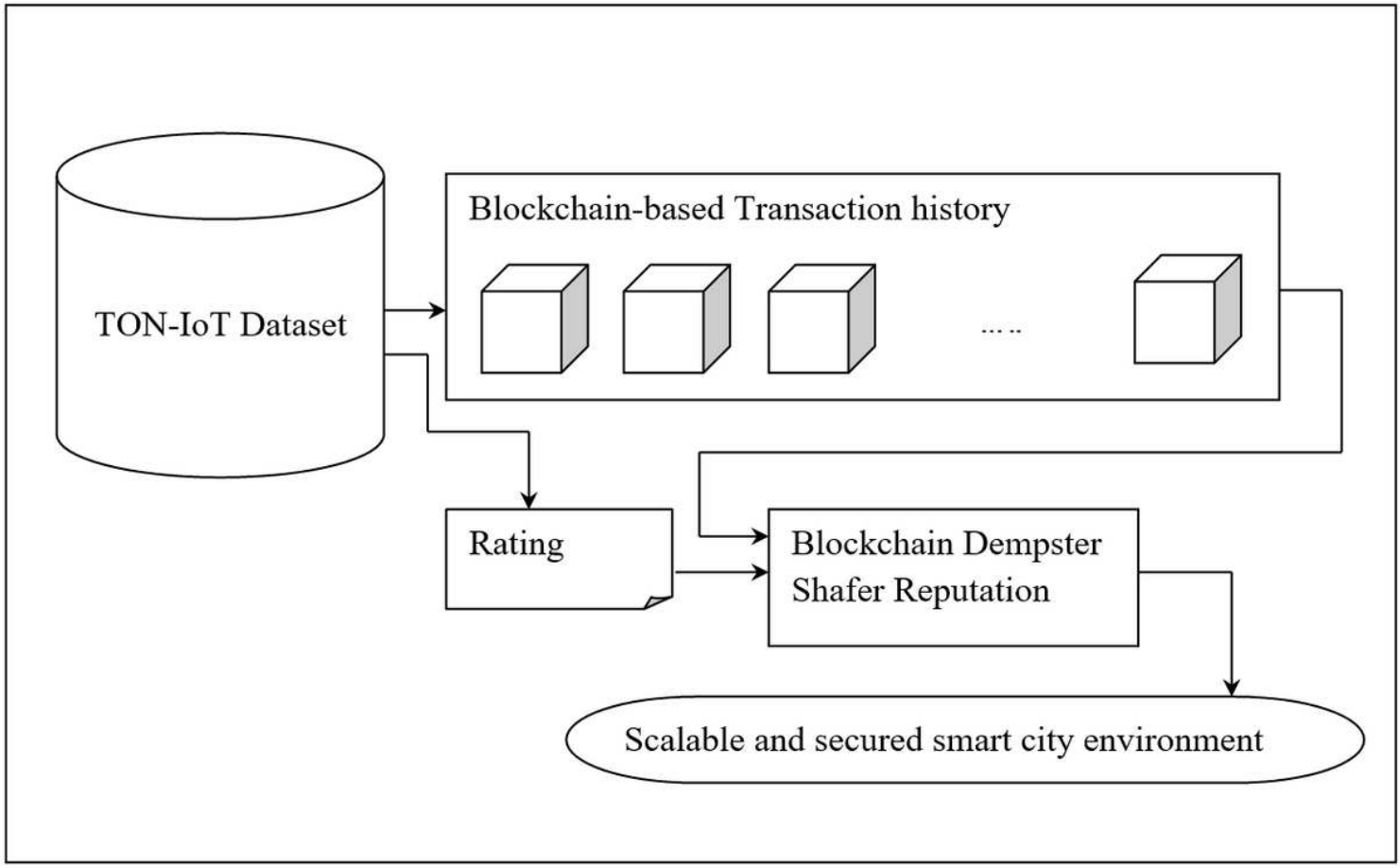

Figure 3

Architecture of Blockchain Dempster Shafer Reputation model

