I.J. Wireless and Microwave Technologies, **2023, 3, 1-13**
Published Online on June 8, 2023 by MECS Press (http://www.mecs-press.org/)
DOI: 10.5815/ijwmt.2023.03.01

Privacy Enhancing for Fog Computing based - IoT

Samaa Y. Tarabay*
Mansoura University / Communication and Electronics Engineering Department, Mansoura, 35516, Egypt
E-mail: Samaayasser92@gmail.com
ORCID iD: https://orcid.org/0000-0002-6926-2346
*Corresponding Author

Ibrahim Yasser
Mansoura University / Communication and Electronics Engineering Department, Mansoura, 35516, Egypt
E-mail: ibrahimyasser14@gmail.com
ORCID iD: https://orcid.org/0000-0001-5411-2567

Ahmed S. Samra
Mansoura University / Communication and Electronics Engineering Department, Mansoura, 35516, Egypt
E-mail: shmed@mans.edu.eg
ORCID iD: https://orcid.org/0000-0003-1801-5895

Abeer T. Khalil
Mansoura University / Communication and Electronics Engineering Department, Mansoura, 35516, Egypt
E-mail: abeer.twakol@mans.edu.eg
ORCID iD: https://orcid.org/0000-0003-4223-2144

Received: 14 November, 2022; Revised: 22 December, 2022; Accepted: 03 March, 2023; Published: 08 June, 2023

Abstract: With the massive inflation of newly developed technologies, recourse to data has become a necessity in light of the current inflation and excessive need dominating the world and developed societies. According to the control of millions of smart devices and sensors connected to an interconnected and controlled automated system within installed scales due to the services provided by IOT devices through the created fog layer that connects the cloud centers and those devices, in addition, very large amounts of that data including public and private are passed through the connection of Internet of Things devices to each other. Smart and advanced networks as one of the fog computing applications play a prominent and accurate role in the infrastructure for reliable and sound data transmission. Accordingly, the process of data aggregation is an important and common matter in the world of fog-enhancing Internet of Things, so preserving the privacy of that data is a matter of concern, and based on this principle, we propose in this paper a model for data aggregation that maintains privacy using a foggy computing environment called PPFDA (privacy preserving based- fog computing data aggregation). We use in our scheme DF homomorphic cryptosystem as it consider one of the aggregation models that ensures the privacy purpose. The theoretical results and analyzes show that our design is ensuring the privacy of data during collection using an algorithm of DF. The results confirm that the proposed scheme achieves security and privacy purposes in modern network systems for the Internet of things based in fog computing. In addition, it contributes significantly to the efficient performance of storage operations.

Index Terms: Fog computing, Internet of things (IOT), Data security & Privacy, Aggregation, DF.

1. Introduction

In recent years, the devices used in the era of modern technology have adopted a rapid and huge prosperity, as these devices have formed collective computing and a connected network governed by many communication systems under the term "Internet of Things" [1]. Where all smart devices and sensors were united and were linked to each other to set them to implement various services and establish service applications (such as medical services and health care follow-up, Smart Parking, smart traffic, etc.), which the human person is subject to daily until it became part of his

practical and daily uses, that led to technological development and became the main feature in developed societies as a factor to attraction of IOT applications continuously and quickly [1,2].

Hence, the principle of collecting data of this technology is presented due to the nature of its performance, as Internet of things devices perform more continuous processing operations, which often have unrestricted access to private information [1,3]. Thus, all of this technology has become under the control of many risks and problems related to the security and privacy of users and making them vulnerable to violation by Internet attackers. In view of the huge expansion in the huge amounts of data and various information about the service users, it is necessary that the system requires the ability to have a high storage capacity to withstand this amount of data in addition to its need for processing operations and getting various decisions and necessary actions towards that data [4]. Accordingly, the concept of fog computing platform began to emerge as an extended structure for cloud computing and to resort to it. As a technology that can be accommodated for this development and to deal with the volume of devices and data exchanged between smart systems. This layer has led to the decentralization of the data centers due to its staying much closer to the IOT devices [5, 6]. Fog computing has almost jumped to become an urgent need for individuals and users, in addition to facilitating millions of services for institutions and companies based on such technology. Fog technology has many advantages that have had the largest share in supporting the world of technology and big data [7]. To mention some of them: real-time application services, low latency, geographical awareness, data aggregation and privacy specially in smart grid networks, support for mobility, less congestion in terms of network and in addition to being able to process operations for a large number of nodes, where distributed fog nodes can aggregate local data received from different devices used by different customers and users before it is transferred to the cloud, so cloud servers don't have to deal with massive amounts of information. Thus reducing bandwidth and cost unlike cloud computing, moreover, the quality of improved service for mobile phone users and enhanced network efficiency [7]. Thus, all of this supports that fog computing will adopt the services of IOT devices more and more efficiently than cloud computing [8, 9]. We will present in our work a model that achieves preserving privacy for fog medium through the principle of data aggregation based on the Internet of Things. “Fig. 1,” shows the fog computing architecture where fog medium are existing between the cloud and the smart cluster head, which makes the system and the model have the developed capabilities added to the fog environment.

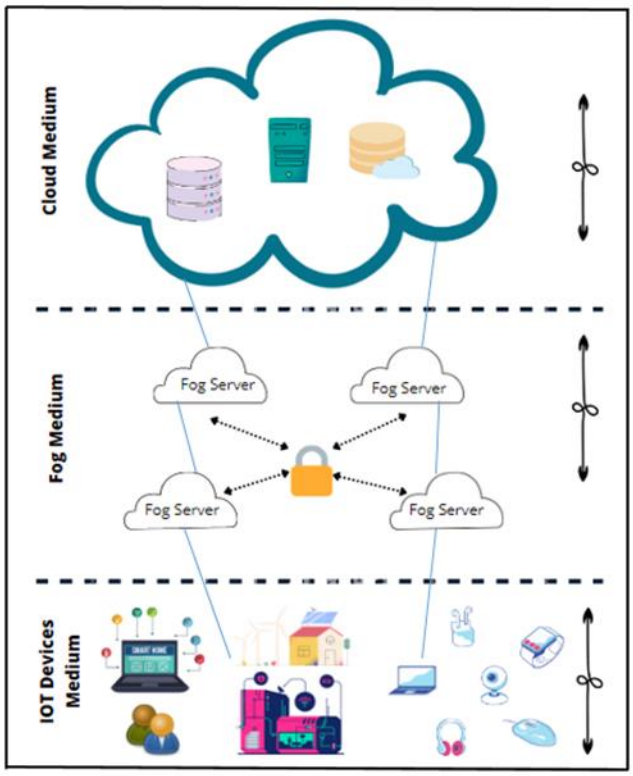

Fig. 1. Fog Computing Architecture

1.1 Related Work

Cloud computing was a good technology for modern systems such as smart grid systems, but with the modern technological leap and the emergence of the world of the Internet of Things, the foggy environment has overcome cloud computing significantly and has become the most promising platform as an ideal solution for such modern systems. But the file of security and privacy is one of the thorny issues that are still being addressed in the first lists in the world of networks, smart and modern technology. Accordingly, a lot of research has been conducted to cover and provide

