PPDMIT: A Lightweight Architecture for Privacy-Preserving Data Aggregation in the Internet of Things

mehdi gheisari (mehdi.gheisari61@gmail.com)
IAU

Research Article

Keywords: Data Aggregation, Internet of Things, Privacy Preservation, Paillier encryption, low-cost

Posted Date: June 23rd, 2022

DOI: https://doi.org/10.21203/rs.3.rs-1771046/v1

PPDMIT: A Lightweight Architecture for Privacy-Preserving Data Aggregation in the Internet of Things

Mehdi Gheisari[1],

Abstract— Data is generated over time by each device in the Internet of Things (IoT) ecosphere. Recent years have seen a resurgence in interest in the IoT due to its positive impact on society. However, due to the automatic management of IoT devices, the possibility of disclosing sensitive information without user consent is high. A situation in which information should not be unintentionally disclosed to outside parties we do not trust, i.e., privacy-preserving. Additionally, IoT devices should share their data with others to perform data aggregation and provide high-level services. There is a trade-off between the amount of data utility and the amount of disclosure of data. This trade-off has been caused a big challenge in this field. To improve this trafe-off efficiency rather than current studies, in this study, we propose a Privacy-Preserving Data Aggregation architecture, PPDMIT, that leverages homomorphic paillier encryption, K-means, a one-way hash chain, and the Chinese Remainder Theorem. We have found that the proposed privacy-preserving architecture achieves a more efficient data aggregation than current studies and improves privacy preservation by utilizing extensive simulations. Moreover, we found that our proposed architecture is highly applicable to IoT environments while preventing unauthorized data disclosure. Specifically, our solution depicted 8.096% improvement over LPDA and 6.508% over PPIOT.

Index Terms—***Data Aggregation, Internet of Things, Privacy Preservation, Paillier encryption, low-cost.***

I. INTRODUCTION

Nowadays, the Internet of Things (IoT) has become increasingly popular in many aspects of our lives. IoT evolved after passing some technologies such as RFID, embedded systems, and wireless sensor networks that aim to sense the environment effectively to make high-level decisions. Each IoT device should produce data over time and collaborate with others [1].

Sensitive information about a building, such as the number of people alive there, may be compromised by this collaboration. In order to avoid possible harm in the future, sensitive data must never be unintentionally disclosed. On the other hand, high-level services such as the aggregation of data must be shared. Since a huge number of IoT devices are performing their actions autonomously, automatic privacy-preserving solutions are of importance for IoT systems. Proposed privacy-preserving solutions should be lightweight because many IoT devices are resource-constrained [2].

On the other hand, "Cloud Computing" (CC) can support IoT environments because it can provide unlimited computing and storage and great virtualization of IoT devices. Cloud computing can be integrated with the IoT to achieve more effective environments, i.e., IoT-Cloud. It is worth mentioning that research on IoT-Cloud is still in its infancy stage [3].

This paper proposes a lightweight solution for IoT-Cloud environments to preserve the privacy of sensed sensitive data more efficiently and achieve efficient data aggregation. This is achieved through leveraging several methods such as homomorphic paillier encryption for providing secure data transfer connection while manipulating over encrypted data is possible, a one-way hash chain with the aim of early false data detection, Gaussian distribution algorithm in order to find valuable data among all of the collected data while it is lightweight, and Chinese remainder theorem for data aggregation[4]. In our proposed solution, Privacy-Preserving Data Management in the Internet of Things (PPDMIT), IoT devices send their data to the Cloud via homomorphic paillier encryption, after which the remote Cloud removes false information and finds valuable information, aggregating it. Data aggregation involves condensing data for purposes of statistical analysis and then expressing it on a condensed basis. Several sources of data are combined into one cluster using data aggregation tools. Our data aggregation methods can give us new insights and help us discover new relationships. The process involves several input packets being received by intermediate nodes such as gateways. Following aggregation, the network will produce one output packet. Based on IoT device data, aggregation is often used to gain more insight into particular groups of people.

In this paper, we propose a lightweight privacy-preserving method for IoT-Cloud environments, namely PPDMIT. Our proposed privacy-preserving architecture is put to the test by running simulations in an IoT environment.

The key contributions are:

- To achieve PPDMIT, at first, each device uses a homomorphic paillier encryption method to send its data to the remote Cloud. And one-way hash chain method is used in the CC for early detection and removing false data.
- We adopt a Gaussian distribution algorithm, K-means, in the Cloud for finding valuable data.
- We use Chinese Remainder Theorem for data aggregation over hybrid IoT devices.

In this way, redundancy in a network can be reduced, protecting privacy. The remaining section of this paper is as follows. We describe relevant background info on the Internet of Things, privacy-preserving methods when it comes to IoT in Section II. Section IV presents the components of the solution. Section V describes the proposed PPDMIT architecture, which is evaluated in Section VI. Section VII summarizes the paper and describes future work.

II. Background

In this section, we ascertain necessary IoT information, privacy-preserving in IoT, and common privacy-preserving methods.

A. Internet of Things

One major component of IoT is wireless sensor networks that are connected through the Internet; some differences with WSNs are:

- IoT covers all types of objects such as humans, handwriting, PCs, and so on.
- In pure IoT, routing is not implemented because each device sends its data directly to the Internet without any broker.
- A whole wireless sensor network can be considered as one node in IoT.

IoT is not a single technology but a set of technologies that are participating in local activities and interacting with each other. The Internet is used to connect all aspects of our lives worldwide to provide high-quality services. IoT affects how we live and how we work and how we can achieve better performance. Whenever and wherever devices are connected, a high level of security should be assured. In addition to physical items, these devices can include vehicles, home appliances, etc. These devices should be equipped with sensors, actuators. It is anticipated that billions of devices will exist by 2025 [1].

Fig. 1 shows the Internet of Things concept from a schematic point of view. As Fig. 1 shows, all devices such as smart cameras are connected to provide more humanized services in the IoT era. As mentioned above, a huge number of connected devices will exist that each one produces data over time, thus leading to Big Data.

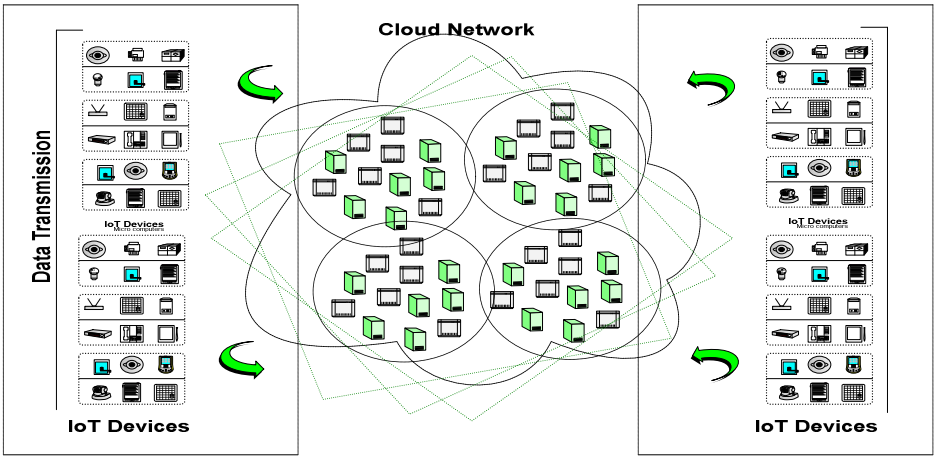

Figure 1. The details of Internet of Things and Cloud network-based [1,6].

B. Privacy Preservation in IoT

Over time, IoT devices produce more and more data. Data should be managed efficiently to provide a better quality of services (QoS). In other words, IoT devices should share their data and collaborate with others. One technology that can be applied to obtain better QoS is data aggregation. Based on data aggregation, we can discover patterns and convert raw data into useful knowledge. However, sensitive data may be disclosed. Thus, we should consider solutions that prevent unintentional disclosure of data to adversaries to reduce the possibility of misusing data and harming the system[5].

Sensitive information can be divided into three main subcategories:

- Personal: e.g., social security number (SSN).
- Sensitive: e.g., Salaries and diseases.

For example, zip code and age are quasi-identifiers. What is the importance of quasi-identifiers? As a result, Quasiidentifiers must be kept private since we can identify individuals by joining data obtained from various external sources, including public voter registration information, hospitals, and news. In order to prevent misuse of sensitive data, these three types of data should remain private. The short and simple answer is that we must protect sensitive data from parties we do not trust and do not want access to. In addition, we can distinguish between two types of privacy-preserving concepts: (1) protection of the content; and (2) protection of the context. [6]. Content protection means protecting sensitive generated data from unintentional disclosure, i.e., we have to provide users a way to process data so that no one can find the original generated sensitive data when we are facing adversaries. In reverse, context data refers to protecting the information of non-sensed-data from information leakages such as sensing time and sensing location.