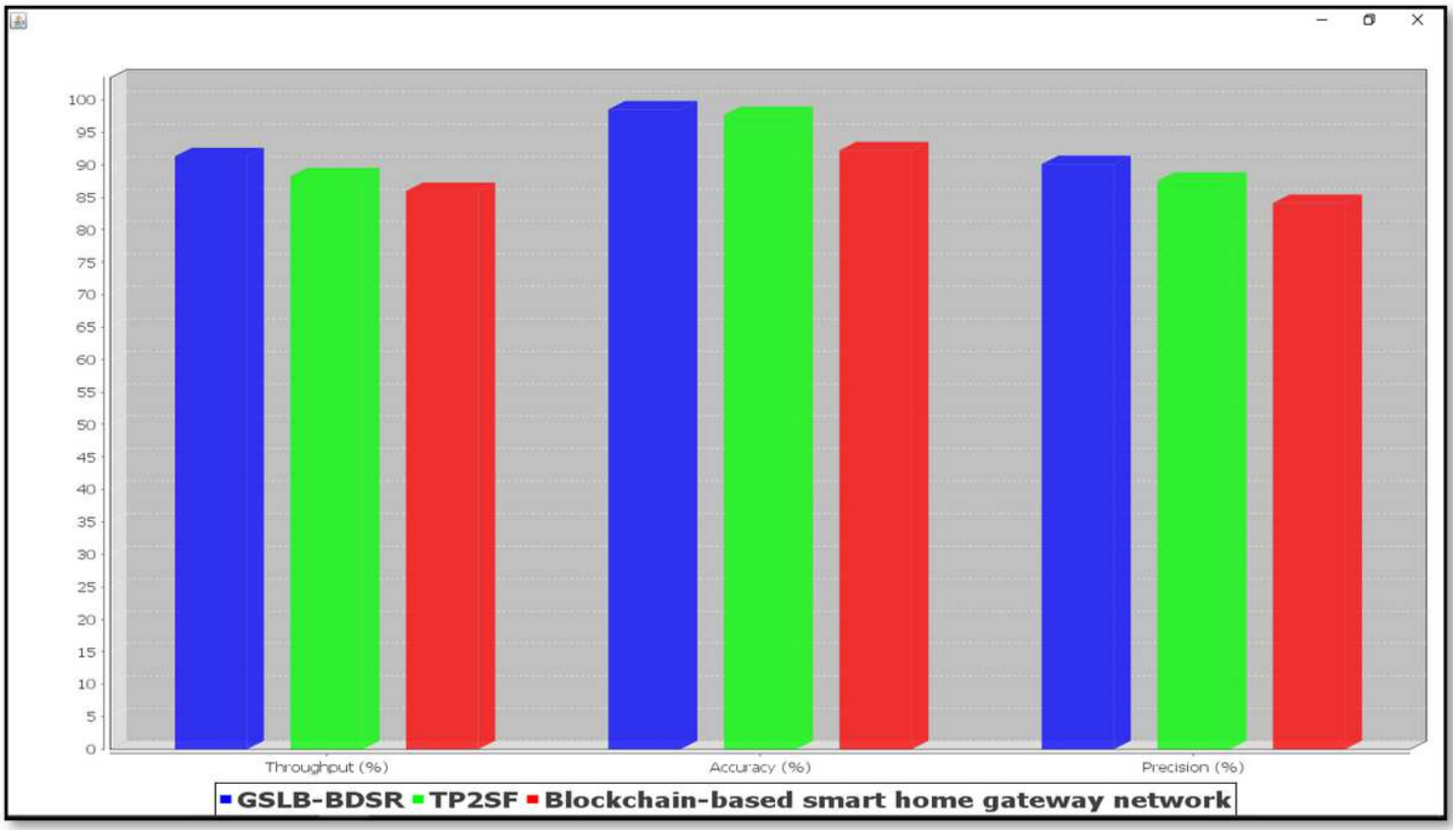

Figure 4

Measurement of throughput, accuracy and precision with the variation in the number of transactions