solutions in such issues that serve this type of system and its privacy, and we will present a brief summary of some of these research works. Dhiah El Diehn [10] designed a model that embodies the preservation of the privacy of cloud-based fog data, where fog was used to secure user data and confidentiality by concealing identities via a reference key. This methodology ensured that users' data and information were not disclosed. An analysis and conclusion base was created for the proposed model to evaluate its performance. Khalid, Tauqeer, et al. [11] proposed a deep discussion where attention was drawn to the mechanisms used in privacy issues in foggy computing and access control processes. The author also touched on many algorithms and processors that were listed by many authors and advanced research in recent years. On the other hand, there are some researches based on the so-called aggregation precept to achieve privacy in the Internet of Things, where a lot of research uses homomorphic encryption methods in order to enhance the principle of privacy. There are many common schemes that are subject to such methods and technologies, which have a large and effective place in many applications related to user consumption such as smart grids, energy consumption, as well as applications related to smart traffic lights and other services. In our work, as we will rely heavily on such kind of schemes. Lu, Rongxing, et al [12] presented lightweight proposal that promotes the development of IOT data privacy. The author relied on the use of Paillier encryption technique, Chinese Remainder Theorem, and one-way hashing chain technology, in order to show a hybrid scheme for data aggregation purposes for the heterogeneous Internet of Things. Moreover, he also mentioned the idea of early filtering by injecting fake data at the edges of the network to ensure authentication and refuse to attack the whole system. The privacy analyzes showed that this proposal led to accurate and improved results for the previous systems. Zhu, Liehuang, et al. [13] presented a smart architecture for the fog network, with some security and privacy issues mentioned. In the article, the author proposed a schema to reinforce authentication during data aggregation in smart fog systems. He used here two types of signatures, one randomizable and short, and the other is blind, in order to achieve anonymous and conditional authentication. It relies on aggregation data on one of the well-known symmetric encryption methods, which is the homomorphic Paillier. Guan, Zhitao, et al. [14] designed an anonymous proposal to preserve privacy based on homomorphic encryption, as the author relied in his work on anonymity through the use of pseudonyms, which are subject to updates individually. Aggregating data through the Paillier algorithm had the share and credit for achieving the best results and their effectiveness well, in addition to being aware of real-time applications. Okay, F. Y., & Ozdemir, S, [15] this paper presents a Privacy-Added Secure Data Collection (SDC) scheme from Domingo-Ferrer's new Fog Computing (FCSG). Where this collection process is done at the level of fog for the purposes of reducing the burden of costs and also reducing the volume of data. The protocol used achieved complete confidentiality of the data with an emphasis on the storage process and ensuring the low costs used compared to other solutions. Accordingly, due to the hierarchical structure of smart systems based on foggy computing, the results show that protocols based on additive homomorphic encryption achieve the privacy of collected data in addition to the efficiency of storage and the size of packets sent to the central cloud. Alabdulatif, et [16] presented a paper dealt with the ability to develop from the DF (Domingo-Ferrer) diagram to be able to deal with the maximum and minimum limits in the same process, and the performance of the experiment was effective to run this proposal in lightweight applications due to the effectiveness of its accuracy and results. In [17] Şimşek, Mehmet Ulvi, et al. This paper deals with the applications of smart grids and the privacy of data consumed through TPS3 security protocol and Shamir Schemes for Secret Sharing (SSS). The system used in this paper supports the credibility through the large number of messages obtained from DCS in each of the two schemes. The results showed that the protocol is highly effective in ensuring consumer privacy protection from external HBC attacks. In [18] the author design a privacy scheme was designed using aggregation algorithms and the proposed protocol bet against collusion data aggregation model for dynamic group between fog and cloud servers, as well as the ability of cloud servers to recover data and compute collections while ensuring end devices and privacy protections. The author also included limiting the bandwidth by filtering redundant and useless data. In addition to the principle of authentication. This design does not support handling of complex data.

Table 1. The abbreviation in our work

Abbreviation	Definition
DAS	Data aggregation security
IOT	Internet of things
SCH	Smart cluster head
CS	Cloud server
Fs	Fog server
TN	Terminal node
HET	Homomorphic Encryption Technique
DF	Domingo Ferrer
ESP	External service provider
HBC	Honest but curious

1.2 Problems Statement

On the modern technological scale and after highlighting the fog medium, the data circulating in such applications that largely deal with foggy services can be categorized as public data and private data. General data is mostly non-sensitive surface information that refers to the total data consumed, for example, such as the application of smart homes that contain various smart devices. As for private data, it is confidential and highly sensitive data that cannot be

identified, and it is represented in the precise data that is unique to each user according to his specific consumption of the device or application used in his case, in addition to this data also includes important and sensitive personal information. Of course, this data must be withheld and not identified by the hacker attackers or by the party responsible for the service and application operators, as the disclosure of such data is allowed by the legitimate users of this service (smart home residents for example), thus ensuring the privacy of the data emitted from Those smart devices.

Of course, millions of smart devices produce very large and huge amounts of data that need continuous processing and analysis, and thus a huge storage capacity that contains this overwhelming amount of data and collecting it continuously without a defect. And that is through cloud services, where the user can access his data, analyzes and receive his detailed reports from the cloud centers, which may constitute a very large onus in addition to the great complexity that cloud centers suffer from. Therefore, the cloud was looked at in the face of default from this aspect, and the load was jumped on fog computing to cover this hiatus and to meet the call towards the requirements of processors and storage, knowing that not all security problems of the distributed fog structure were ended due to the novelty of the model. Hence the urgency for the existence of methods that contributes to compressing, reducing and aggregating data in order to control the quality and efficiency of the system.

In the scheme proposed in this paper, we contribute to solving this problem by using DAS schemes that ensure the added privacy and confidentiality of data through homogeneous encryption based on data aggregation. These operations are represented in executing a concatenation of commands on the ciphered data, without revealing the privacy and intrusion on its details.