In more detail, privacy types can be divided into four main subcategories [7-9]:

- Data privacy: preserving the privacy of produced data
- Location privacy: keeping the locations of IoT devices private.
- Time privacy: keeping the sensing time private.
- User privacy: maintaining user behaviors private.

Based on the IoT Security Threat Map that was published in 2017 by Beecham research group [10,11], security challenges, as shown in Fig. 2, are becoming worse over time, and we

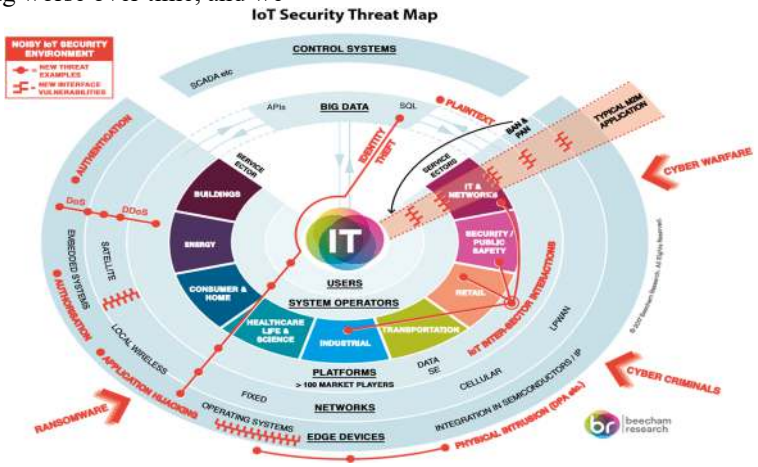

Figure 2. IoT Security Threat Map[12].

need to address them. The figure shows that damages that may stem from attackers mainly occur in three areas: attacks to platforms, networks, and edge devices. Recently, most attacks tend to IoT Inter-Sector interactions part of IoT environment such as buildings' data, health care data, and so on [13].

C. Privacy-Preserving Methods

These methods are described in this section as ways of preserving privacy. Six privacy-preserving solutions are available in environments that deal with large amounts of data and want to maintain privacy. An explanation of the methods is provided in Table I.

Table I PRIVACY-PRESERVING TECHNIQUES [14].

Privacy-preserving Techniques	Attributes
Data Distortion	Contains data operations like perturbation, blocking, aggregation, merging, swapping, sampling
Data or rules hidden	Hiding sensitive data or rules
K-anonymity	Processing the anonymization procedure of data
L-diverse	Maintains diversity of sensitive attributes by keeping at least K group sizes
Taxonomy tree	Limiting information leakage with the help of tree
Randomization	For example, adding random noises to data based on a logic

III. RELATED WORKS

In this section, we describe literature that tries to perform aggregation while keeping the privacy of data.

Martonosi in [15] explained in detail the concerns of how to store data in IoT and cloud environments in terms of security and privacy while they are prepared to be aggregated. They explained the policies followed by the U.S. government for handling privacy-preserved. Various technologies and tools for different kinds of applications are discussed. However, they did not show any data aggregation methods for IoT devices while preserving data privacy.

In [16], based on each participant's secret key, the authors proposed an efficient algorithm to aggregate data with privacy preservation. There is, however, one disadvantage, namely the inexcusable degree of privacy-preservation. In other words, if the secret key is penetrated one time, it would be easier for the rest of the attacks to misuse the system's vulnerability. Moreover, their solution is not able to remove false data and is not effective in aggregating hybrid IoT devices' data.

In order to achieve better data aggregation while preserving privacy, authors in [17] have been employed homographic paillier encryption. One of its main restrictions is that the method only depends on encryption to provide privacy from outsiders that cause unacceptable privacy-preserving levels. Moreover, their solution can address the diversity among devices effectively.

Raju *et al.* in [18] applied the homomorphic encryption method to multiplying protocols to preserve privacy. But, it has some drawbacks, such as an unacceptable privacy-preserving degree. Moreover, their solution is not robust against false data generated by adversaries.

Mukkamala *et al.* in [19] compared a Fuzzy-based approach of mapping. The authors combined several values into one singular value for having a more efficient further process. The combination brings privacy while saving the bandwidth of the network. One of its drawbacks is its high computational cost.

In [20], the authors proposed a novel idea for identifying sensitive attributes automatically and, then, the data is modified so that the original properties of data are preserved. One of its notable drawbacks is that their method cannot be generalized to cover a variety of domains. Moreover, the authors did not calculate the amount of overhead of their solution.

Moreover, authors in [21] proposed an outsourcing association rule mining that is approximately secure and preserves privacy by leveraging both data privacy and mining privacy. One advantage is that the solution enables false data to be identified in the mining process. However, one disadvantage is that it is non-deterministic against adversaries in cloud servers that sometimes causes high computational cost.

In [22], authors have proposed a lightweight data aggregation scheme for fog computing-enhanced IoT, called Lightweight Privacy Data Aggregation, to address this challenge (LPDA). It not only aggregates data from hybrid IoT devices into one but also filters early injected false data by utilizing the homomorphic Paillier encryption plus the Chinese Remainder Theorem along with the one-way hash chain technique. LPDA has been thoroughly evaluated for security and privacy enhancement with differential privacy techniques to show that it is both secure and private.

Authors in [21] described a homomorphic public-key encryption scheme for binary digits. They developed a PIR protocol that reduces the data strikingly to achieve data privacy[23]. The authors used an election system to check the validity of ballots given by users. They suggested a 2DNF protocol which is described for safety from malicious users and preserving the privacy of users. One of the most striking drawbacks is that this work did not consider false data and/or save the network's bandwidth.

Tassa *et al.* in [24] described a distributed protocol based on association rules in the Databases distributed on multiple servers that are spread horizontally. One of its drawbacks is that they did not propose an effective protocol for disparity verification, and they also did not consider the amount of communication cost. Fortunately, their system is approximately accurate.

In [25], authors have presented several additional challenges in terms of privacy and security. They have proposed a new architecture for smart homes, the IOTFLA, combining Federated Learning and secure data aggregation while focusing on security and privacy. In achieving more security and privacy in smart homes, we hope that our proposal will be a step forward.

Zhang *et al.* in [26] have been proposed a method for anonymity; one privacy-preserving method depends on an efficient quasi-identifier index. They also tried to protect privacy when new data is added to the data set. One of its drawbacks is that this work did not consider false data. Moreover, they did not check whether or not data is valuable.

To fill the gap of current studies, we propose PPDMIT to provide efficient IoT environments that preserve the privacy of generated data while performing data aggregation over hybrid IoT devices' data. Besides, PPDMIT considers both false and valuable data to obtain efficient and clean IoT environments.

IV. FUNDAMENTAL COMPONENTS OF PPDMIT

In this section, we pay attention to the necessary background information for designing our solution.

A. Homomorphic Cryptosystem

It makes it possible to perform complex calculations on encrypted data without compromising the encryption with homomorphic cryptosystems. This cryptosystem is based on the decisional composite residual assumption. Simply and straightforwardly, we can perform operations on encrypted data and get the encrypted result that, when decrypted, would be the same as we would get if the operations were performed on the decrypted text in the first place. Keeping data a secret from others is the main purpose of data transformation. Data security can also be ensured with encryption. A sensible approach would be to see homomorphic encryption as transparent and secure so that manipulators can manipulate data without stealing it. In addition, the data is transparent so that any manipulator can look at the data without being able to manipulate it. In brief, the third party can manipulate received encrypted data and sends it back to the data owner while manipulating it without allowing anyone else to understand it [28]. The encrypted information of m_1 and m_2 can be computed from the public key when the $m_1 + m_2$ encryption key is missing. Below is a detailed explanation of how it works.

- It will be necessary to simultaneously and independently pick two large prime numbers p and q so that. $(pq,(p-1)(q-1))=1$ .These prime numbers must also be equal in length.
- It will be determined by calculating $n = pq, and, \lambda = \mathrm{lcm}(p-1, q-1)$ from 1 by using Least Common Multiple.
- The random integer is selected at in Z

- By checking the existence of the modular multiplicative inverse, ensure that n divides the order of g: $\mu = (L(g^{\lambda} \bmod n^2))^{-1} \bmod n$
- L is the definition of function $L(x) = \dfrac{x-1}{n}$
- A public key consisting of (n, g) is required for encryption and a private key consisting of (λ, μ) is required for decryption.

