International Journal of Mechatronics, Electrical and Computer Technology (IJMEC)
ISSN: 2305-0543 (Online), ISSN: 2411-6173 (Print)
Vol. 12 (44), Apr. 2022, pp. 5151-5157

Block Chain Performance in 5G and LTE in IoT Platform for Industrial Applications

Amirhossein Ghasemi[1]
Department of Engineering, Bozorgmehr University of Qaenat, Qaen Iran
ghasemi@buqaen.ac.ir
Tel Number: +98-56131006804

Mohsen Saberi [2]
Department of Engineering, Bozorgmehr University of Qaenat, Qaen Iran
saberi@buqaen.ac.ir
Tel Number: +98-56131006804

***Abstract*—The Internet of Things (IoT) requires the creation of new structures that use edge and fog computing environments due to the lack of optimal quality of services and bandwidth requirements. This new paradigm can accomplish many of internet tasks on the edge and fog which is capable to confronting a wide range of technologies in the IoT. For example, edge and fog computing can be used in smart home, smart city, smart driving and other things that are planned based on IoT mechanisms. Since resource management along with quality of services in the internet has been challenging in recent years as the technology has grown, providing integrated structures is essential and connecting to 5G and LTE standards due to more internet speed. For this purpose, Block Chain with a minimum computational complexity and high level of flexibility are provided which are capable to create gateways for the IoT-based edge and fog computation with a regular and optimal access mechanism for 5G and LTE. This research aims to provide a secure gateway structure with the maximum privacy of data in the connected 5G and LTE internet environment with multiple edge and fog computing. The use of encryption mechanisms including DTLS and FSK is considered as the main approach used in the Block Chain structure for transmitting and receiving data in industrial application. The proposed approach is called the Secure Gateway Block Chain Edge Fog in IoT or SGBCH-IoT. Improving the quality of services includes delays, passivity, probability of data detection, probability of miss detection, and data lose rate to manage the resources of the network. The results represented that the proposed approach has better performance in comparison to others.**

Keywords: BlockChain, Edge and Fog Computing, Internet of Things (IoT), Resource Management, , 5G, LTE

I. Introduction

The Internet of Things network is presented as the newest Internet-based computer networking model and structure. This network works as several objects communicate with each other through an array of sensors or other technologies such as Bluetooth which can send and receive data. The growth of such a network which don't need human resource intermediaries can send and receive data through objects at certain times and will surely lead to high development. This expansion on a large scale can display various challenges. A series of challenges include security, routing, clustering, reliability, and more. In this case, it is necessary to propose new and advanced solutions that operate intelligently [1]. Security is considered as the one of the most perilous challenges of the IoT. So that various objects connected to the Internet may be subjected to various cybercrime attacks and since humans do not directly interfere with the sending and receiving of data in such a network, so there may be many problems in an environment or organization and other sections. An obvious example of this is that sensors in smart homes that have remote control capabilities through the IoT can cause cyber-attacks, and overlap control settings. This can be a huge cost to users of the IoT. Therefore, providing new security solutions are essential [2]. Cryptography can solve many problems in security. Cryptography is used as a coding structure to codify data. To do this, it should have access to the main structure of the applicable programs covered by the IoT and can encrypt their data in sending and receiving. One of the structures that this research is trying to encrypt is the use of lightweight protocols. Cryptography of communication channels with lightweight protocols can be a new issue in the IoT. Creating a secure environment used with responsive schema at the level of the Constrained Application Protocol (CoAP). The use of cryptographic structures at the level of the applied data layer is based on the security mechanism of the Datagram Transport Layer Security (DTLS) with the Pre-Shared Key (PSK) [3]. Denial of Service (DoS) or Distributed Denial of Services (DDoS) are two main attacks in application layer of IoT. This research attempts to provide a secure gateway regardless of the type of attack that may be used on edge and fog computing. The use of edge and fog computing in the IoT as well as cloud and fog computing can be seen on the IoT in the Fig. 1.

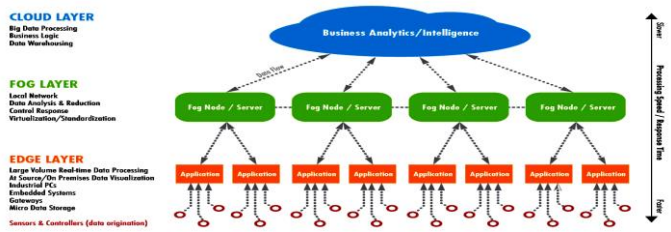

Fig. 1. Cloud, fog and edge computing in IoT environment

It is expected that to create a new multi-edge secured gateway on the IoT which can be provided to resource management. The purpose of resource management is the Quality of Service (QoS) which includes throughput, Bit Error Rate (BER), delay, and Signal-to-Noise Ratio (SNR). All these things will be provided and created on the safe gateway. In general, the most important goals pursued by this research include:

Presentation of a new Block Chain secured prototype model to guarantee the security of the IoT

providing a cryptographic model on gateway based on the security mechanism of the data Datagram Transport Layer Security (DTLS) with the Pre-Shared Key (PSK) in the Block Chain in the platform of multiple edge and fog computing-based IoT connection to 5G and LTE.

Block Chain Overview

The name "Blockchain" itself refers to the structure of the Blockchain's data can be thought of as an immutable chain of events. Data, mostly in the form of transactions, is grouped together in a block. This block is then packaged with a reference to the previous block, which contains a reference to the block before that, etc. Blockchain is "distributed" because every participant in the network holds a copy of this append only ledger. All participants, or peers, must agree on the state of the ledger and unauthorized changes to that ledger must be reasonably detectable. In reality, Blockchain technology requires (1) a distributed ledger among peers, (2) a consensus protocol to ensure that all peers have the same copy, and (3) a cryptographic infrastructure. Every other detail is determined by the desired application.