1.3 Contributions goal and design road-map

In this part, we will present the contributions that we will make through the proposed in brief points as follows:

- The model presents a proposed architecture that achieves the precept of data aggregation from the motive of maintaining data privacy against third parties, where fog servers are distributed between (CS) and smart clusters head (SCH), as these servers contribute to reducing traffic congestion, organizing communication effectively and accurately compared to cloud-based models due to the low latency of fog server as a result of proximity property.
- It is used two efficient symmetric encryption technique in the system. One of them is one of the protocols that used in DAS protocols "Domingo-Ferrer" (and the other technique is based on chaotic map and space filling curve (detailed of this technique will described later in another article).
- The proposed protocol utilizes DF method in a multilayer architecture that simplify data collecting on the fog computing using HET.
- The proposed model ensures the data privacy and security, and as well minimizes the quantity of data that stored in CS.
- The result shows that privacy analysis verifies through our proposed model as we will show later.

The rest of our article is built as follows: section 2 will present overview for fog computing architecture including its layer and features. In section 3 will be presented for our proposed model and step techniques in details. While part 4 deals with the performance evaluation and expected results of the proposed model. Conclusion and future work will be shown in part 5.

2. Fog Computing Architecture

A standard architecture or a classic model of fog computing environment should be as the one in “Fig. 1,”. Where the foggy structure includes devices based on secure network connections with each other, such as routers, servers, proxy servers, encryption devices, etc. [11]. And the establishment of these devices in a location close to the IOT devices in order to help it to link with the server provider through this middle fog layer [19,20], In what follows, a brief characterization of every layer is presented.

2.1 IOT Device Layer

This layer refer to a several end devices which called Internet of Things devices from which the user derives many services through huge amounts of service-provided applications [21].Also they are known as "terminal Node" (TN). These devices skimp on their ability to power and limiting in their resources, and therefore still fail to maintain the privacy and security of users. According to these devices' primary role in collecting consumer data, this data is likely to be invaded and violated by attackers or who wish to explore more about the nature and data of users and their various personal records. [18] Therefore, these devices were in need of a better and more advanced computing (fog computing) and an improvement in terms of security and privacy protection. Therefore, the fog computing was keen on extending users to the principle of authentication by documenting their data, approving their records, and establishing secure communication channels in the entire system[22]. In addition, IOT devices are unable to store efficiently and are stored only temporarily. Accordingly, the fog layer handles the processing and analysis of data sent from IOT devices, which

makes the technology of these devices and their application practical and more applicable because they do not need large storage capability and therefore do not cause a great danger in the event of theft the data [22,23].

2.2 Fog layer

The fog layer, which is a layer that acts as a communication hub between the IOT devices layer and the central cloud, and includes a large number of foggy nodes, which are represented in devices such as routers, servers, servers, etc., and the role of this layer is formed in the processes of processors, data analysis and approval of users wanting to join the node through the principle of authentication and receiving their data through Internet of Things devices [24].

2.3 Cloud layer

The cloud layer, which is the upper layer of the fog layer, where the centers and cloud servers are stationed for permanent storage of data sent from the fog, in addition to the data analysis and processing service [24,25].

2.4 Fog Computing Characteristics

Due to fog computing has had a great credit for filling the hole between the central cloud and IOT devices by using local servers [26]. It has many advantages that surpassed the cloud environment due to its characteristics that greatly facilitated data handling, in addition to directing it towards trying to preserving the privacy of its data and users, we will present some of these characteristics in the following:

- Locations: It includes distributing fog servers in successive stations so that they are aware of the locations of IOT devices connected to the actual network. Thus, it ensures the quality of the transmitted data and that related to location-based services [26, 27].
- Latency: A prominent feature of the fog environment is the provision of latency, whereby the data can be managed and processed in a user-close location without the interference of the cloud, thus reducing network congestion and faster response time for real-time applications [27]. Therefore, reducing the response time is absolutely necessary in order to avoid any failure that may occur in one way or another.
- Nearness: Foggy computing allows the advantage of being close to the end customers, and thus allowing the data and users to be dealt with closer and better, which simplifies the extraction of important and useful information [21].
- Privacy: Fog computing contributes to controlling data privacy, as a result of providing and activating the processing feature without referring to the cloud in addition to latency. Fog servers help in the ability of fog service users to store their data temporarily by ensuring the privacy of that information and speed of response. So we can analyze sensitive data locally and that's ensure privacy from attacks [28].
- Aggregation operation: Foggy computing has the ability to carry out operations of so-called aggregation operations, due to the difficulty of routing all relevant data from the Internet of Things individually or separately [15], so it requires the provision of the aggregation feature, and accordingly it reduces network traffic and reduces the burden on communication channels, especially in applications associated with complex services and big data [13-15, 28].
- Mobility Support: Fog computing services are not limited to fixed stations only, but also have the ability to deal with applications or mobile stations, so they support ease of movement and mobility [28, 29].

2.5 Background of fog Applications Security

The sweeping and emerging development in modern and advanced fog systems and applications has gained a prominent position, greater control effectiveness and guaranteed reliability [19]. These developments and technologies follow security holes that hinder systems and lead them to unreliability for all their users and those in charge of them. Therefore, considering the security of these technologies is extremely important, given the seriousness of these vulnerabilities in the system. Accordingly, these systems require many security factors that provide the system with security and privacy [20, 21]. We will present some of the general and main points of the requirements below as shown in “Fig. 2,”

1. Availability: If the availability of the network is not confirmed, it affects the disruption of data confidentiality and its proper flow. The availability process resists denial-of-service (DOS) attacks that help corrupt or block data. Where it is necessary to make the data actually available in the event that users need to access it [30].
2. Integrity: It means that data send and received in the same format which cannot be modified or corrupted from unwanted tampering during transfer. Also it disallows unauthorized access to sensitive data through fake users and not authorized to use. It guarantees data reliability, effectiveness, and protection of accuracy. As frowning with the data and changing its features may exhaust the entire system and make it subject to wrong and illogical decisions and orders [31].
3. Confidentiality: This feature closely parallels the principle of privacy. Where the data is made available only to the legitimate users of it and withheld from the fake. Users' data must be covered and completely confidential due to the sensitivity of its content because it contains sensitive and personal information of its

users and is not subject to disclosure or violation. Some attackers are trolling to find out the activities of legitimate users and the extent of their use in certain fields and applications. Therefore, it is imperative for the system to create a strong and supported protection to maintain the confidentiality and privacy of that data [25, 32].

4. Authentication: it is a controlling access privileges and confirmation that the two parties between whom communication takes place are the original parties and the data is intended to be communicated to them without any forgery occurring to any of the parties as legitimate users as it builds the user's trust and protects from Man in the Middle Attack [5,7].