By exploiting certain discrete logarithms that are easily computed, Paylier's cryptosystem works. By using the binomial theorem as an example,

$$(1+n)^x = \sum_{k=0}^{x} \binom{x}{k} n^k = 1 + nx + \binom{x}{2} n^2$$

As a consequence of the theorem, we have:

$(1+n)^x \equiv 1 + nx \pmod{n^2}$ and $y = (1+n)^x \bmod n^2$, then: $x \equiv \dfrac{y-1}{n} \pmod{n^2}$

Accordingly:

$L((1+n)^x \bmod n^2) \equiv x \pmod{n}$,

The definition of the function L is the (QUOTIENT OF INTERINTEGER DIVISION).

Homomorphic properties make the system malleable, however. This security feature does not protect against adaptive chosen-DDos does not offer the highest level of semantic security. Cryptographic strength is usually not malleability. Although an IoT system and cryptographic threshold protocol might not require this property, other applications might.

B. One-Way Hashing

This is the most famous cryptographic primitive as it involves successively building up one-way hashes of data. One-way functions are algorithms that map data of arbitrary size to strings with a fixed size, and it is impossible to find and invert the original data given the algorithm's formula. Hashing is a form of data protection that is used to secure strings and files. By hashing, information can be converted to a digest message or a hash, which is a number derived from a string or text. These available digests make it easy to verify whether sent and received messages have the same hash and no tampering. Call numbers booked using libraries within a domain are an example of a hash function. A library's books are identified by their unique call numbers so that it is possible to locate them by their call number. A hash function returns a unique hash number that is called a universal hash function to verify data. In hashing, received data and digest cannot be reversed to the original one, for example, MD5 in [29]. The oneway hash function can also be applied in various domains such as database indexing, caching, program compilation, error checking, or false data selection. The function is one-way, meaning that it cannot be inverted or reversed. When searching for messages that produce a given hash, most people use brute-force searching to see if different inputs produce a match or they use rainbow tables of matched hashes. Modern cryptography relies on cryptographic hash functions. A hash function's advantages are that it enables insertion, deletion, and retrieval simultaneously. IMN devices, which are able to filter false data, can assist in fighting PPDMIT false data injection attacks(Figure 2) [30].

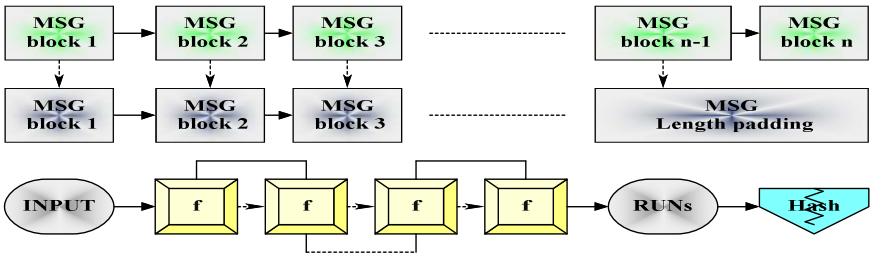

Figure 2. Optimal cryptographic hashing requires deterministic hashing

C. Chinese Remainder Theorem

The Chinese remainder theorem is a theorem of number theory, which discovers the remainders of the Euclidean division of an integer, *N*, by several integers, then, one can determine the remainder of the division of number N uniquely by the product of

these integers, provided that the divisors are pairwise coprime[31-41]. An important calculation algorithm in modular arithmetic which enables a person to solve simultaneous equations concerning different moduli in considerable generality. In brief, it addresses such problems of finding a number that, for example, leaves a remainder of 0 when the number is divided by 5, remainder 6 when the number is divided by 7, and remainder 10 when it is divided by 12. The simplest result is 370. It is notable to mention that the result is not unique since any multiple of 5×7×12=420 can be added to it, and the result will still satisfy the problem. Furthermore, it is widely acceptable for large computing with large devices because it allows replacing the limitation on the size of the result with several similar operations on small integers. It provides a unique solution to simultaneous linear congruence. In our scenario, we use it for data aggregation over massive IoT devices.

Chinese remainder theorem states that, given a given n , a series of remainders may be obtained by division by several integers based on Euclidean division. Under the condition that the divisors are coprimes, it is possible to determine the remainder of n by computing the product of these integers. In this way, as long as one knows a bound on the size of the result, a computation can be replaced by a few smaller computations. We may call these integers $n_1, \ldots, n_k$ moduli or divisors because they are greater than 1. We may call these integers moduli or divisors because they are greater than 1. Because these integers are greater than 1, we can call them moduli or divisors. Let us denote the product of n_i by N .

For example, if $a_1, \ldots, a_k$ are any entire integers, and n_i are pairwise coprime, then the system is congruent:

$$x = a_1 \quad (\text{mod} \quad n_1)$$
$$\ldots$$
$$x = a_k \quad (\text{mod} \quad n_k)$$

The congruence between two solutions to a problem is modulo N.

$$x_1 = x_2 \quad (\text{mod}\, N \quad for(all))$$

The remainder of the Euclidean division of x by each n_i can be used to determine whether a value x is a solution. It is sufficient to check each integer between 0 and N until the solution successively is found for this problem. Despite being straightforward, this method is extremely inefficient. The solution must be checked for integers (including 0). For the example considered here, we need to check t integers (including 0). There is a constant factor in the size of the input, so the input is up to N digits, and there are an average of N operations in the calculation. We are therefore trying to find a polynomial $P(X)$ that is congruent with:

$$P(X) \equiv A_i(X).\left(\text{mod}\, P_i(X)\right) = \prod_{i=1}^{k} P_i(X).Q_i(X) = \frac{Q(X)}{P_i(X)} \qquad for \quad \square \quad i = 1, \ldots, k$$

When $\frac{1}{Q(X)}$ is decomposed into partial fractions, we obtain $S_i(X)$ polynomials of degree $\bigcap_{i=1}^{n} X_i S_i(X) < \bigcap_{i=1}^{n} X_i d_i$ with degrees F, as shown below.

$$\frac{1}{Q(X)} = \sum_{i=1}^{k} \frac{S_i(X)}{P_i(X)} \qquad \rightarrow \quad 1 = \sum_{i=1}^{k} S_i(X) Q_i(X).$$

Therefore, by dividing by the polynomial, one gets the solution to the simultaneous congruence system:

$$\sum_{i=1}^{k} A_i(X)S_i(X)Q_i(X) \qquad 1 \le i \le k.$$

$$\sum_{i=1}^{k} A_i(X)S_i(X)Q_i(X) = A_i(X) + \sum_{j=1}^{k} (A_j(X) - A_i(X))S_j(X)Q_j(X) =$$

$$A_i(X).(\bmod P_i(X)),$$

The degree of a solution with degree greater than $D = \sum_{i=1}^{k} d_i$ may be greater than one. The unique solution with less than degree D is obtained by dividing $B_i(X)$ by $A_i(X)S_i(X)$ by $P_i(X)$ and finding the remainder. Hence, we have the solution.

$$P(X)_{all} = \sum_{i=1}^{k} B_i(X)Q_i(X)_{all}$$

V. The Proposed Method - PPDMIT

This section aims to describe the PPDMIT, a model for IoT environments for data aggregation while preserving the privacy of sensitive data.

A. Algorithm of PPDMIT

The algorithm of the PPDMDIT in schematic form is depicted in Fig. 3. The figure shows our proposed method for performing data aggregation while preserving privacy in the Cloud-based Internet of Things environment from a schematic point of view. Intending to achieve data aggregation while preserving data privacy efficiently, PPDMIT leverages four steps. It is notable to mention that the last three steps (i.e., steps 2, 3, and 4) are deployed in the cloud environment, while step 1 is applied at the IoT device level. In more detail, in step 1, IoT devices hash their data, apply homomorphic paillier encryption method to their data and send them to the Cloud. In step 2, before data aggregation is performed by leveraging the Chinese Remainder Theorem, some refinements should be done; for example, the cloud server applies a one-way chain method to remove false data. In step 3, the cloud server applies K-means clustering algorithm to differentiate valuable data from non-valuable ones. Finally, in step 4, the cloud server does aggregation using the Chinese Remainder Theorem (Fig. 4 or Algorithm 1).