A. Consensus Protocols

We provide an overarching classification for consensus methods. In-depth protocol algorithms and mathematical proofs of robustness are beyond the scope of this paper. Consensus protocols have their own massive pool of research effort and are well-reviewed in other works [4]:

1) Lottery Election: Lottery election, such as Proof of Work (PoW), relies on probability to "elect" a consensus leader who determines the order of incoming transactions, usually for a set amount of time. In Bitcoin, peer nodes append a nonce to a block and calculate the hash value. The resulting value must have some pre-determined number of leading zeros. Peers constantly hash new values in order to find the

Article History:
Received Date: Nov. 03, 2021, Accepted Date: Jan. 06, 2022, Available Online: Apr. 01, 2022

correct "answer." The first peer to find the right nonce broadcasts its results to the network, who verifies and appends the block organized by the winning leader. This temporary leader is the one that determines the order of transactions within its announced block. In this case, difficulty is determined by the number of leading zeros and the leader is only the leader for one block. Other lottery election examples include Proof of Stake (PoS) and Proof of Elapsed Time (PoET) [4], although this is by no means an exhaustive list. Note that election difficulty and leader term lengths could be configurable parameters.

2) Majority Election: Majority election refers to a majority of peers voting on a particular value. Peers could vote to validate a transaction, or vote upon a block leader. The distinction here is that majority election does not rely on probability, but is instead far more communication-bound - the notable example being Practical Byzantine Fault Tolerance (PBFT) [5]. Consensus in this manner must take care to manage its upscaling to prevent significant communication overhead. The general trend is to create "round robin" or subgroup voting pools to mitigate scaling issues [6].

B. Implementation Differences

1) Read-Write Access: Blockchain systems can be defined by what entities have read and write access to the ledger. As aforementioned, write access is append-only. If any peer can read the ledger, it is public. If the read access is limited, it is private. If any peer can append to the ledger, it is permission less. If write access is limited, it is permissioned. Bitcoin serves as the prime example of a public, permission less Blockchain network. Anyone can participate in the network and the ledger is open to the public. Anonymity is preserved by the use of public-private key pairs. Public networks tend to require computationally heavy consensus methods - or, in the case of Ethereum's ethash method [7], computation and memory-intensive. This is mainly to protect against Sybil attacks and prevent double-spending (see II-C). A network like Sovrin [8] is public and permissioned. Anyone has access to ledger information, but additions to the ledger can only be made by specific set of participants. Permissioned Blockchain have the benefit of not requiring consensus methods as resource-intensive as permission-less systems, since unauthorized parties could be revoked for not being part of a whitelist. Privacy is not a goal for Sovrin, which is an identity management system. Alas, even for Bitcoin's anonymous addressing, true privacy is not guaranteed on a public network [9]. Private, permissioned Blockchain like Hyperledger Fabric [10] target enterprise applications, where businesses may want the fault tolerance and self-management offered by Blockchain within a private network. Smaller networks reduce communication overhead, but tend to be less secure as a result - large, public networks have the advantage of peer numbers, where a 51 percent majority attack is more difficult to execute.

2) Block Handling: Block handling refers to methods which try to reduce Blockchain latencies, either in writing to the ledger or reading from it for transaction validation. These methods include block ordering, pruning, and ledger sharing. Block ordering can be handled in a number of ways. Bitcoin can result in forks - when more than one peer concurrently broadcasts a valid block to append to the ledger. At that point, peers will continue to "race" against one another to find the next hash value, and once the longer chain is created, the other peers will adopt that chain. Ethereum mitigates this wasted effort by creating incentives to include so-called "orphaned" blocks into the main chain. Directed Acyclic Graphs (DAG) have also been suggested for block ordering to decrease ordering delay [11, 12]. Whereas traditional Blockchain are mostly linear in structure, DAG Blockchain allow for more complex web chains. Block pruning has been suggested to reduce ledger size [13] [14], generally by reducing older blocks into a new "jumpoff" point from which the ledger can continue. As long as all peers reach consensus and agree to prune, the ledger can be collectively reduced. This method needs to carefully define at which point old data is considered "old enough." Ledger sharing is another method to reduce ledger read times. A system could provide service-specific Blockchain, such as in [13-15]. Transaction validations would avoid searching through unnecessary blocks in order to find relevant information, but be linked at common blocks for some set interval. Other proposed protocols with ledger sharing can be found in [15, 16].

Possible attack vectors on a Blockchain network. Which the peer node outside the inner shaded area is the only non-malicious actor presented in Fig. 2.

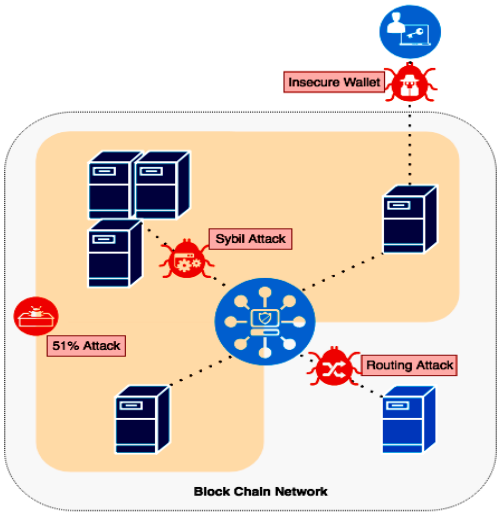

Fig. 2. Possible attack vectors on a Blockchain network. In this case, the peer node outside the inner shaded area is the only non-malicious actor.

LTE Review

LTE has emerged as a very flexible radio access technology, supporting multiple system bandwidth configurations. LTE bandwidth is flexible in the physical layer from 1.4 MHz to 20 MHz, with each terminal capable of supporting the widest bandwidth allocation. The highest data rate in this technology is predicted to be 100Mbps downstream and 50Mbps upstream [17]. LTE covers a wide range of Internet and multimedia services, even at very high speeds. It is therefore designed to support high bandwidth, low latency and complex traffic models. LTE uses multiple orthogonal frequency division or OFDMA downstream access. OFDMA divides the frequency band into several perpendicular sub-frequencies. This helps to improve the system's ability to provide high data rates, multi-user diversity and inter-symbol compression [17]. A LTE network consists of a series of components in architecture whose understanding helps to understand this structure. An LTE network consists of an evolved packet core or ECP and an E-UTRAN universal radio access network. EPC is a fully IP-based network and a switched packet or PS network in LTE systems. Voice service is a switched-circuit network service or CS used by the IP-IMS multimedia network subsystem. The EPC consists of a home or HSS shared server and a server or SGW port, a packet data network or PDN port with a shared home or HSS server. When the user equipment connects to the EPC, the MME realizes the EPC must perform cross-validation with the EU. The e-UTRAN includes eNodeB's global terrestrial radio access network base stations that communicate with the EU. In general, based on these explanations, the LTE architecture can be seen in Fig. 3 [19, 18].