Fig. 2. Fog computing security requirements graph

3. Privacy-Preserving Data Aggregation Model

In this part, the proposed model in our work and its detailed steps will be addressed also the clarification of the general scheme will be presented.

3.1 Proposed Scheme and Assumptions

The proposed model presented is a structure consisting of four consecutive levels. And each level leads a set of independent functions from the other, thus creating an integrated system in working with the cooperation of each layer with the other. The first level includes Internet of Things devices, which consist of millions of devices used in communication operations and responsible for the transmission of user's data, while the second layer includes the SCH, which receives data from Internet of things devices. As each SCH is connected to the FS, which is stationed in the third layer in which processing operations and caching services can be performed [15]. And finally, these fog servers send the final data to the central cloud servers, where the data is running by ESP. Figure (3) below show our flowchart of our proposed work.

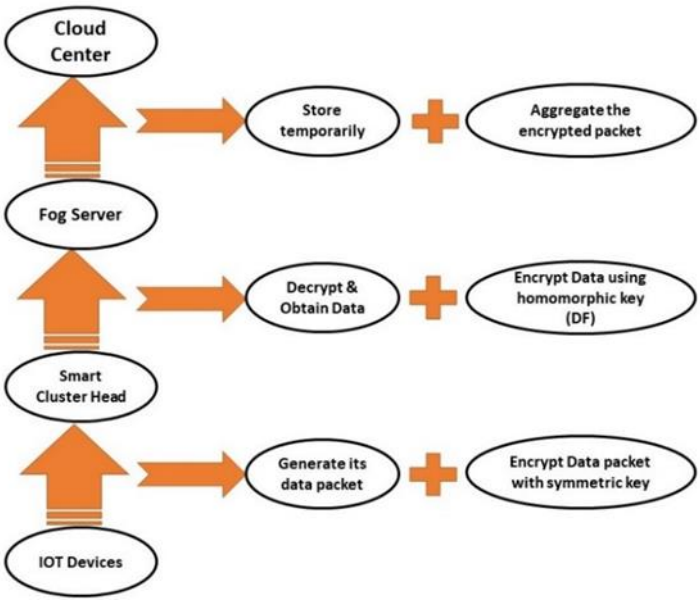

Fig. 3. Proposed Model flowchart

Table 2. Assumptions

Assumption 1	Data is stored in fog servers temporarily, and sent to cloud centers to be stored permanently.
Assumption 2	The authentication process is done on each Internet of Things device before joining the network or system, as each device is independent.
Assumption 3	Users can search for their close fog servers to review their data.
Assumption 4	We use 200 numbers of IOT devices and 100 numbers of IOT requests.
Assumption 5	Cloud center and Fog server operators are both independent.
Assumption 6	The positions of devices in our simulation is as follow: -Cloud:500,900 -Fog server1: 250,700 / Fog server2: 500,700 / Fog server3: 750,700 -SCH1: 250,500 / SCH2:500,500 / SCH3: 750,500
Assumption 7	Before sending data by IOT devices to SCH, the data is encrypted using symmetric key based algorithm (the detailed of this step is not include in our article).
Assumption 8	Our data is data image with random sizable (128/ 256/ 512/ 1024).

The process of aggregation data is to reduce the amount of data, so there are different mechanisms that are integrating data, hierarchical grouping, and trying to improve the integrity of the system through data aggregation. And in a fog environment where intermediate nodes are available with different efficiencies. This technology contributes to achieving the location awareness feature for each of the fog nodes in addition to utilizing the resources [33]. Data aggregation aims to secure the collection of similar data from different sensors to obtain different views of the same situation or case in order to improve the security and privacy of fog-based IOT applications. This role plays a major benefit in increasing the reliability of the system since less data quantities are generated for the efficient behavior of the system in distributed networks in fault-tolerant cases. These technologies are highly visible in the application and tracking of smart vehicles to ensure their safety [34]. Where data is aggregated and communicated for efficient and secure traffic that is subject to a wide range of protocols responsible for data integrity and privacy [33].

3.2 DF for privacy-based DAs Technique

Domingo-Ferrer is a scheme that is considered one of the collection protocols that guarantee security, including features that may be similar with the privacy characteristics to perform the basic mathematical operations [15, 16].As these protocols help reduce the packets of data that are stored and transmitted. Therefore, it is considered one of the protocols that have a valuable role in the privacy of aggregated data that can implement all basic operations [15], where the addition factor is used [$\oplus$] [16].so it can be used to ensure safe aggregation operations in modern systems.

$$Decryption_k(Encryption(S_1) \oplus Encryption(S_2)) = S_1 \oplus S_2 \quad (1)$$

- *Parameters nomination*

-We will start with two public parameter which are named a, b and two secret parameter which are named c, d.
- a is consider as big integer, & it must has numerous little divisors.
- b is a small integer and b > 2.
- Every data that is encrypted will be form within a sets, so b refer to the size of set.
- c is a small divisor of a and c > 1.
- d $\in$ U_a and r^{-1}mod a must exist.
- Converting image into linear text.
- reshaping of m*n*3 image into 1xp, where p=m*n*3

- *Encryption process*

- In this part the data will be divided to small values L $\in$ Uc as a number of b size of set (L_1, $L_{2,}$ ... L_z), L = Σb i=1 L_i mod c where L $\in$ Uc then calculate cipher data through the key.

$$D = Encrypt(L) = L_1 d^1 \bmod a, l_2 d^2, ... l_z d^z \bmod a \quad (2)$$

- *Aggregation Process*

- Here aggregation operation is presented by $D_1 = enc(L_1)$ & $D_2 = enc(L_2)$.
- The aggregated of encrypted data could be determined as the equation below:

$$D_{ag} = D_1 + D_2 \bmod a = enc(L_1 + L_2) \bmod a \quad (3)$$

- *Decryption Process*

- This step can be performed as the equation below:

$$Decryption(D_{ag}) = D_{ag1} d^{-1} \bmod a + D_{ag2}\, \mathrm{d}^{-2} \bmod a ... D_{agz} d^{-d} \bmod a \tag{4}$$