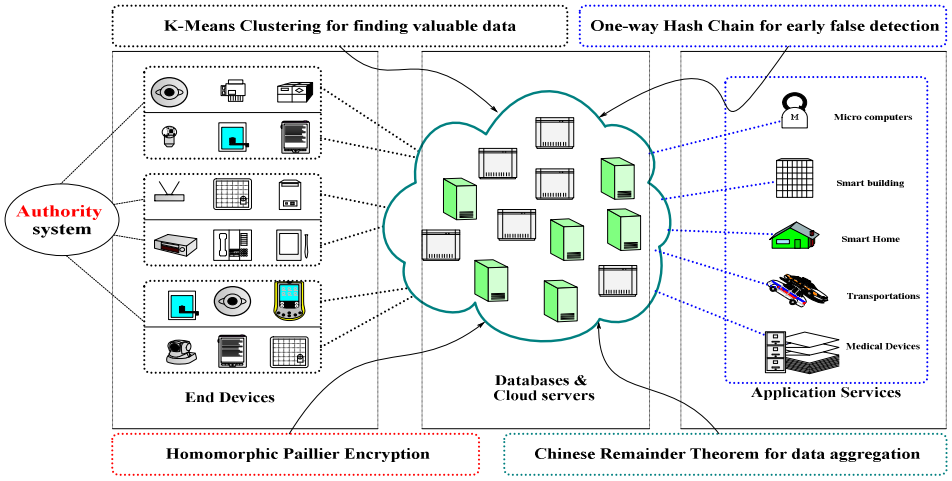

Figure 3. Proposed Privacy-Preserving Data Management in IoT.

Algorithm 1: PPDMIT

The data is contained in the window: Identification and Query for IoT devices.

The query result has been encrypted using users' private key

Leverages is provided to the data access layer by the user

One-Way Hashing: An algorithm that maps an arbitrary size of data to a cryptographic hash function (CHF)

Homomorphic Cryptosystem: Run Gaussian distribution algorithm in the Cloud for finding valuable data.

K-means in order to find valuable data

Run: homomorphic paillier encryption for encrypting IoT devices

The data has been entered: Identification, Query

Results of an Q(*) query encrypted using users' PINs

Calculations will be performed by the data access layer

Chinese Remainder Theorem: each device uses homomorphic paillier encryption

for sending data to the remote cloud

one-way hash chain method is used

detection and removing false data.

one-way chain for early false detection

Server computes : *The data access layer will pass to n servers*

The layer that computes data access: according to the query x data points will be queried

The data access layer will perform calculations

Computed costs of preserving privacy: *CPU usage*

Figure 4. Algorithm PPDMIT leverages for Privacy-Preserving Data Management in IoT.

VI. Performance Evaluation

In this section, we simulate PPDMIT to verify its performance in OpenIoT. Open IoT bridges this gap between the semantics and data computing so IoT applications in the Cloud can have unified semantics. Open IoT is using a generalized standard model for semantic unification of diverse IoT systems by using the W3C Semantic Sensor Network ontology (SSN). Using its infrastructure, all I/O devices are able to gather and annotate data in a semantic manner. Depending on how similar the data sets are, Open IoT can also provide a special feature that permits easy linking. In this manner, it is capable of dealing with data streams compatible with mobile sensors without needing extraneous interfaces. In addition to providing a wide range of tools, it supports cloud-based IoT applications, hence reducing the programming effort. Global Sensor Networks (GSN) is an open-source project by Github that provides open-source libraries for Open IoT. As one of the top ten open source projects, Open IoT has been honored with the Black Duck award. We did simulation using OpenIoT software [27] (Figure 5). In the simulation setup, 100 homogeneous temperature devices are producing sensitive data while sending their data to the Cloud for data aggregation. Each device senses a random value between 10 to 100. IoT devices are assumed to have unique identification numbers that are natural integer numbers less than 101. In the first step, each device calculates the remainder of its value by its unique ID. Then, they hash their data to the data range between 110 and 220. The data range numbers are based on our assumption, and we note that other ranges of numbers can be used instead. So, more investigation is needed to find the best values. After hashing the values, IoT devices apply Microsoft SEAL (a homomorphic encryption scheme), an open-source library that provides a set of encryption libraries to perform computations directly on the encrypted data. A note of significance is that we used the Brakerski/Fan Vercauteren (BFV) homomorphic encryption scheme as an assumption, and additional research is required to determine the best option.

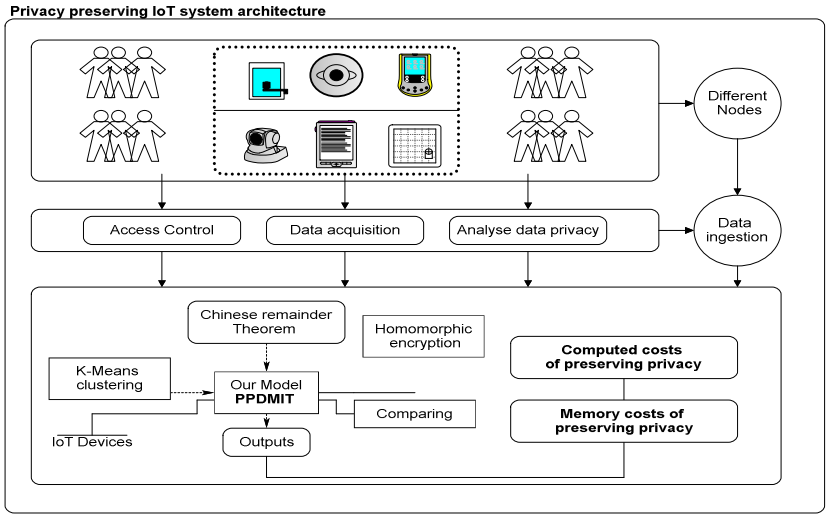

Figure 5. Details of implementation and simulation in OpenIoT

After enabling the manipulation of encrypted data by applying the homomorphic encryption method, IoT devices send their data to the cloud server. The cloud server firstly applies the one-way hash function to find false data. So, we can resist unwanted adversaries that are trying to inject false data into the system. In the next step, step 3, the cloud server applies the K-means classification algorithm to find valuable data from non-valuable ones with k=3. In other words, we have two classes: valuable data and non-valuable data that are determined by K- means algorithm. In our scenario, data is more valuable if it is used in more than 80 percent of the occurrences. Shortly and straightforwardly, if the usage number of IoT device data is higher than 80 percent, it is considered valuable data. It is notable to mention that since our scenario does not involve many IoT devices, we use K-means. In the case of a large volume of data, we need to use a stronger classifier, and we leave it as future research work. Sixty-six out of one hundred IoT devices' data is valuable that can be used for data aggregation as step 4 with leveraging Chinese remainder theorem (CRT). As a result, our solution can aggregate encrypted IoT devices data while preventing false data injection and removing non-valuable data. For evaluating PPDMIT, we calculate two important evaluation metrics that are: (1) computational cost to find whether or not devices can afford it, and (2) the number of unwanted disclosure of data.

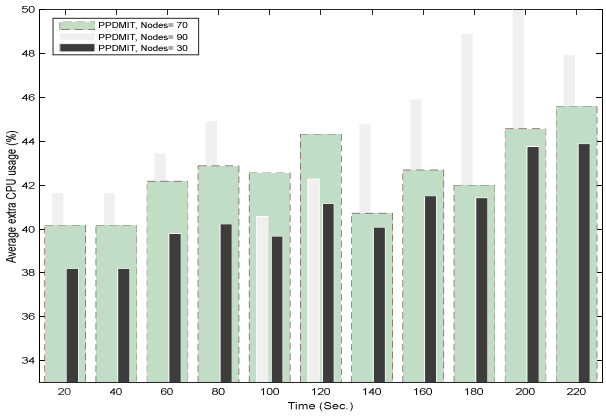

Figure 6. The details of Computed costs of preserving privacy, extra CPU usage-average in different Nodes.

Fig. 6 shows the amount of the computational cost of the system. It is evident that the amount of PPDMIT overload in average is around 35 percent. Although 35 percent is affordable to many IoT devices, it would be better to use it only for highly demanded privacy devices thanks to the advancement of technology. Fig.7 shows the number of unintentional disclosure of data in our scenario. In our scenario, IoT devices send their data to the cloud server through 42 middle nodes. Among those nodes, 20 ones are malicious nodes, so that they are trying to eavesdrop on the passing data while five nodes inject false data to deviate the data. In general, out of 20 malicious nodes, two ones were able to penetrate the homomorphic encrypted data and find original data and deviate them.

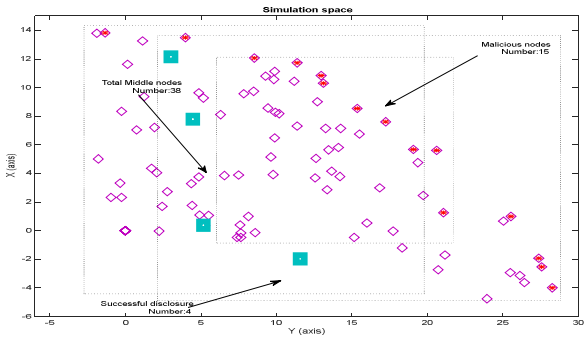

Figure 7. Number of unintentional disclosure of data.