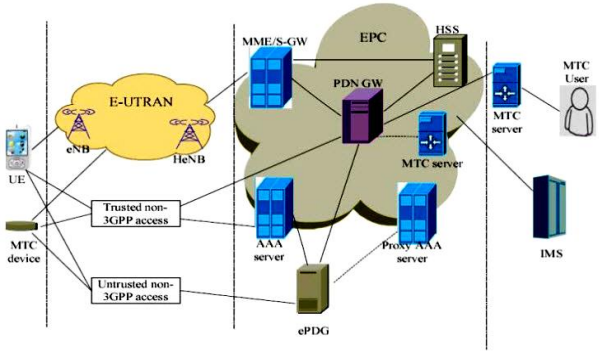

Fig. 3. LTE architecture

IEEE Office - SEET Complex, Federal University of Technology, Owerri, Nigeria, https://aeuso.org
EISSN: 2305-0543, PISSN: 2411-6173

5G Review

Called 5G, the fifth generation of mobile wireless communications promises to lower latency, offer greater stability, the ability to connect many more devices at once, and move more data thanks to faster speeds. These features have the potential to supercharge business, and that's one of the reasons 66 percent of businesses plan to deploy 5G by 2020, according to a study by Gartner. Ultimately, 5G takes advantage of higher-frequency bands in the radio spectrum that have a lot of capacity but shorter wavelengths. Cisco estimates that by 2020, 5G will generate three times more traffic than the average 4G connection, and those connections will make up 3 percent of total mobile connections [20].

II. Literature Review

Security is one of the important issues on the IoT which has been investigated in a variety of ways. Initially, cryptographic security methods are examined in the IoT and the other mechanisms for creating gateways are investigated for various purposes. The use of a key-based algorithm to safeguard the sharing of information proposed in [21]. In fact, a homomorphic cryptographic structure provided that had a key structure in identifying data and preventing different attacks. In [22], a new approach to protecting the privacy of connected devices to internet based on cryptographic principles is presented. The proposed effective and resilient approach designed to be briefly named CA-ABE. Detecting the features in the attacks counted as the encryption location. Another approach proposed by the presentation of the content structure of the cryptographic on the IoT is also presented in [23] which is named KP-ABE. In [24], a new method called REATO provided to encrypt incoming and outgoing data at the channel level in the context of the IoT aimed at securing, detecting and identifying DoS attacks. In [25], lightweight protocols features used to provide a security schema in the context of the IoT. Attributed-based Encryption (ABE) introduced as a new solution to encrypt and secure network environments that modeled and simulated in this research based on Elliptic Curve Ciphering (ECC). Reducing communication costs and improving the security of the Iot has been highlighted as the main objectives of the research. In [26], presented the LESS method as a lightweight protocol for encryption-based security in the IoT. The use of encryption with DTLS and the PSK has been considered as cryptographic methods.

In [27], a review article for security solutions has been developed based on cryptographic mechanisms such as the DES and AES algorithms. Various studies had shown that proposing secure solutions in the application layer of data provides better results. Also in [28], a study of security solutions and the challenges ahead with the use of principles and methods of encryption proposed. There was also a study on the security principles of the IoT based on the use of various protocols such as Z-WAVE and Zig Bee which presented in [29]. In [30], the optimization of the security of the DTLS based on the access schema for the health system on the IoT proposed. This research has been designed to detect DoS attacks. Using the creation of a secure environment with a response-level schema at the level of the application restricted in this study which combined the security of the DTLS and leaded to a secure environment. One of the similar articles to this study proposed in [31] which modeled a lightweight edge gateway for the IoT named LEGIoT. This model designed a gateway suitable in IoT and Edge computing scenarios. The gateway relies on microservices and lightweight virtualization technologies. LEGIoT designed to be hardware agnostic and its implementation tested within a real sensor network. Obtained results demonstrated the scalability to host different applications meant to provide a wide range of IoT services.

Other studies have been done for the use of edge computing in the IoT along with the review of its challenges which collected in [32]. Some problems and challenges notices such as high latency, low Spectral Efficiency (SE), and non-adaptive machine type of communication. In [33], a flexible security interfacing in the IoT presented based on the end-to-end fog computing. The use of optimal schematic decider algorithm considered as the idea. The use of evolutionary game theory structures presented in [34] to address the security challenges in fog computing. In [35], Internet security secured objects and solutions based on the study of attacks on cloud layers, cloud computing, fog, and edges. Also, in [36] discussed the use of fog computing in the IoT based on the type of equipment and used standards. In [37], a state-of-the-art knowledge network behavior in fog and edge computing based on security challenges proposed. The construction of a multi-layered framework based on previous knowledge in this research has been considered to take into account the security principles for sending and receiving data. In [38] used cryptographic principles to ensure data security. The simultaneous of two cryptographic algorithms called CCA and ABE, has been considered in this study which represented the results of the decryption and encryption of information at the time of sending and receiving data, and a secure environment for fog and edge computing. In [39] surveyed a case study on the issues and security challenges of the two computing systems mean fog and edge. Identifying unconventional behaviors and norms in various fog and edge computing protocols considered. In [40], the use of network-based software and cloud computing has been studied and studied as a supply chain environment for sending and receiving data with security visibility, deployment, routing, and clustering in the context of the IoT. Also, in [41], privacy studied by security conditions for the use of fog and edge computing in the IoT. Providing a secure privacy protocol for transmitting and receiving data based on the principles of cryptography was the main objective of this research in 5G and LTE connection-based of industrial applications. Also, some others studies proposed methods for LTE and 5G standard which can be used in IoT. For example, in [42], a new handover algorithm proposed for LTE and LTE-A which estimated bandwidth and other QoS. In another research which proposed in [43], a new downlink scheduling algorithm used for real time traffic in LTE systems. These two researches need to improve which can be connected to IoT and using Block Chain in their methods. In 5G studies, a new energy efficiency optimization proposed in [44] which used spectral efficiency maximization. Reducing energy was the main goal of this research. Also, in [45], a new method proposed for QoS performance evaluation by using 5G in IoT and other indoor environment networks which considered throughput, bandwidth, jitter, delay, SNR and also BER when using 5G technology in connections in indoor networks. These two research needs to improve which can be estimated their method in IoT and Block Chain platforms.