- Then regain the total value of original Data through this equation:

$$L_T = \sum_i^z L_{Ti} \bmod c \tag{5}$$

PROPOSED ALGORITHM STEPS

Stage 1: Every IOT apparatus generates its data packet and formatted with PKT [$\mathbf{IOT_{Data}}$] = (Info).
Stage 2: It's the encrypted step where every data packet is encrypted using a symmetric encryption key to fortify the duct of linkage between IOT and $\mathbf{SCH_g}$ layer and to achieve confidentiality for the data.
Stage 3: The IOT device is forwarding the data packet to the SCH layer which is accountable for getting the inputs information from IOT apparatus.
Stage 4: Every $\mathbf{SCH_g}$ decrypts the extradited packet of data to procure (Info), thereafter encrypts it ($\mathbf{C_{Info}}$) with the HET key (DF), cloud server will be shared with.
Stage 5: Subsequently, $\mathbf{SCH_g}$ forms the packet of data which is encrypted the step previously with the format PKT [$\mathbf{SCH_g}$] = ($\mathbf{C_{Info}}$), and forward them to the fog layer.
Stage 6: Fog servers are incapable to decrypt the extradited packets that previously encrypted due to no sharing keys with them.
Stage 7: The encrypted data packet can be stored tentatively in fog servers, and wait for a while so that users can require for certain information for a particular device in case they need (fine-grained access information).
Stage 8: Fog server can confirm for user's access through authentication operation step to allow them to decrypt the encrypted packets that are transmitted from each ($\mathbf{SCH_g}$)with their own keys. If not, each fog server will aggregate the encrypted packet using DF properties scheme and form it as PKT [fog] = ($\mathbf{Agg_g}$), then sends this aggregated data to the cloud medium.
Stage 9: The aggregated data packet will be always stored in CS.
Stage 10: The cloud server have the permission to decrypt the related aggregated data packets with the user shared key and get the data as PKT [Cloud].

4. Performance Analysis

In this proposal, SDA scheme is used mainly to obtain the product of the aggregation, encryption and decryption operations, and therefore gratitude to these SDA processes, the privacy of accurate data is ensured, knowing that the data aggregation processes contribute very significantly to the integrity and efficiency of data transmission, storage and efficiency. In view of our proposed algorithm in our paper, all the steps are obtained to establish eventuality of the system. All of our experiments have been implemented using core i7-2670QM ,2.20GHz with RAM 6.00 GB windows 10 Machine, fulfillment of proposed algorithm is applied using MATLAB R2018a where all the proposed operations were done in encryption, aggregation and decryption techniques. We applied our data as the standard Lena image with random sizable (128, 256, 512, 1024).

4.1 privacy analysis

To mention the protection of privacy and not to be hacked or snooped, and as we mentioned earlier, private keys are supposed to be shared between SCH and the cloud server independently, in addition, this secret key is never shared with foggers in order to avoid any attacks from service operators and maintain The complete confidentiality of the system and data. Where the protocol used ensures the privacy of data for users as it is one of the secure aggregated protocols used in such foggy systems and their applications. Let's assume that both the fog and cloud servers are subject to the HBC adversary paradigm and let's present some theoretical scenarios that show the extent to which the principle of privacy is achieved through our proposed protocol. This kind of Homomorphic aggregation supplies fog servers with the ability to enable the addition assignment without disclosing secret keys. When we say that each IOT device generates its data for each device independently. Then these data packets are encrypted in the SCH stage. This encoded data is aggregated and gained for each SCH as the output of the aggregation process. Therefore, when it is assumed that there is an attacker who follows these steps and wants to reveal the data out of curiosity, the data is still in a state of concealment because he does not have the secret keys for decryption due to secret keys are not shared with fog servers to be very robust towards the service operators. When studying another case of attack, for example, when there is bad intention by the system attackers to access the data and change its features or corrupt it, even though these people who follow the details of the data legitimately, but they can be accessed through intrusion detection techniques Therefore, if fake data is encrypted, then it is collected by fake encrypted data packets and then these collected packets will be sent to the cloud centers, and even though the cloud server has the shared secret key, it will not find the data correctly with the real information or consumption and the result will not be the same in the case logical $\text{result} \neq \text{Agg}_{\text{enc pckt}}$. Therefore, it is possible to scan for pseudo-packets before they are transferred to the upper layer of the cloud. Finally, in the case of tracking by the cloud centers themselves for accurate data and for applications that are subject to energy consumption and other related. After the aggregation operations, the fog server transfers that collected data to the cloud server to store it permanently and for different storage purposes. Where this is not considered a privacy crime or hacking, because those responsible for operating the service in the cloud centers do not have the right to obtain or disclose

detailed data despite their sharing of the secret key, so it keeps the collected data only, and if the encryption packet is decrypted by an attacker, he does not understand the detailed data of each IOT device.

4.2 Experimental analysis

This section presents a comprehensive evaluation of the proposed algorithm for encryption and aggregation operations, including the security protocol used in addition to the decryption operations. We depend here in the work on the assumption that the interaction between the nodes that share in sending and transmitting data to the other is smoothly. As default values we use 200 numbers of IOT devices and 100 numbers of IOT requests as shown in "Fig. 4,"