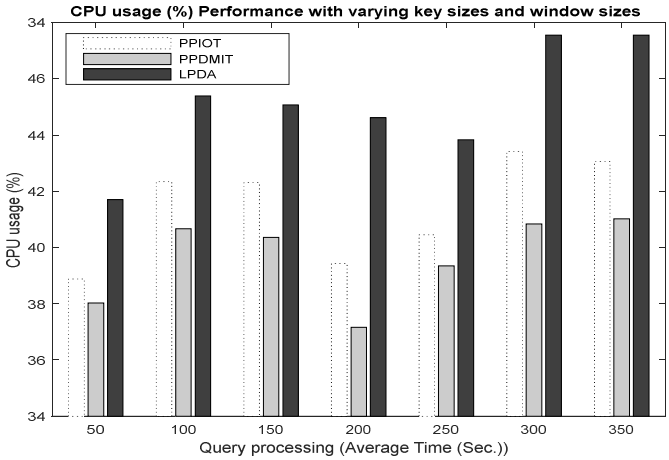

Figure 8. The details of Computed costs of preserving privacy, extra CPU usage-average in LPDA, PPIOT, and PPDMIT.

A simulation of the IoT environment has been run to test our proposed privacy architecture. In addition, CPU consumption should be compared to similar tasks. For the PPDMIT method, each device sends its data to the Cloud using paillier homomorphic encryption. To detect and remove incorrect data in the early phase, the one-way hash chain method has been used in CC. We have also adopted an algorithm for finding valuable data in the Cloud-based on the Gaussian distribution. As well as this, the Chinese residual theorem is applied to data gathered from IoT hybrid devices. The proposed PPDMIT method is compared with LPDA [22] and PPIOT [1].In this experiment, we investigated the effects of using the key sizes of Paillier processing capabilities to evaluate the CPU usage average of IoT systems. Since there is no prior key exchange in the proposed scheme, this experiment is relevant.

Consequently, Paillier key combinations of any size are available to the user. A summary of the results can be found in Figure 8. Observations of the experiments indicate that key size has a negligible impact on query performance except when 2024 is selected as the key size. When querying sensor data over 9 hours, performance is within 1 s with a 2024 key size. The PPDMIT method is compared to LPDA and PPLOT in order to show better results for computed costs of preserving privacy. As can be seen, the proposed method has experienced an 8.096% improvement over LPDA and 6.508% over PPIOT.

VII. Conclusion

The quality of life of individuals is expected to be impacted by data analytics based on information from the Internet of Things devices. IoT data aggregation, however, requires careful consideration of security and privacy. A centralized server is usually used to aggregate IoT data. However, it is challenging to coordinate efforts between untrustworthy and sensitive data parties if a distributed approach is used. This paper proposed a method that preserves sensitive data in the IoT-Cloud environment while performing data aggregation, PPDMIT. It leveraged four techniques for improving the efficiency: (1) one-way chain for early false detection, (2) homomorphic paillier encryption for encrypting IoT devices' data when they want to send their data to the data aggregator, (3) K-means in order to find valuable data, and (4) Chinese remainder theorem for data aggregation of IoT devices. We evaluated PPDMIT from the amount of overload to the system perspective. One of the future works is evaluating PPDMIT

more comprehensively. Another promising work is applying other privacy-preserving techniques such as the Differential Privacy technique or anonymization technique.

Acknowledgment: This work was supported by Basic Research Project of Shenzhen, China (JCYJ20200109113405927) and Basic Research Project of Shenzhen, China (JCYJ20190806142601687)

References

[1] Gheisari, M., Esnaashari, M. (2017). A survey to face recognition algorithms: advantageous and disadvantageous. *Journal Modern Technology & Engineering, V. 2*(1), pp. 57-65.

```
@Article{imagesurvey,
 author  = {M.Gheisari and M. Esnaashari},
 title   = {A survey to face recognition algorithms: advantageous and disadvantageous},
 journal = {Journal Modern Technology \& Engineering},
 year    = {2017},
 volume  = {2},
 number  = {1},
 pages   = {57-65},
}
```

[2] Gheisari, M., Baloochi, H., Gharghi, M., & Khajehyousefi, M. (2012). An Evaluation of Two Proposed Systems of Sensor Data's Storage in Total Data Parameter. *International Geoinformatics Research and Development Journal*.

```
@article{gheisari2012evaluation,
  title={An Evaluation of Two Proposed Systems of Sensor Data's Storage in Total Data Parameter},
  author={Gheisari, Mehdi and Baloochi, Hamed and Gharghi, Meysam and Khajehyousefi, Mehdi},
  journal={International Geoinformatics Research and Development Journal},
  year={2012}
}
```

[3] Gheisari, M.. Design, Implementation and Evaluation of SemHD: a New Semantic Hierarchical Sensor Data Storage. **Indian Journal of Innovations and Developments**, [S.l.], p. 115-120, mar. 2012. ISSN 2277 - 5390. Available at: <http://ijid.informaticspublishing.com/index.php/ijid/article/view/31604>. Date accessed: 21 Jun. 2018.

```
@Article{SemHD,
  author =  {GHEISARI, M},
  title =   {Design, Implementation and Evaluation of SemHD},
  journal = {Indian Journal of Innovations and Developments},
  year =    {2012},
  pages =   {115-120},
  month =   {March}
}
```

[4] M. Gheisari *et al.*, "NSSSD: A new semantic hierarchical storage for sensor data," *2016 IEEE 20th International Conference on Computer Supported Cooperative Work in Design (CSCWD)*, Nanchang, 2016, pp. 174-179.

```
@INPROCEEDINGS{7565984,
author={M. Gheisari and A. A. Movassagh and Y. Qin and J. Yong and X. Tao and J. Zhang and H. Shen},
booktitle={2016 IEEE 20th International Conference on Computer Supported Cooperative Work in Design (CSCWD)},
```

```
title={NSSSD: A new semantic hierarchical storage for sensor data},
year={2016},
volume={},
number={},
pages={174-179},
month={May},}
```

[5] M. Gheisari, G. Wang and M. Z. A. Bhuiyan, "A Survey on Deep Learning in Big Data," *2017 IEEE International Conference on Computational Science and Engineering (CSE) and IEEE International Conference on Embedded and Ubiquitous Computing (EUC)*, Guangzhou, 2017, pp. 173-180.

```
 @INPROCEEDINGS{8005992,
author={M. Gheisari and G. Wang and M. Z. A. Bhuiyan},
booktitle={2017 IEEE International Conference on Computational Science and Engineering (CSE) and IEEE International Conference on Embedded and Ubiquitous Computing (EUC)},
title={A Survey on Deep Learning in Big Data},
year={2017},
volume={2},
number={},
pages={173-180},
month={July},}
```

[6] M. Jafari, J. Wang, Y. Qin, M. Gheisari, A. S. Shahabi and X. Tao, "Automatic text summarization using fuzzy inference," *2016 22nd International Conference on Automation and Computing (ICAC)*, Colchester, 2016, pp. 256-260.

```
 @INPROCEEDINGS{7604928,
author={M. Jafari and J. Wang and Y. Qin and M. Gheisari and A. S. Shahabi and X. Tao},
booktitle={2016 22nd International Conference on Automation and Computing (ICAC)},
title={Automatic text summarization using fuzzy inference},
year={2016},
volume={},
number={},
pages={256-260},

ISSN={},
month={Sept},}
```

[6] Gheisari, Mehdi, et al. "An Evaluation of Two Proposed Systems of Sensor Data's Storage in Total Data Parameter." *International Geoinformatics Research and Development Journal* (2012).

```
@article{gheisari2012evaluation,
  title={An Evaluation of Two Proposed Systems of Sensor Data's Storage in Total Data Parameter},
  author={Gheisari, Mehdi and Baloochi, Hamed and Gharghi, Meysam and Khajehyousefi, Mehdi},
  journal={International Geoinformatics Research and Development Journal},
```

```
  year={2012}
}
```

[7] Gheisari, Mehdi. "The Effectiveness of Schema Therapy Integrated with Neurological Rehabilitation Methods to Improve Executive Functions in Patients with Chronic Depression." *Health Science Journal* 10.4 (2016) page:1-6.

```
@article{gheisari2016effectiveness,
  title={The Effectiveness of Schema Therapy Integrated with Neurological
Rehabilitation Methods to Improve Executive Functions in Patients with Chronic
Depression},
  author={Gheisari, Mehdi},
  journal={Health Science Journal},
  volume={10},
  number={4},
  year={2016},
page={1:6}
  publisher={iMedPub}
}
```