In [46], a new method designed for IoT which was optimized for wideband antenna that could improve performance. This method represented that its antenna can be used easily within compact communication device to increase total efficiency. Also, outdoor and industrial application of IoT proposed in [47] with Ethernet networks. The traffic model for multimedia data was proposed in industrial environment via IoT with four models named M1, M2, M3 and M4 which could support more data size, had tolerance to loss data, and some features which improved traffic of IoT in industrial environments.

III. Proposed Approach

The proposed method is an IoT which created based on a number of interconnected and portable equipment in the defined network dimension which connected to 5G and LTE. It is clear to communication protocols are necessary to transfer data and this research use Block Chain. Maintaining the security of transmitting and receiving data is an important issue that the Block Chain must address. Therefore, there will be an attempt to optimize the Block Chain which in this approach is to use a cryptographic structure at the level of the application data layers known as DTLS by combining the PSK method. Since using the DTLS security mechanism in Block Chain to encryption should initially assumed that it works like HTTP and can simultaneously be both client and server. The data is working asynchronously in a grid-like data structure such as UDP in the method of security mechanism of the DTLS unlike HTTP. In fact, UDP is the lowest level of data processing in the DTLS. But as long as the UDP, like TCP is unstable in data encryption, a layer-based query/response concept is also added to this part of the method of DTLS that synchronizes with UDP data and other asynchronous interactions in data retrieval, and this section begins with cryptography based on these two sections. But the need of using a key structure to decrypt is also the main need for this work. Therefore, in this phase of the Block Chain, which has its own method of DTLS, the PSK method is also added and the data are encrypted simultaneously and asynchronously, and can be on the decrypted-on destination and accessed to the application layer and transmitted on the IoT.

Parts of the combined algorithm of the DTLS will need to be modified by combining the PSK method used in Block Chain. Hence, the

IEEE Office - SEET Complex, Federal University of Technology, Owerri, Nigeria, https://aeuso.org
EISSN: 2305-0543, PISSN: 2411-6173

structure of the DTLS which is based on the structure of the encryption of HTTP, TCP, and UDP protocols is changed; so that the encryption method will be hashed. Similarly, the PSK method has an essential core of cryptographic training that leads to maintaining security. In this section of the PSK method, the cryptographic structure is the AES algorithm, but will try to improve the AES algorithm by inserting various encrypted keys and certain values of the attack intervals in the network. So, attack information extract and collect in the phase of improving the PSK method, also to the keys on the recipient's side. The purpose of diversity in cryptographic states is known as a principle, especially when data is to be sent at the level of a network through communication channels from sender to recipient. This variation means that a code must not always be common and must change over time to minimize the permeability of the ramifications. If it should be possible to do these two actions in a combined method of DTLS by PSK in the Block Chain, maintaining the confidentiality based on the optimal encryption with the hash structure and the improved encryption algorithm AES that can detect attacks in the multi-edge computing in the IoT. It is worth noting, however, that at the time of encryption on the transmitter and receiver information in the PSK method based on the optimized AES algorithm, the DTLS method will also be affected and will create a structure that can identify other attacks on the gateway and moreover, generalizable to more data. In general, the proposed approach called the Secure Gateway Block Chain Edge-Fog in IoT or SGBCH-IoT. As reference article, it can be named [14], which offers a general schematics and architecture, and with its changes, this approach using the edge on the IoT attempts to provide a secure gateway by improving quality of services and resources as shown in Fig. 4.

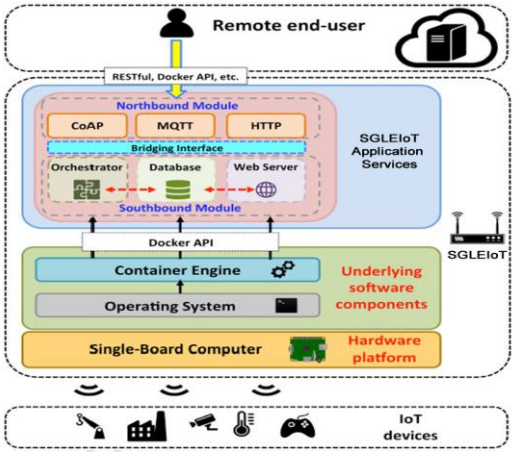

Fig. 4. Proposed approach architecture

Table (1), represent the main parameters of this study to model gateway. All of these parameters mentioned in Table (1) are used in the equation of this research which are placed in the form of a table to avoid redundancy of the description.

TABLE 1. PROPOSED MODEL MAIN PARAMETERS

Description	Mathematic Symbols
Network graph	$\xi = (I \cup \{A\}.E)$
n data provider set	I
Data submitter (transmission)	A
Network communication set	E
Measurement number for e iteration	T_e
i raw data record in e iteration	$r_{i,e,t}$
i raw data provider in e iteration	$R_{i,e}$
Raw data domain	$\mathcal{R}$
Cumulative function	α
Summarizer function	$fs: \mathcal{R}^{T_e} \to S^{T_e}$
Data record summarizer	$s_{i,e,t}$
i summarizer date in e iteration	$S_{i,e}$
Summarizer domain data	S
e local error in iteration and t time	$\epsilon_{e,t}$
e global error in iteration and t time	$\varepsilon_{e,t}$
Data groups	$G \subset I$
Data groups numbers	m
Internal data integration groups	$a_{e,t}^{G}$
Data supplier (transmitter and receiver)	a, a_1, a_2
Local group error for G group	$\epsilon_{e,t}^{G}$
Total group error for G group	$\varepsilon_{e,t}^{G}$

At first, the confidentiality of data must be modeled. Hence, the local error is in the form of equation (1) at the SGBCH-IoT gateway.