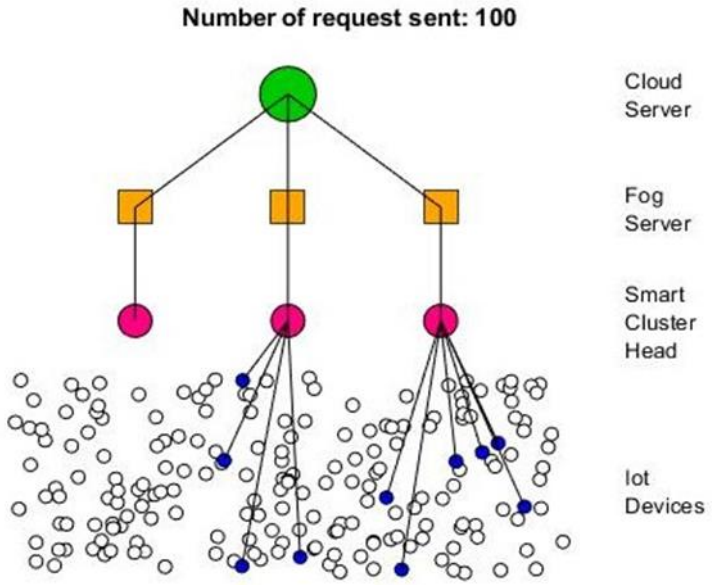

Fig. 4. The proposed Model Simulation

This paragraph deals with the evaluation of the algorithm scheme in terms of several factors, which are the execution time of the whole system, encryption, decoding and aggregation. In addition to increasing the sizes of sent packets and the balance of servers in the system, moreover the storage efficiency fulfillment In short, the proposed structure was created consisting of 4 different mediums for integrated functions between the IOT devices layer and the smart cluster head layer, followed by the fog mediator and finally the central cloud layer. Encryption was implemented twice in the model with the motive of strengthening and improving the degree of security and confidentiality of the data in addition to providing privacy. This was achieved through two approved schemes accompanied by some assumptions that were imposed on the system to obtain the best results. In the first encoding stage, we used a symmetric-and-hybrid encryption between each Hilbert Curve (Space filling curve/ Scan methods) and chaotic maps (details of this cipher will be mentioned in another paper), while the second coding phase was carried out through the homomorphic encryption using DF.And it is worth mentioning that one of the important things that must be taken into account is the number of sets/tuples due to the inevitability of balancing them in terms of solidity and computational costs. Also the large number of sets/ tuples lead to a system with more solidity and greater strength, and thus will block the system against any external attacks that want to penetrate its privacy, but at the same time, it increases the complexity of the system, which in turn to an increase in the computational cost. In such systems, the priority is determined according to the user's need for the application. The more complex the system is accompanied by non-simple cryptographic methods, thus it will increase the time of the system's implementation of the algorithm and increase its cost. Moreover, it will increase the required processing operations and vice versa, the simpler the encryption method and the less used tuples the system was less complex and less expensive. Therefore, it is highly dependent on the need of users and service operators in terms of their requirements in the respective application. As shown in "Fig. 5," as we raise in the no. of IOT request, the no. of execution time as we seen in the graph the encryption line and followed by aggregation and decryption will raise as well with different rates. In our case, the cipher operations used were rather complicated, so it somehow affected the coding time and the system processes.

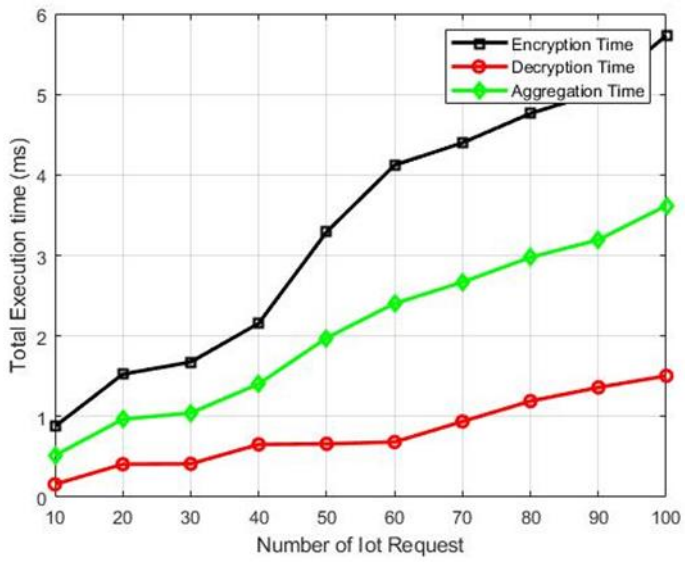

Fig. 5. The total execution time

Where the execution time is measured here as equal to the sum of all of the encryption, aggregation and decryption, and therefore the change in the number of requests sent from Internet of Things devices may affect the execution time of the system. As every DAS scheme performs one of the operations of encryption, aggregation and decryption in a completely different way from the others. By comparing the proposed model with other models in terms of the time used for encoding, aggregation and decoding time, here in [35] the author used the Paillier scheme as one of the schemes he used in related topics, we will find that our model DF achieves an encoding time faster than the one in [33]. this supports the principle that such schemes may change their impact based on the datum, factors and number of tuples used in each process.

On the other hand, and to mention the performance evaluation, depending on the number of packages available in the system, it affects the change in the amounts of data received by the fog servers. Based on network hypotheses, the total quantity of data received to fog servers is measured depending on the actual number sent to those servers and its ciphered packets sizes. Looking at "Fig. 6," it indicates the amount of data received for the fog servers and its relation with the actual packet transmitted as well. Where the total amount of data received by FS is determined by the multiplying of packet's no. transmit to fog medium and the size of every packet. As in our simulation we used 3 device of the fog and each device is a completely different distance from the cloud center, so it also differs at different logical rates.

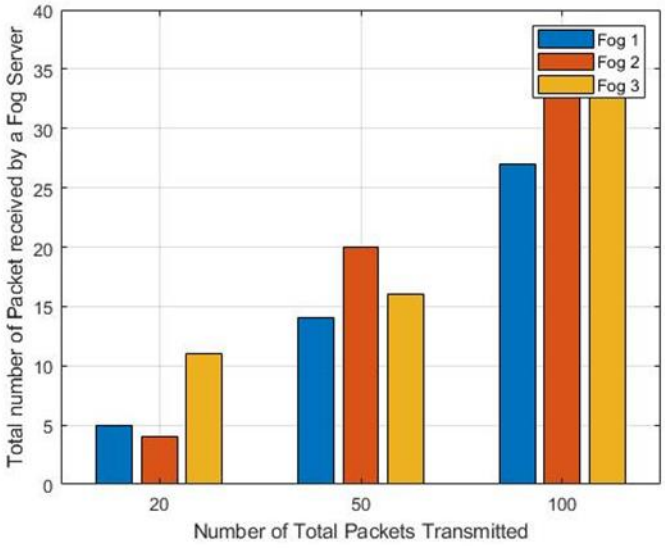

Fig. 6. The amount of data received by Fog server.

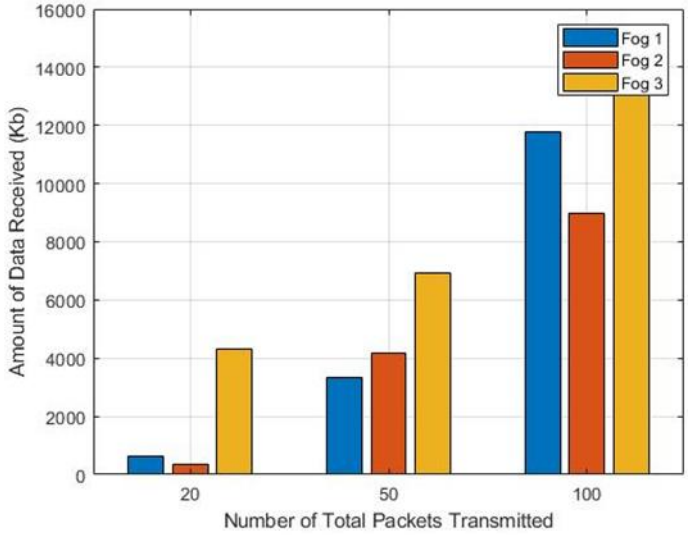

Fig. 7. The amount of data received by cloud server

In the final step of the proposed system, and as we mentioned before, the encrypted and aggregated packets are sent to the cloud centers in the upper layer, in which the data is permanently and located until it is needed later after decrypting it. Logically, the greater the quantities and sizes of the packets sent to the upper layer, this creates a heavy burden on that layer, in addition, it constitutes a large deficit in the storage capacity and loads, which in turn impede the performance of functions in the cloud centers, and consequently, the response time will increase with a very large latency. Therefore, fog servers reduce that load and can deal with it, so that the cloud in turn costs less packets and less burden. As "Fig. 7," shows the relationship between the quantities of transmitted packets and the packets received by the cloud, it is expected to notice from the figure the decrease in the size of those packets, thanks to the DAS schemes, from which we conclude that these schemes contribute significantly to reducing the number of packets, as we can say that in a step Aggregation When the aggregated packets increase, the lowering in total data volume raise, and thus this confirms that the proposed protocol in our work works on storage efficiency by relying on fog servers to minimize the ratio of data stored inside the CS.