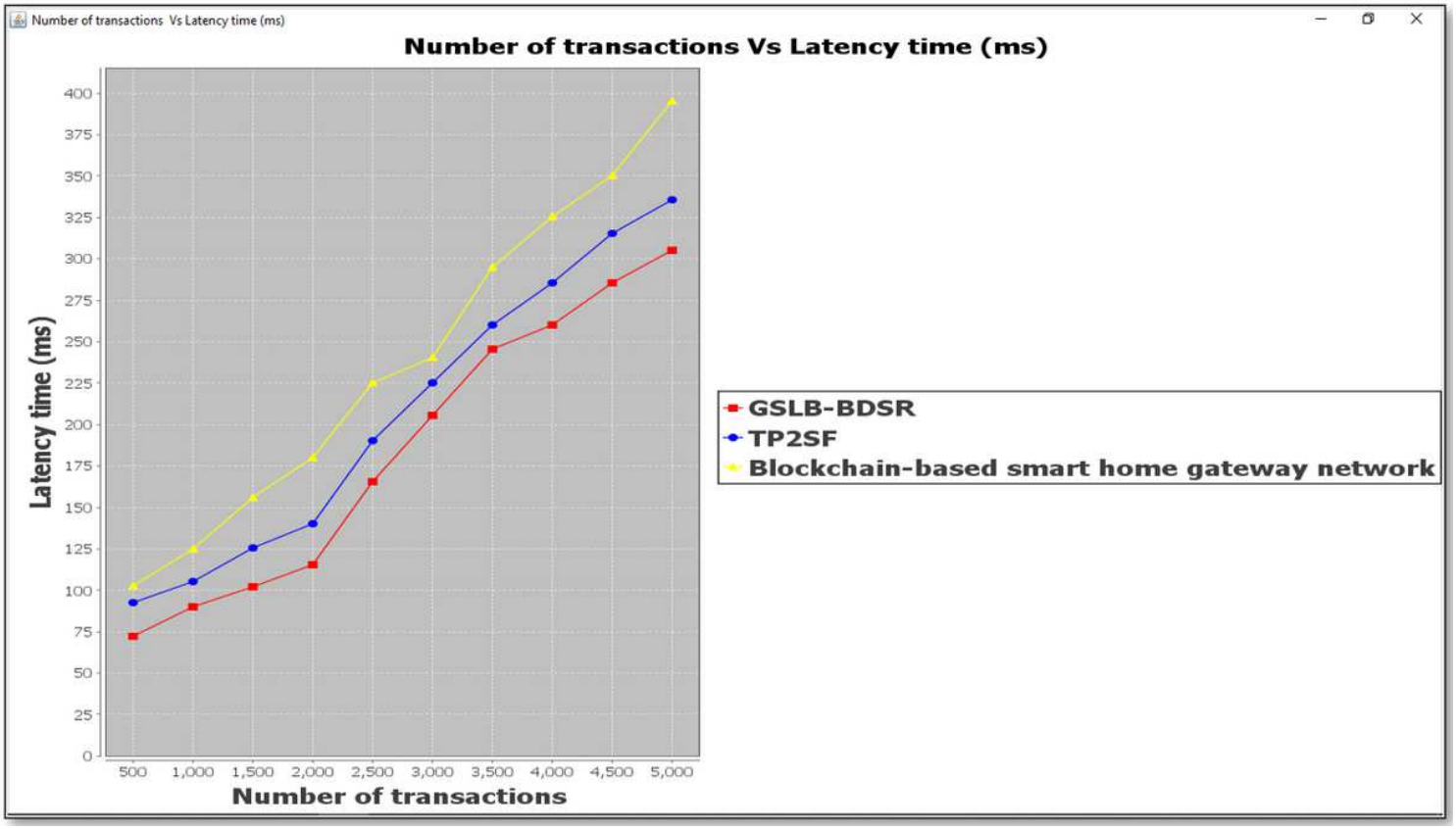

Figure 5

Measurement of latency time with the variation in the number of transactions