$$\epsilon_{e,t} = \frac{1}{n}\sum_{i=1}^{n} \epsilon_{i,e,t} = \frac{|r_{i,e,t} - s_{i,e,t}|}{|r_{i,e,t}| + |s_{i,e,t}|} \quad (1)$$

In the above equation, each section is the difference between raw data and summary in the provider i (sender or receiver of data). A higher-level local error in detecting attacks gives greater security and confidentiality. It should be noted that local error does not depend on cumulative function. The precision of the confidentiality of data in detecting attacks is calculated by general error which is in accordance with equation (2).

$$\varepsilon_{e,t} = \frac{|\alpha(R_{e,t}) - \alpha(S_{e,t})|}{|\alpha(R_{e,t})| + |\alpha(S_{e,t})|} \quad (2)$$

Given the fact that the confidentiality of data is possible under the conditions of equation (1) and (2), the average difference between raw data $R_{e,t} = (r_{i,e,t})_{i=1}^{n}$ and the summarized data $S_{e,t} = (s_{i,e,t})_{i=1}^{n}$. The higher the overall error, the lower the response will be to maintain the confidentiality of information in communicating and detecting attacks. To maintain the confidentiality of data when communicating devices, they must compute a cumulative distribution function between raw data and cumulative data, which is called a local group error whose relationship is as equation (3).

$$\epsilon_{e,t}^{G} = \frac{|r_{i,e,t} - a_{e,t}^{G}|}{|r_{i,e,t}| + |a_{e,t}^{G}|}, i \in G \quad (3)$$

Similarly, the cumulative distribution function must be computed between aggregated data and cumulative data, which is called the sum of the group error by calculating with equation (4).

$$\varepsilon_{e,t}^{G} = \sum_{i \in G} \frac{|s_{i,e,t} - a_{e,t}^{G}|}{|s_{i,e,t}| + |a_{e,t}^{G}|} \quad (4)$$

The calculation of the throughput in the secure gateway is given by the equation (5), the delay calculation is in the form of the equation (6), and the bit error rate calculation is in the form equation (7).

$$Throughput = Max_{Window_{Size}}^{f_w(t+1)} \times Delay^{f_w(t+1)} \times RTT^{N_{data}} \quad (5)$$

$$Latency_{D(n)} = \left(\frac{1}{\left(\frac{4}{tan^2 \frac{\theta}{2}}\right)^{\frac{2}{f_w(t+1)}} \sqrt{a(N_{data})}} \right) \quad (6)$$

$$BER = 1 - (1 - B_e)^{N_{data}} = 1 - e^{N_{data} log(1-B_e)} + f_w(t+1) \quad (7)$$

In equation (5), $Max_{Window_{Size}}$ is the maximum window size in the evaluation of sending and receiving data, which can be calculated after calculating the delay in equation (6). RTT is the time it takes to send data in sweep along the way in the IoT. It is worth noting that the calculation of latency has been done end-to-end.

IEEE Office - SEET Complex, Federal University of Technology, Owerri, Nigeria, https://aeuso.org
EISSN: 2305-0543, PISSN: 2411-6173

In the SNR as a quantitative and qualitative measure in the context of the IoT as a quality of services issue, there is an important problem. A value below 12 indicates a serious noise problem in the data. A value above 20 is a satisfactory state and a value greater than 30 is the appropriate amount. In fact, the higher the index, the better, is a better signal in the original data. The signal-to-noise rate is defined as the signal strength rate to the noise power ratio, which is according to equation (8).

$$SNR = \frac{P_{signal}}{P_{noise}} \quad (8)$$

P is the mean value of the signal strength. Due to the fact that most signals have a dynamic range, they are logarithmically denoted by dB, which is given by equation (9) for the power signal and equation (10) for the noise signal.

$$P_{signal,dB} = 10log_{10}(P_{signal}) \quad (9)$$

$$P_{noise,dB} = 10log_{10}(P_{noise}) \quad (10)$$

IV. Simulation and Results

MATLAB used as simulation platform to implement the proposed approach. Due to simplicity of coding in MATLAB, it used instead of powerful simulation tools such as NS-3, NS-2, OPNet, OMNet++, GloMoSIM, JSIM, IoTSIM and so on. Also some evaluation criteria used to guarantee the proposed approach and comparison to other methods.

Initial structure for IoT is necessary in simulation. It is essential to provide a basic dimension to the IoT. Defining parameters in simulation worlds is too important to examine the proposed approach and results in a concrete manner in order to obtain assumptions and goals from it. In the simulation world, defining the dimensions of a grid means that it will not be covered outside of it, but in the real world, using the tools and the equipment, the uncovered points can be partly close to the coverage range. The Table (2), shows the initial values for the general settings of the IoT, including the number of sensor nodes (which includes equipment such as Bluetooth, etc. for communication with the IoT), sampling rate, primary energy, network dimensions, etc. and adjusts their initial parameters with empirical visibility.

TABLE 2. INITIAL SETTINGS OF IOT NETWORK

X and Y dimension supported in IoT area	100×100 m^2
Sensor nodes number in IoT	300 nodes
Package number in IoT to transmit	100 packages
Maximum size of packages in IoT to transmit	100 MB
Minimum size of packages in IoT to transmit	1 KB
Sampling time in seconds	8 seconds
Initial SNR in transmitting and receiving data	5 dB
SNR range based on drop in transmitting and receiving data	20 – 20 dB
Nodes deployment in IoT environment	Random
Modulation for transmitting and receiving data	BPSK
Block Chain initial threshold in fault tolerance time	0.1
Energy of each nodes	1 Joule
Total energy of IoT	300 nodes × 1 Joule = 300 Joule

Probability of detection and data privacy considered in IoT-edge-fog gateway connected to LTE and 5G which presented in Fig. 5.