5. Conclusion and Future Work

With the great expansion of Internet of Things devices and the superiority of the fog field over the central cloud and the uncontrolled inflation of the generated data and its continuous movement within many services and daily requirements, maintaining the privacy and security of that data and the complexity of processing it has become very urgent as it is the nerve of development due to the evolution of the world of hacks, crimes and attacks The urgency on such smart and modern fog systems. On the other hand, cloud servers suffered in such gaps due to their inability to protect against the leakage and corruption of transmitted data. Therefore, in this paper, we have implemented a fog structure based on the precept of aggregation and privacy within the secure aggregation protocols named PPFDA distributed through the fog servers to serve as a support for the cloud centers, commensurate with the characteristics of the fog and its work, which reduces the response time for service users and reduce communication traffic problems. The proposed model results ensure data privacy accurately due to the use of the DF scheme as one of the DSA secure aggregation schemes. Performance was evaluated in terms of execution time, transmission and storage efficiency, and especially data privacy efficiency. As we assumed in our paper, the proposed model ensures the effectiveness of authentication before including the network or system and thus combines security through symmetric encryption based on chaotic maps (details are presented in another paper) and data privacy from third parties through the characteristics of DAS schemes. It allows the use of our approach in many applications and services such as smart grid, consumption data and billing, as well as smart traffic light applications and others. However, in our future projects, we will strive to develop plans to preserve privacy and data protection more broadly in fog computing and to consider improving the available mechanisms, given that the security mechanisms are still in various and multiple security holes.

References

[1] Abou-Tair, D. E. D., Buechsenstein, S., & Khalifeh, A. (2020). A fog computing-based framework for privacy preserving IoT environments. *INTERNATIONAL ARAB JOURNAL OF INFORMATION TECHNOLOGY*, *17*(3), 306-315.

[2] Butun, I., Sari, A., & Österberg, P. (2019, January). Security implications of fog computing on the internet of things. In *2019 IEEE International Conference on Consumer Electronics (ICCE)* (pp. 1-6). IEEE.

[3] Wang, X., Wang, L., Li, Y., & Gai, K. (2018). Privacy-aware efficient fine-grained data access control in Internet of medical things based fog computing. *IEEE Access*, *6*, 47657-47665.

[4] Zhou, W., Jia, Y., Peng, A., Zhang, Y., & Liu, P. (2018). The effect of iot new features on security and privacy: New threats, existing solutions, and challenges yet to be solved. *IEEE Internet of things Journal*, *6*(2), 1606-1616.

[5] Amin, R., Kunal, S., Saha, A., Das, D., & Alamri, A. (2020). CFSec: Password based secure communication protocol in cloud-fog environment. *Journal of Parallel and Distributed Computing*, *140*, 52-62.

[6] Alzoubi, Y. I., Osmanaj, V. H., Jaradat, A., & Al‐Ahmad, A. (2021). Fog computing security and privacy for the Internet of Thing applications: State‐of‐the‐art. *Security and Privacy*, *4*(2), e145.

[7] Razouk, W., Sgandurra, D., & Sakurai, K. (2017, October). A new security middleware architecture based on fog computing and cloud to support IoT constrained devices. In *Proceedings of the 1st international conference on internet of things and machine learning* (pp. 1-8).

[8] Zhang, P., Zhou, M., & Fortino, G. (2018). Security and trust issues in fog computing: A survey. *Future Generation Computer Systems*, *88*, 16-27.

[9] Guan, Y., Shao, J., Wei, G., & Xie, M. (2018). Data security and privacy in fog computing. *IEEE Network*, *32*(5), 106-111.

[10] Dhiah El Diehn, I., Büchsenstein, S., & Khalifeh, A. (2018, June). A Privacy Preserving Framework for the Internet of Things. In *2018 19th IEEE/ACIS International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD)* (pp. 27-31). IEEE.

[11] Khalid, T., Abbasi, M. A. K., Zuraiz, M., Khan, A. N., Ali, M., Ahmad, R. W. & Aslam, M. (2021). A survey on privacy and access control schemes in fog computing. *International Journal of Communication Systems*, *34*(2), e4181.

[12] Lu, R., Heung, K., Lashkari, A. H., & Ghorbani, A. A. (2017). A lightweight privacy-preserving data aggregation scheme for fog computing-enhanced IoT. *IEEE access*, *5*, 3302-3312.

[13] Zhu, L., Li, M., Zhang, Z., Xu, C., Zhang, R., Du, X., & Guizani, N. (2019). Privacy-preserving authentication and data aggregation for fog-based smart grid. *IEEE Communications Magazine*, *57*(6), 80-85.

[14] Guan, Z., Zhang, Y., Wu, L., Wu, J., Li, J., Ma, Y., & Hu, J. (2019). APPA: An anonymous and privacy preserving data aggregation scheme for fog-enhanced IoT. *Journal of Network and Computer Applications*, *125*, 82-92.

[15] Okay, F. Y., & Ozdemir, S. (2018, April). A secure data aggregation protocol for fog computing based smart grids. In *2018 IEEE 12th International Conference on Compatibility, Power Electronics and Power Engineering (CPE-POWERENG 2018)* (pp. 1-6). IEEE.

[16] Alabdulatif, A., & Kaosar, M. (2016). Privacy preserving cloud computation using Domingo-Ferrer scheme. *Journal of King Saud University-Computer and Information Sciences*, *28*(1), 27-36.

[17] Şimşek, M. U., Yıldırım Okay, F., Mert, D., & Özdemir, S. (2018). TPS3: A privacy preserving data collection protocol for smart grids. *Information Security Journal: A Global Perspective*, *27*(2), 102-118.