[8] Rezaeiye, Payam Porkar, and Mehdi Gheisari. "Performance analysis of two sensor data storages." *Proceedings of 2nd International Conference on Circuits, Systems, Communications & Computers (CSCC)*. 2011.

```
 @inproceedings{rezaeiye2011performance,
   title={Performance analysis of two sensor data storages},
   author={Rezaeiye, Payam Porkar and Gheisari, Mehdi},
   booktitle={Proceedings of 2nd International Conference on Circuits, Systems,
Communications \& Computers (CSCC)},
   pages={133--136},
   year={2011}
 }
```

[9] Gheisari, Mehdi, et al. "A Comparison with some Sensor Network Storages." *International Conference on Computer and Computer Intelligence (ICCCI 2011)*. ASME Press, 2011.

```
 @inproceedings{gheisari2011comparison,
   title={A Comparison with some Sensor Network Storages},
   author={Gheisari, Mehdi and Bahekmat, Maliheh and Setoodeh, Hamid Reza and
Khajehyousefi, Mehdi},
   booktitle={International Conference on Computer and Computer Intelligence (ICCCI
2011)},
   year={2011},
   organization={ASME Press}
 }
```

[10] GhadakSaz, Ehsan, et al. "Design, Implement and Compare two proposed sensor data's storages Named SemHD and SSW." *From Editor in Chief* (2012): 78.

```
 @article{ghadaksaz2012design,
   title={Design, Implement and Compare two proposed sensor data's storages Named SemHD
and SSW},
   author={GhadakSaz, Ehsan and Amini, Mohammad Reza and Porkar, Payam and Gheisari,
Mehdi},
   journal={From Editor in Chief},
```

```
    pages={78},
    year={2012}
  }
```

[11] Rezaeiye, Payam Porkar, et al. "Statistical method used for doing better corneal junction operation." *Advanced Materials Research*. Vol. 548. Trans Tech Publications, 2012.

```
  @inproceedings{rezaeiye2012statistical,
    title={Statistical method used for doing better corneal junction operation},
    author={P.P.Rezaeiye and P.P. Rezaeiye and E.Karbalayi and M.Gheisari},
    booktitle={Advanced Materials Research},
    volume={548},
    pages={762--766},
    year={2012},
    organization={Trans Tech Publ}

  }
```

[12] Gheisari, M., A. R. Bagheri. "SHD: a New Sensor Data Storage." *In 5th international symposium on advances in science & technology*. 2011.

```
  @inproceedings{gheisari2011shd,
    title={SHD: a New Sensor Data Storage},
    author={Gheisari, M and Bagheri, AR },
    booktitle={In 5th international symposium on advances in science \& technology},
    year={2011}
  }
```

[13] Porkar, Payam, et al. "A Comparison with Two Sensor Data Storages in Energy." *International Conference on Computer and Computer Intelligence (ICCCI 2011)*. ASME Press, 2011.

```
  @inproceedings{porkar2011comparison,
    title={A Comparison with Two Sensor Data Storagesin Energy},
    author={P.P.Porkar and M.Gheisari and G.H.Bazyari and Z.Kaviyanjahromi},
    booktitle={International Conference on Computer and Computer Intelligence (ICCCI
2011)},
    year={2011},
    organization={ASME Press}
  }
```

[14] Gheisari, Mehdi, and Mehdi Esnaashari. "Data Storages in Wireless Sensor Networks to Deal With Disaster Management." *Emergency and Disaster Management: Concepts, Methodologies, Tools, and Applications*. IGI Global, 2019. 655-682.

```
  @incollection{gheisari2019data,
    title={Data Storages in Wireless Sensor Networks to Deal With Disaster Management},
    author={M.Gheisari and M.Esnaashari},
    booktitle={Emergency and Disaster Management: Concepts, Methodologies, Tools, and
Applications},
    pages={655--682},
    year={2019},
    publisher={IGI Global}
  }
```

[16] Rezaeiye, Payam Porkar, et al. "Agent programming with object oriented (C++)." *Electrical, Computer and Communication Technologies (ICECCT), 2017 Second International Conference on*. IEEE, 2017.

```
@inproceedings{rezaeiye2017agent,
  title={Agent programming with object oriented (C++)},
  author={ P.P. Rezaeiye,  and p.p. Rezaeiye and E. F. Gh. M. Beig and H. Mohseni and R. Kaviani and M. Gheisari and M. Golzar},
  booktitle={Electrical, Computer and Communication Technologies (ICECCT), 2017 Second International Conference on},
  pages={1--10},
  year={2017},
  organization={IEEE}
}
```

[17] Gheisari, Mehdi, et al. "MAPP: A Modular Arithmetic Algorithm for Privacy Preserving in IoT." *Ubiquitous Computing and Communications (ISPA/IUCC), 2017 IEEE International Symposium on Parallel and Distributed Processing with Applications and 2017 IEEE International Conference on*. IEEE, 2017.

```
@inproceedings{gheisari2017mapp,
  title={MAPP: A Modular Arithmetic Algorithm for Privacy Preserving in IoT},
  author={M,Gheisari and G,Wang and M.D.Z.A, Bhuiyan and Z, Wei},
  booktitle={Ubiquitous Computing and Communications (ISPA/IUCC), 2017 IEEE International Symposium on Parallel and Distributed Processing with Applications and 2017 IEEE International Conference on},
  pages={897--903},
  year={2017},
  organization={IEEE}
}
```

[18] Ashourian, Mohsen, Mehdi Gheisari, and Ali Hashemi. "An Improved Node Scheduling Scheme for Resilient Packet Ring Network." *Majlesi Journal of Electrical Engineering* 9.2 (2015): 43.

```
@article{ashourian2015improved,
  title={An Improved Node Scheduling Scheme for Resilient Packet Ring Network},
  author={M,Ashourian and M,Gheisari and A,Hashemi},
  journal={Majlesi Journal of Electrical Engineering},
  volume={9},
  number={2},
  pages={43},
  year={2015},
  publisher={Islamic Azad University Majlesi}
}
```

[19] Sharifzadeh, Manaf, Kaveh Bashash,Shahram Bashokian, and mehdi gheisari. "A Comparison with two semantic sensor data storages in total data transmission." *arXiv preprint arXiv:1401.7499* (2014).

```
@article{sharifzadeh2014comparison,
  title={A Comparison with two semantic sensor data storages in total data transmission},
  author={Sharifzadeh, Manaf and Bashash, Kaveh and Bashokian, Shahram and others},
  journal={arXiv preprint arXiv:1401.7499},
  year={2014}
```

```
}
```

[20] Porkar, P., Mojtaba Fazli, and M. Gheisari. "Sensor networks challenges." *11th international conference on data networks, DNCOCO '12*. 2012.

```
@inproceedings{porkar2012sensor,
  title={Sensor networks challenges},
  author={Porkar, P and Fazli, Mojtaba and Gheisari, M},
  booktitle={11th international conference on data networks, DNCOCO '12},
  year={2012}
}
```

[22] Khajehyousefi, Mehdi, et al. "A Comparison with Three Proposed Sensors Data's Storages." *International Conference on Advanced Computer Theory and Engineering, 4th (ICACTE 2011)*. ASME Press, 2011.

```
@inproceedings{khajehyousefi2011comparison,
  title={A Comparison with Three Proposed Sensors Data's Storages},
  author={Khajehyousefi, Mehdi and Karimi, Mehdi and Bazyari, Gholam Hossein and
Gheisari, Mehdi},
  booktitle={International Conference on Advanced Computer Theory and Engineering,
4th (ICACTE 2011)},
  year={2011},
  organization={ASME Press}
}
```

[23] Fakhimi, Esmaeil, et al. "Design Two Sensor Data Storages." *International Conference on Advanced Computer Theory and Engineering, 4th (ICACTE 2011)*. ASME Press, 2011.

```
@inproceedings{fakhimi2011design,
  title={Design Two Sensor Data Storages},
  author={Fakhimi, Esmaeil and Ajandak, Ghorban and Gheisari, Mehdi and Bahekmat,
Maliheh},
  booktitle={International Conference on Advanced Computer Theory and Engineering,
4th (ICACTE 2011)},
  year={2011},
  organization={ASME Press}
}
```

[24] Gheisari, Mehdi. "Design, implementation and evaluation of SemHD: a new semantic hierarchical sensor data storage." *Indian Journal of Innovations and Developments* 1.3 (2012): 115-120.

```
@article{gheisari2012design,
  title={Design, implementation and evaluation of SemHD: a new semantic hierarchical
sensor data storage},
  author={Gheisari, Mehdi},
  journal={Indian Journal of Innovations and Developments},
  volume={1},
  number={3},
  pages={115--120},
  year={2012}
}
```