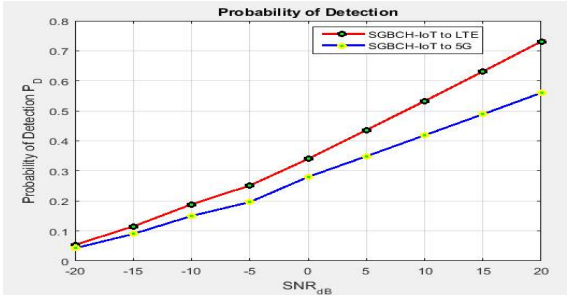

Fig. 5. Probability of detection output for encrypted data to data privacy in gateway

According to Fig. 3, it is clear that the proposed approach SGBCH-IoT connected to LTE has a better probability of detection capability than SGBCH-IoT connected to 5G in the gateway. The highest probability of detection is the superiority criterion. The proposed method has added more capabilities to the SGBCH-IoT connected to 5G to maintain the confidentiality of data at the time of their probability of detection. Also, Probability of Miss Detection (PMD) in encryption consider (which could be due to the existence of severe noise and interruption in the IoT-based edge-fog computing) which can be affect in lost data rate and preventing its privacy. The lower probability of miss detection can be guaranteed to improve the loss data rate. Fig. 6. represent the probability of miss detection of SGBCH-IoT connected to LTE and 5G.

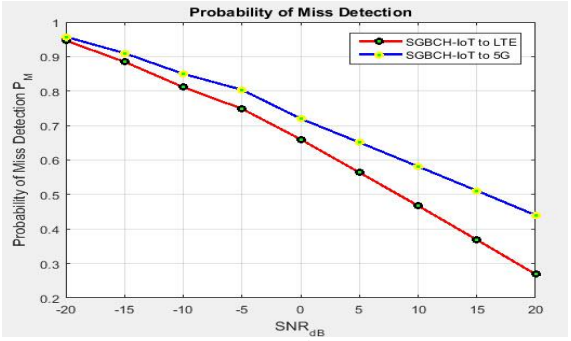

Fig. 6. Probability of miss detection

It is shown in Fig. 4., that the proposed approach SGBCH-IoT connected to LTE has the better probability of miss detection than the SGBCH-IoT connected to 5G in the gateway. The structure of DTLS and FSK in this section have also had a significant impact on the SGBCH-IoT connected to 5G during the encryption of data in the BPSK-based messaging channel. The result of this section shows that the proposed SGBCH-IoT connected to LTE method has a functional superiority in minimizing the probability of miss detection. This can certainly prove to be as low as possible to reduce the data loss rate in transmitting them from origin to destination in the context of the IoT-based edge-fog computing gateway. Fig. 7. shows the data loss rate of SGBCH-IoT connected to LTE and 5G.

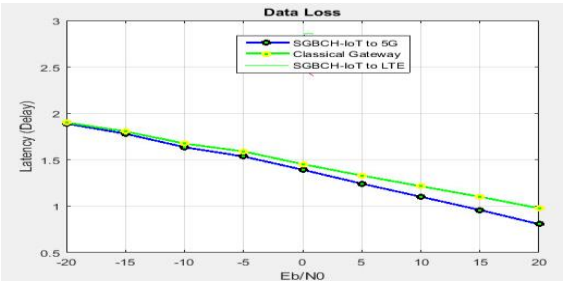

Fig. 7. Data lose rate

Based on Fig. 7 and the previous description, the proposed approach SGBCH-IoT connected to LTE has equal data loss rate with the classical gateway model, but SGBCH-IoT connected to 5G is lower than that. The combined structure of the DTLS and FSK in this section, as well as the probability of miss detection, have shown their high ability. It should be noted that the data loss rate in the SGBCH-IoT connected to 5G communication is desirable, but may be different at the time of encryption in this study with 8 bits of information in the BPSK modulation-based communication channels. It should be assumed that the upcoming chart proves this. In the following, after creating a safe environment, quality of services criteria to evaluation consider. Initially, it is considered that the delay in Fig. 8. which represent the delay after applying the proposed approach for the secure gateway on the IoT-based edge-fog computing compared to the SGBCH-IoT connected to LTE and 5G and the classic gateway.

IEEE Office - SEET Complex, Federal University of Technology, Owerri, Nigeria, https://aeuso.org
EISSN: 2305-0543, PISSN: 2411-6173

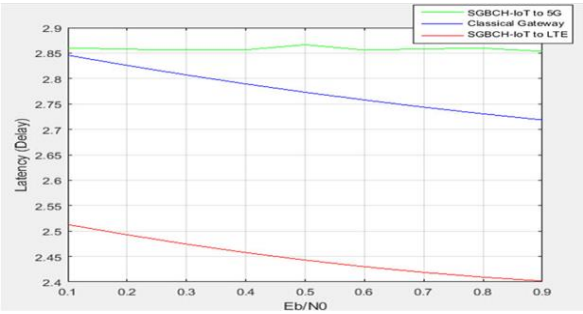

Fig. 8. Delay of proposed approach in comparison to others

In Fig. 8, the delay diagram of the proposed red-color scheme is characterized by a lower delay rate than the previous two methods including the SGBCH-IoT connected to 5G and the classical gateway in the same conditions. In the following, examination of the amount of data transmitted in bits considered. If the environment is secure, the data is decoded by the DTLS and FSK-based encryption, in the sender, encrypted and in the receiver. The results of the throughput in the IoT-based edge-fog computing gateway for SGBCH-IoT connected to LTE and 5G represent in Fig. 9.

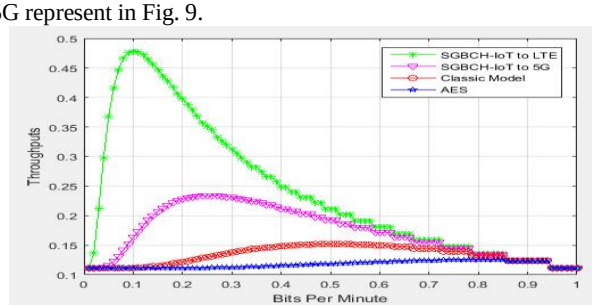

Fig. 9. Throughput rate for proposed approach in comparison to others

According to Fig. 9. which is compared with the SGBCH-IoT connected to 5G, the classic model and the use of the AES algorithm, it is shown that the green graph has a higher permeability rate than the other methods. But over time, this rate is declining and is roughly the same in other ways. Fig. 10, shows the proposed ROC approach in comparison to SGBCH-IoT connected to 5G, the classic model and the use of the AES algorithm.