[18] Shen, X., Zhu, L., Xu, C., Sharif, K., & Lu, R. (2020). A privacy-preserving data aggregation scheme for dynamic groups in fog computing. *Information Sciences*, *514*, 118-130.

[19] Lin, X., Ni, J., & Xuemin (Sherman) Shen. (2018). *Privacy-enhancing fog computing and its applications*. Basel: Springer International Publishing.

[20] Yousefpour, A., Fung, C., Nguyen, T., Kadiyala, K., Jalali, F., Niakanlahiji, A., & Jue, J. P. (2019). All one needs to know about fog computing and related edge computing paradigms: A complete survey. *Journal of Systems Architecture*, *98*, 289-330.

[21] Rahmani, A. M., Liljeberg, P., Preden, J. S., & Jantsch, A. (Eds.). (2017). *Fog computing in the internet of things: Intelligence at the edge*. Springer.

[22] Tawalbeh, L. A., Muheidat, F., Tawalbeh, M., & Quwaider, M. (2020). IoT Privacy and security: Challenges and solutions. *Applied Sciences*, *10*(12), 4102.

[23] Alamer, A. (2021). Security and privacy-awareness in a software-defined Fog computing network for the Internet of Things. *Optical Switching and Networking*, *41*, 100616.

[24] Sen, A. A. A., & Yamin, M. (2021). Advantages of using fog in IoT applications. *International Journal of Information Technology*, *13*(3), 829-837.

[25] Ashi, Z., Al-Fawa'reh, M., & Al-Fayoumi, M. (2020). Fog computing: security challenges and countermeasures. *Int. J. Comput. Appl*, *175*(15), 30-36.

[26] Sabireen, H., & Neelanarayanan, V. (2021). A review on fog computing: architecture, fog with IoT, algorithms and research challenges. *Ict Express*, *7*(2), 162-176.

[27] Ali, A., Ahmed, M., Imran, M., & Khattak, H. A. (2020). Security and privacy issues in fog computing. *Fog Computing: Theory and Practice*, 105-137.

[28] Alrawais, A., Alhothaily, A., Hu, C., & Cheng, X. (2017). Fog computing for the internet of things: Security and privacy issues. *IEEE Internet Computing*, *21*(2), 34-42.

[29] Bonomi, F., Milito, R., Zhu, J., & Addepalli, S. (2012, August). Fog computing and its role in the internet of things. In *Proceedings of the first edition of the MCC workshop on Mobile cloud computing* (pp. 13-16).

[30] Lu, R., Liang, X., Li, X., Lin, X., & Shen, X. (2012). EPPA: An efficient and privacy-preserving aggregation scheme for secure smart grid communications. *IEEE Transactions on Parallel and Distributed Systems*, *23*(9), 1621-1631.

[31] Yan, Y., Qian, Y., Sharif, H., & Tipper, D. (2012). A survey on cyber security for smart grid communications. *IEEE Communications Surveys & Tutorials*, *14*(4), 998-1010.

[32] Yang, L., Xue, H., & Li, F. (2014, November). Privacy-preserving data sharing in smart grid systems. In *2014 IEEE International Conference on Smart Grid Communications (SmartGridComm)* (pp. 878-883). IEEE.

[33] Bellavista, P., Berrocal, J., Corradi, A., Das, S. K., Foschini, L., & Zanni, A. (2019). A survey on fog computing for the Internet of Things. Pervasive and mobile computing, 52, 71-99.

[34] Liu, J., Li, J., Zhang, L., Dai, F., Zhang, Y., Meng, X., & Shen, J. (2018). Secure intelligent traffic light control using fog computing. Future Generation Computer Systems, 78, 817-824.

[35] Yildirim Okay, F., Ozdemir, S., & Xiao, Y. (2020). Fog computing‐based privacy preserving data aggregation protocols. *Transactions on Emerging Telecommunications Technologies*, *31*(4), e3900.

Authors' Profiles

Samaa Y. Tarabay received the B.S degree in Electronics and Communications Engineering Department, Faculty of Engineering from Misr higher institute of Engineering and Technology, Mansoura, Egypt and prepostgraduate from the Electronics and Communications Engineering Department, Mansoura University, Egypt, in 2015 and 2017, respectively.

Ibrahim Yasser received the B.Sc. degree in electronics and communications from Benha University, Egypt, and the M.Sc. and Ph.D. degrees from the Electronics and Communications Engineering Department, Mansoura University, Egypt, in 2016 and 2020, respectively. His research work has been materialized in books and ISI index articles in international specialty journals. His research interests include neutrosophic sets, security, multimedia, fog and cloud computing, chaotic maps, machine learning, big data, artificial intelligent, medical image analysis, computer-aided diagnosis, and flexible education. Future research interests include design security techniques for the cloud requiring little user awareness and computer-aided diagnosis medical images analysis. He is a member of chief editors for Neutrosophic Knowledge journal.

Ahmed S. Samra received the B.Sc. and the M.Sc degree in communications engineering from Menoufia University 1977, 1982 respectively, and the PhD. degree in optical communications and integrated optics from ENSEG, Grernoble, France in 1988, France in 1988. Reviewer for some international journals and conferences; (Optical engineering journal, Optoelectronic Review journal, Optoelectronics and advanced Materials rapid communication journal, Optik journal, and the six international conference on wireless and optical communication networks WOCN 2009). Supervisor for about 70 M.Sc. and Ph.D. Thesis, and more than 90 accepted papers in a national and international journals and conferences .Head of communication and computer Department, Faculty of Technology , El-madina El-monawara, Saudi Arabian .Head of Electronics and Communication Engineering Department , Faculty of Engineering , Mansoura University. Director of Biomedical Engineering Program, Faculty of Engineering, Mansoura University. Director for Training unit, Faculty of Engineering, Mansoura University.He is now a professor at the faculty of engineering, Mansoura University. His research interests are in the field of optical communications, integrated Optics and optical measurement techniques.

Abeer T. Khalil received the B.Sc. and Ph.D. degrees from the Electronics and Communications Engineering Department, Faculty of Engineering, Mansoura University, in 2001 and 2013, respectively. She is currently working as an Associate Professor at the Electronics and Communications Department, Faculty of Engineering, Mansoura University. She has published more than 30 articles and supervised ten postgraduate students in many universities. She is interested in wireless networking and hardware realizations of digital system.

How to cite this paper: Samaa Y. Tarabay, Ibrahim Yasser, Ahmed S. Samra, Abeer T. Khalil, "Privacy Enhancing for Fog Computing based - IoT", International Journal of Wireless and Microwave Technologies(IJWMT), Vol.13, No.3, pp. 1-13, 2023. DOI:10.5815/ijwmt.2023.03.01