[25] Rezaeiye, Payam Porkar, et al. "Creating an ontology using protégé: concepts and taxonomies in brief."

```
@Article{rezaeiyecreating,
  author  = {Rezaeiye, Payam Porkar and Fazli, Mojtaba and Sharifzadeh, Manaf and Moghaddam, Hani and Gheisari, Mehdi},
  title   = {Creating an ontology using protege: concepts and taxonomies in brief},
  journal = {Advances in Mathematical and Computational Methods},
  volume={1},
  number={3},
  pages={115--120},
  year={2012}
}
```

[26] Gheisari M., Wang G., Chen S., Ghorbani H. (2018) IoT-SDNPP: A Method for Privacy-Preserving in Smart City with Software Defined Networking. In: Vaidya J., Li J. (eds) Algorithms and Architectures for Parallel Processing. ICA3PP 2018. Lecture Notes in Computer Science, vol 11337. Springer, Cham

```
@InProceedings{10.1007/978-3-030-05063-4_24,
author="Gheisari, Mehdi and Wang, Guojun and Chen, Shuhong and Ghorbani, Hamidreza",
title="IoT-SDNPP: A Method for Privacy-Preserving in Smart City with Software Defined Networking",
booktitle="Algorithms and Architectures for Parallel Processing",
year="2018",
publisher="Springer International Publishing",
pages="303--312",
}
```

[28] **Mehdi Gheisari**, Guojun Wang, Shuhong Chen, Ali Seyfollahi, A Method for Privacy-preserving in IoT-SDN Integration Environment, 16th IEEE International Symposium on Parallel and Distributed Processing with Applications (ISPA 2018), 11-13 Dec. 2018, Melbourne, Australia

```
@InProceedings{ISPA2018,
  author    = {Mehdi Gheisari, Guojun Wang, Shuhong Chen, Ali Seyfollahi},
  title     = {A Method for Privacy-preserving in IoT-SDN Integration Environment},
  booktitle = {16th IEEE International Symposium on Parallel and Distributed Processing with Applications (ISPA 2018)},
  year      = {11-13 Dec. 2018, Melbourne, Australia},
  journal   = {16th IEEE International Symposium on Parallel and Distributed Processing with Applications (ISPA 2018)},
}
```

[29] M. M. Motahari Kia, J. A. Alzubi, M. Gheisari, X. Zhang, M. Rahimi and Y. Qin, "A Novel Method for Recognition of Persian Alphabet by Using Fuzzy Neural Network," in *IEEE Access*, vol. 6, pp. 77265-77271, 2018.

```
@ARTICLE{ACCESSOCR,
author={M. M. Motahari Kia and J. A. Alzubi and M. Gheisari and X. Zhang and M. Rahimi and Y. Qin},
journal={IEEE Access},
title={A Novel Method for Recognition of Persian Alphabet by Using Fuzzy Neural Network},
year={2018},
volume={6},
```

number={},
pages={77265-77271},
month={},}

[30] Alzubi J.A., Yaghoubi A., Gheisari M., Qin Y. (2018) Improve Heteroscedastic Discriminant Analysis by Using CBP Algorithm. In: Vaidya J., Li J. (eds) Algorithms and Architectures for Parallel Processing. ICA3PP 2018. Lecture Notes in Computer Science, vol 11335. Springer, Cham

```
@InProceedings{10.1007/978-3-030-05054-2_10,
author="Alzubi, Jafar A.and Yaghoubi, Ali and Gheisari, Mehdi and Qin, Yongrui",
title="Improve Heteroscedastic Discriminant Analysis by Using CBP Algorithm",
booktitle="Algorithms and Architectures for Parallel Processing",
year="2018",
publisher="Springer International Publishing",
address="Cham",
pages="130--144",
}
```

[31] Jayaraman Sethuraman, Jafar Alzubi, Ramachandran Manikandan, Mehdi Gheisari* and Ambeshwar Kumar, “Eccentric Methodology with Optimization to Unearth Hidden Facts of Search Engine Result Pages”, Recent Patents on Computer Science (2018) 11: 1. https://doi.org/10.2174/2213275911666181115093050

```
@Article{searchengine,
  author  = {Jayaraman Sethuraman, Jafar Alzubi, Ramachandran Manikandan, Mehdi Gheisari},
  title   = {Eccentric Methodology with Optimization to Unearth Hidden Facts of Search Engine Result Pages},
  journal = {Recent Patents on Computer Science},
  year    = {2018},
  pages   = {11:1},
}
```

[32] Mehdi Gheisari, Guojun Wang, Wazir Zada Khan, Christian Fernández-Campusano,
A context-aware privacy-preserving method for IoT-based smart city using Software Defined Networking,
Computers & Security, Volume 87, 2019, 101470, ISSN 0167-4048,
https://doi.org/10.1016/j.cose.2019.02.006.
(http://www.sciencedirect.com/science/article/pii/S0167404818313336)
CCF B, IF=3.0

@article{GHEISARI2019101470,
title = "A context-aware privacy-preserving method for IoT-based smart city using Software Defined Networking",
journal = "Computers & Security",
volume = "87",
pages = "101470",
year = "2019",
issn = "0167-4048",
doi = "https://doi.org/10.1016/j.cose.2019.02.006",
url = "http://www.sciencedirect.com/science/article/pii/S0167404818313336",
author = "Mehdi Gheisari and Guojun Wang and Wazir Zada Khan and Christian Fernández-Campusano",
}

[33] Mehdi Gheisari, Guojun Wang, Shuhong Chen,
An Edge Computing-enhanced Internet of Things Framework for Privacy-preserving in Smart City,
Computers & Electrical Engineering,Volume 81,2020,106504,ISSN 0045-7906,

```
  @article{GHEISARI2020106504,
  title = "An Edge Computing-enhanced Internet of Things Framework for Privacy-preserving in Smart City",
  journal = "Computers & Electrical Engineering",
  volume = "81",
  pages = "106504",
  year = "2020",
  issn = "0045-7906",
  doi = "https://doi.org/10.1016/j.compeleceng.2019.106504",
  url = "http://www.sciencedirect.com/science/article/pii/S0045790618329082",
  author = "Mehdi Gheisari and Guojun Wang and Shuhong Chen",
  }
```

[34] Gheisari, M., Alzubi, J., Zhang, X. *et al.* Correction to: A new algorithm for optimization of quality of service in peer to peer wireless mesh networks. *Wireless Netw* **25,** 4445 (2019). https://doi.org/10.1007/s11276-019-02016-4

```
  @Article{Gheisari2019,
  author="Gheisari, Mehdi
  and Alzubi, Jafar
  and Zhang, Xioabo
  and Kose, Utku
  and Saucedo, Jose Antonio Marmolejo",
  title="A new algorithm for optimization of quality of service in peer to peer wireless mesh networks",
  journal="Wireless Networks",
  year="2019",
  month="Mar",
  day="23",
  }
```

[35] X. Zhang, F. Fan, M. Gheisari and G. Srivastava, "A Novel Auto-Focus Method for Image Processing Using Laser Triangulation," in *IEEE Access*, vol. 7, pp. 64837-64843, 2019. doi: 10.1109/ACCESS.2019.2914186

@ARTICLE{8703430,
author={X. {Zhang} and F. {Fan} and M. {Gheisari} and G. {Srivastava}},
journal={IEEE Access},
title={A Novel Auto-Focus Method for Image Processing Using Laser Triangulation},
year={2019},
volume={7},
number={},
pages={64837-64843},
doi={10.1109/ACCESS.2019.2914186},
ISSN={2169-3536},
month={},}

[36] A. Hendalianpour *et al*., "Hybrid Model of IVFRN-BWM and Robust Goal Programming in Agile and Flexible Supply Chain, a Case Study: Automobile Industry," in *IEEE Access*, vol. 7, pp. 71481-71492, 2019.
doi: 10.1109/ACCESS.2019.2915309

@ARTICLE{8713447,
author={A. {Hendalianpour} and M. {Fakhrabadi} and X. {Zhang} and M. R. {Feylizadeh} and M. {Gheisari} and P. {Liu} and N. {Ashktorab}},
journal={IEEE Access},
title={Hybrid Model of IVFRN-BWM and Robust Goal Programming in Agile and Flexible Supply Chain, a Case Study: Automobile Industry},
year={2019},
volume={7},
number={},
pages={71481-71492},
ISSN={2169-3536},
month={},}

[37] M. Gheisari et al., "An Optimization Model for Software Quality Prediction With Case Study Analysis Using MATLAB," in IEEE Access, vol. 7, pp. 85123-85138, 2019, doi: 10.1109/ACCESS.2019.2920879.