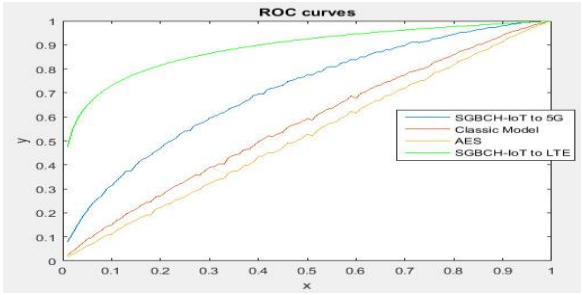

Fig. 10. Proposed method ROC curve in comparison to other methods

Based on Fig. 10. represented that proposed method has better ROC curve in comparison to others. A secure gateway created based on DTLS and FSK in IoT-based edge-fog computing which represented that this gateway has good performance of quality of services to manage resources.

Conclusion

In this research, the Secure Gateway Block Chain Edge-Fog in IoT or SGBCH-IoT introduced. The performance of SGBCH-IoT in IoT-based edge-fog computing environment was tested in simulation. DTLS and FSK-based encryption operations are performed on a Block Chain platform in the structure of this gateway. The flexibility and improvement of the SGBCH-IoT connected to LTE technology vs. SGBCH-IoT connected to 5G technology efficiency can be determined by considering resource management and quality of service criteria including delay, throughput, probability of detection, the probability of miss detection and data loss rate. Of course, as improvements are made in these cases, there may be some other weaknesses that can be considered as their future solutions.

References

[1] Hugh Boyes, Bil Hallaq, Joe Cunningham, and Tim Watson. The industrial internet of things (IIoT): An analysis framework. Computers in Industry, Volume 101, Pages 1-12, October 2018.

[2] Kewei Sha, Wei Wei, T. Andrew Yang, Zhiwei Wang, and Weisong Shi. On security challenges and open issues in Internet of Things. Future Generation Computer Systems, Volume 83, Pages 326-337, June 2018.

[3] Libing Wu, Biwen Chen, Kim-Kwang Raymond Choo, and Debiao He. Efficient and secure searchable encryption protocol for cloud-based Internet of Things. Journal of Parallel and Distributed Computing, Volume 111, Pages 152-161, January 2018.

[4] C. Cachin and M. Vukoli`c, "Blockchain consensus protocols in the wild," 2017.

[5] M. Castro and B. Liskov, "Practical byzantine fault tolerance and proactive recovery," in Proceedings of the Third Symposium on Operating Systems Design and Implementation, Vol. 20, ACM, November 2002.

[6] D. Mazi`eres, "The stellar consensus protocol: A federated model for internet-level consensus," tech. rep., Stellar Development Foundation, 2016.

[7] "A next-generation smart contract and decentralized application platform," 2017. https://github.com/ethereum/wiki/wiki/White-Paper.

[8] P. Windley and D. Reed, "Sovrin: A protocol and token for selfsovereign identity and decentralized trust," tech. rep., Sovrin Foundation, 2018.

[9] E. Ben-Sasson, A. Chiesa, C. Garman, M. Green, I. Miers, E. Tromer, and M. Virza, "Zerocash: Decentralized anonymous payments from bitcoin," in IEEE Symposium on Security and Privacy, 2014.

[10] "Hyperledger fabric," 2015. https://hyperledger.org/projects/fabric.

[11] Y. Lewenberg, Y. Sompolinsky, and A. Zohar, "Inclusive block chain protocols," in Financial Cryptography, pp. 528–547, 2015.

[12] S. Popov, "The tangle," tech. rep., IOTA, 2017.

[13] E. Kokoris-Kogias, P. Jovanovic, L. Gasser, N. Gailly, E. Syta, and B. Ford, "Omniledger: A secure, scale-out, decentralized ledger via sharding," IACR Cryptology ePrint Archive, vol. 2017, p. 406, 2017.

[14] A. E. Gencer, R. van Renesse, and E. G. Sirer, "Service-oriented sharding with aspen," 2016.

[15] M. Al-Bassam, A. Sonnino, S. Bano, D. Hrycyszyn, and G. Danezis, "Chainspace: A sharded smart contracts platform," 2017.

[16] L. Luu, V. Narayanan, C. Zheng, J. Bajewa, S. Gilbert, and P. Saxena,"A secure sharding protocol for open blockchains," in Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, no. 17-30 in CCS -16, 2016.

[17] Moustafa M. Nasralla, Nabeel Khan, and Maria G. Martini. Content-aware downlink scheduling for LTE wireless systems: A survey and performance comparison of key approaches. Computer Communications, Volume 130, Pages 78-100, October 2018.

[18] L. R. Priya, and K. Rubasoundar. LTE: An Enhanced Hybrid Domain Downlink Scheduling. Cognitive Systems Research, In press, accepted manuscript, Available online 18 July 2018.

[19] Piergiuseppe Bettassa Copet, Guido Marchetto, Riccardo Sisto, and Luciana Costa. Formal verification of LTE-UMTS and LTE–LTE handover procedures. Computer Standards & Interfaces, Volume 50, Pages 92-106, February 2017.

[20] Divya Prerna, Rajkumar Tekchandani, and Neeraj Kumar. Device-to-device content caching techniques in 5G: A taxonomy, solutions, and challenges. Computer Communications, Volume 153, Pages 48-84, 1 March 2020.

[21] Pengcheng Wei, and Zhen Zhou. Research on security of information sharing in Internet of Things based on key algorithm. Future Generation Computer Systems, In press, accepted manuscript, Available online 12 May 2018.

[22] Qi Han, Yinghui Zhang, and Hui Li. Efficient and robust attribute-based encryption supporting access policy hiding in Internet of Things. Future Generation Computer Systems, Volume 83, Pages 269-277, June 2018.

[23] Jungyub Lee, Sungmin Oh, and Ju Wook Jang. A Work in Progress: Context based Encryption Scheme for Internet of Things. Procedia Computer Science, Volume 56, Pages 271-275, 2015.

[24] Sabrina Sicari, Alessandra Rizzardi, Daniele Miorandi, and Alberto Coen-Porisini. REATO: REActing TO Denial of Service attacks in the Internet of Things. Computer Networks, Volume 137, Pages 37-48, 4 June 2018.

[25] Xuanxia Yao, Zhi Chen, and Ye Tian. A lightweight attribute-based encryption scheme for the Internet of Things. Future Generation Computer Systems, Volume 49, Pages 104-112, August 2015.

IEEE Office - SEET Complex, Federal University of Technology, Owerri, Nigeria, https://aeuso.org
EISSN: 2305-0543, PISSN: 2411-6173

[26] Abhijan Bhattacharyya, Tulika Bose, Soma Bandyopadhyay, Arijit Ukil, and Arpan Pal. LESS: Lightweight Establishment of Secure SessionA Cross-Layer Approach Using CoAP and DTLS-PSK Channel Encryption. 2015 29th International Conference on Advanced Information Networking and Applications Workshops, Pages 682-687, 2015.

[27] Kewei Sha, Wei Wei, T. Andrew Yang, Zhiwei Wang, and Weisong Shi. On security challenges and open issues in Internet of Things. Future Generation Computer Systems, Volume 83, Pages 326-337, June 2018.

[28] Arbia Riahi Sfar, Enrico Natalizio, Yacine Challal, and Zied Chtourou. A roadmap for security challenges in the Internet of Things. Digital Communications and Networks, Volume 4, Issue 2, Pages 118-137, April 2018.

[29] News. Securing the Internet of Things. Network Security, Volume 2018, Issue 1, Page 4, January 2018.

[30] Priyan Malarvizhi Kumar, and Usha Devi Gandhi. Enhanced DTLS with CoAP-based authentication scheme for the internet of things in healthcare application. Springer, J Supercomput DOI 10.1007/s11227-017-2169-5, 2017.

[31] Roberto Morabito, Riccardo Petrolo, Valeria Loscrì, and Nathalie Mitton. Reprint of : LEGIoT: A Lightweight Edge Gateway for the Internet of Things. Future Generation Computer Systems, Volume 92, Pages 1157-1171, March 2019.

[32] Roberto Morabito, Riccardo Petrolo, Valeria Loscrì, and Nathalie Mitton. Reprint of : LEGIoT: A Lightweight Edge Gateway for the Internet of Things. Future Generation Computer Systems, Volume 92, Pages 1157-1171, March 2019.

[33] Yuan Ai, Mugen Peng, and Kecheng Zhang. Edge computing technologies for Internet of Things: a primer. Digital Communications and Networks, Volume 4, Issue 2, April 2018, Pages 77-86.

[34] Yan Sun, Fuhong Lin, Nan Zhang. (2018). A security mechanism based on evolutionary game in fog computing. Saudi Journal of Biological Sciences, Vol. 25, Issue 2, pp. 237-241.

[35] Jianbing Ni, Kuan Zhang, Xiaodong Lin. (2017). Securing Fog Computing for Internet of Things Applications: Challenges and Solutions. IEEE Communications Surveys & Tutorials, Vol. 20, Issue 1.

[36] Binara N. B. Ekanayake, Malka N. Halgamuge, Ali Syed. Review: Security and Privacy Issues of Fog Computing for the Internet of Things (IoT). Cognitive Computing for Big Data Systems over IoT, pp. 139-174.

[37] R. Rapuzzi, and M. Repetto. (2018). Building situational awareness for network threats in fog/edge computing: Emerging paradigms beyond the security perimeter model. Future Generation Computer Systems, Vol. 85, pp. 235-249.

[38] Cong Zuo, Jun Shao, Guiyi Wei, Mande Xie, and Min Ji. (2018). CCA-secure ABE with outsourced decryption for fog computing. Future Generation Computer Systems, Vol. 78, Part 2, pp. 730-738.

[39] Rodrigo Roman, Javier Lopez, and Masahiro Mambo. (2018). Mobile edge computing, Fog et al.: A survey and analysis of security threats and challenges. Future Generation Computer Systems, Vol. 78, Part 2, pp. 680-698.

[40] Ola Salman, Imad Elhajj, Ali Chehab, and Ayman Kayssi. (2018). IoT survey: An SDN and fog computing perspective. Computer Networks, Vol. 143, pp. 221-246.

[41] Alexandre Viejo, and David Sánchez. (2018). Secure and Privacy-Preserving Orchestration and Delivery of Fog-Enabled IoT Services. Ad Hoc Networks, In press, accepted manuscript, Available online 15 August 2018.

[42] Ismail Angri, Abdellah Najid, and Mohammed Mahfoudi. (2019). Available Bandwidth and RSRP Based Handover Algorithm for LTE/LTE-Advanced Networks Tested in LTE-Sim Simulator. International Journal of Electronics and Telecommunications, Vol. 65, No 1, pp. 85-93.

[43] Mohammed Mahfoudi, Moulhime El Bekkali, Abdellah Najd, M. El Ghazi, and Said Mazer. (2015). A New Downlink Scheduling Algorithm Proposed for Real Time Traffic in LTE System. International Journal of Electronics and Telecommunications, Vol. 61, No 4.

[44] Bujar Krasniqi, Blerim Rexha, and Betim Maloku. (2018). Energy Efficiency Optimization by Spectral Efficiency Maximization in 5G Networks. International Journal of Electronics and Telecommunications, Vol. 64, No 4, pp. 497–503.

[45] Faizan Qamar, MHD Nour Hindia, Talib Abbas, Kaharudin Bin Dimyati, and Iraj S. Amiri. (2019). Investigation of QoS Performance Evaluation over 5G Network for Indoor Environment at Millimeter Wave Bands. International Journal of Electronics and Telecommunications, Vol. 65, No 1, pp. 95-101.

[46] Muhammad Aziz ul Haq, and Sławomir Kozieł. (2017). Design Optimization and Trade-Offs of Miniaturized Wideband Antenna for Internet of Things Applications. Metrology and Measurement Systems, Vol. 24, No. 3, pp. 463–471.

[47] M. Głąbowski, S. Hanczewski, M. Stasiak, M. Weissenberg, P. Zwierzykowski, and V. Bai. (2020). Traffic Modeling in Industrial Ethernet Networks. International Journal of Electronics and Telecommunications, Vol. 66, No. 1, pp. 145-153.

IEEE Office - SEET Complex, Federal University of Technology, Owerri, Nigeria, https://aeuso.org
EISSN: 2305-0543, PISSN: 2411-6173