@ARTICLE{8731856,
author={M. {Gheisari} and D. {Panwar} and P. {Tomar} and H. {Harsh} and X. {Zhang} and A. {Solanki} and A. {Nayyar} and J. A. {Alzubi}},
journal={IEEE Access},
title={An Optimization Model for Software Quality Prediction With Case Study Analysis Using MATLAB},
year={2019},
volume={7},
number={},
pages={85123-85138},
ISSN={2169-3536},
month={},}

[38] Noor, F, Sajid, A, Shah, SBH, Zaman, M, Gheisari, M, Mariappan, V. Bayesian estimation and prediction for Burr-Rayleigh mixture model using censored data. *Int J Commun Syst*. 2019;e4094. https://doi.org/10.1002/dac.4094

@article{doi:10.1002/dac.4094,
author = {Noor, Farzana and Sajid, Ahthasham and Shah, Syed Bilal Hussain and Zaman, Mehwish and Gheisari, Mehdi and Mariappan, Vinayagam},
title = {Bayesian estimation and prediction for Burr-Rayleigh mixture model using censored data},
journal = {International Journal of Communication Systems},
volume = {0},
number = {0},
pages = {e4094},
}

[39] M. Gheisari, Q. Pham, M. Alazab, X. Zhang, C. Fernández-Campusano and G. Srivastava, "ECA: An Edge Computing Architecture for Privacy-Preserving in IoT-Based Smart City," in *IEEE Access*, vol. 7, pp. 155779-155786, 2019. doi: 10.1109/ACCESS.2019.2937177

@ARTICLE{8811469,
author={M. {Gheisari} and Q. {Pham} and M. {Alazab} and X. {Zhang} and C. {Fernández-Campusano} and G. {Srivastava}},
journal={IEEE Access},
title={ECA: An Edge Computing Architecture for Privacy-Preserving in IoT-Based Smart City},
year={2019},
volume={7},
number={},
pages={155779-155786},
ISSN={2169-3536},
month={},}

[40] M. Gheisari *et al*., "A Survey on Clustering Algorithms in Wireless Sensor Networks: Challenges, Research, and Trends," *2020 International Computer Symposium (ICS)*, Tainan, Taiwan, 2020, pp. 294-299, doi: 10.1109/ICS51289.2020.00065.

@INPROCEEDINGS{9359086, author={M. {Gheisari} and A. A. {Abbasi} and Z. {Sayari} and Q. {Rizvi} and A. {Asheralieva} and S. {Banu} and F. M. {Awaysheh} and S. B. H. {Shah} and K. A. {Raza}}, booktitle={2020 International Computer Symposium (ICS)}, title={A Survey on Clustering Algorithms in Wireless Sensor Networks: Challenges, Research, and Trends}, year={2020}, volume={}, number={}, pages={294-299}, doi={10.1109/ICS51289.2020.00065}}

[41] Kannan, S.; Dhiman, G.; Natarajan, Y.; Sharma, A.; Mohanty, S.N.; Soni, M.; Easwaran, U.; Ghorbani, H.; Asheralieva, A.; Gheisari, M. Ubiquitous Vehicular Ad-Hoc Network Computing Using Deep Neural Network with IoT-Based Bat Agents for Traffic Management. *Electronics* **2021**, *10*, 785. https://doi.org/10.3390/electronics10070785

@Article{electronics10070785,
AUTHOR = {Kannan, Srihari and Dhiman, Gaurav and Natarajan, Yuvaraj and Sharma, Ashutosh and Mohanty, Sachi Nandan and Soni, Mukesh and Easwaran, Udayakumar and Ghorbani, Hamidreza and Asheralieva, Alia and Gheisari, Mehdi},
TITLE = {Ubiquitous Vehicular Ad-Hoc Network Computing Using Deep Neural Network with IoT-Based Bat Agents for Traffic Management},

```
  JOURNAL = {Electronics},
  VOLUME = {10},
  YEAR = {2021},
  NUMBER = {7},
  ARTICLE-NUMBER = {785},
  URL = {https://www.mdpi.com/2079-9292/10/7/785},
  }
```

[42] Movassagh, A.A., Alzubi, J.A., Gheisari, M. *et al.* Artificial neural networks training algorithm integrating invasive weed optimization with differential evolutionary model. *J Ambient Intell Human Comput* (2021). https://doi.org/10.1007/s12652-020-02623-6

```
  @Article{Movassagh2021,
    author      = {Ali Akbar Movassagh and Jafar A. Alzubi and Mehdi Gheisari and
Mohamadtaghi Rahimi and Senthilkumar Mohan and Aaqif Afzaal Abbasi and Narjes Nabipour},
    journal   = {Journal of Ambient Intelligence and Humanized Computing},
    title      = {Artificial neural networks training algorithm integrating invasive
weed optimization with differential evolutionary model},
    year      = {2021},
    month     = {mar},
    doi       = {10.1007/s12652-020-02623-6},
    publisher = {Springer Science and Business Media {LLC}},
  }
```

[43] Shao, Yongfu, et al. "Optimization of Ultrasound Information Imaging Algorithm in Cardiovascular Disease Based on Image Enhancement." *Mathematical Problems in Engineering* 2021 (2021).

```
  @article{shao2021optimization,
    title={Optimization of Ultrasound Information Imaging Algorithm in Cardiovascular
Disease Based on Image Enhancement},
    author={Shao, Yongfu and Wu, Jue and Ou, Hongping and Pei, Min and Liu, Li and
Movassagh, Ali Akbar and Sharma, Ashutosh and Dhiman, Gaurav and Gheisari, Mehdi and
Asheralieva, Alia},
    journal={Mathematical Problems in Engineering},
    volume={2021},
    year={2021},
    publisher={Hindawi}
  }
```

[44] Gheisari, M., Najafabadi, H. E., Alzubi, J. A., Gao, J., Wang, G., Abbasi, A. A., & Castiglione, A. (2021). OBPP: An ontology-based framework for privacy-preserving in IoT-based smart city. *Future Generation Computer Systems*.

```
  @article{GHEISARI20211,
  title = {OBPP: An ontology-based framework for privacy-preserving in IoT-based smart
city},
  journal = {Future Generation Computer Systems},
  volume = {123},
  pages = {1-13},
  year = {2021},
  issn = {0167-739X},
  author = {Mehdi Gheisari and Hamid Esmaeili Najafabadi and Jafar A. Alzubi and Jiechao
Gao and Guojun Wang and Aaqif Afzaal Abbasi and Aniello Castiglione},
  }
```

[45] Hosseini Bamakan S M, Rahbar E, Gheisari M. Role of Wearable Technology in the Diagnosis and Prevention of COVID-19. J Research Health. 2021; 11 (4) :1-1

```
@ARTICLE{Hosseini Bamakan,
author = {Hosseini Bamakan, Seyed Mojtaba and Rahbar, Ehsan and Gheisari, Mehdi and },
title = {Role of Wearable Technology in the Diagnosis and Prevention of COVID-19},
volume = {11},
number = {4},
eprint = {http://jrh.gmu.ac.ir/article-1-1961-en.docx},
journal = {Journal of Research and Health},
doi = {10.32598/JRH.11.4.1903.1},
year = {2021}
}
```

[46] S. Afrasiabi, B. Behdani, M. Afrasiabi, M. Mohammadi, A. Asheralieva and M. Gheisari, "Differential Protection of Power Transformers based on RSLVQ-Gradient Approach Considering SFCL," *2021 IEEE Madrid PowerTech*, 2021, pp. 1-6, doi: 10.1109/PowerTech46648.2021.9494873.

```
@INPROCEEDINGS{9494873, author={Afrasiabi, Shahabodin and Behdani, Behzad and Afrasiabi, Mousa and Mohammadi, Mohammad and Asheralieva, Alia and Gheisari, Mehdi}, booktitle={2021 IEEE Madrid PowerTech}, title={Differential Protection of Power Transformers based on RSLVQ-Gradient Approach Considering SFCL}, year={2021}, volume={}, number={}, pages={1-6}, doi={10.1109/PowerTech46648.2021.9494873}}
```

[47] B. Behdani, M. Allahbakhshi, A. Asheralieva and M. Gheisari, "Analytical Method for Ferroresonance Solutions in Series Compensated Power Systems due to GICs: A Graphical Approach," *2021 IEEE Madrid PowerTech*, 2021, pp. 1-6, doi: 10.1109/PowerTech46648.2021.9494921.

```
@INPROCEEDINGS{9494921, author={Behdani, Behzad and Allahbakhshi, Mehdi and Asheralieva, Alia and Gheisari, Mehdi}, booktitle={2021 IEEE Madrid PowerTech}, title={Analytical Method for Ferroresonance Solutions in Series Compensated Power Systems due to GICs: A Graphical Approach}, year={2021}, volume={}, number={}, pages={1-6}, doi={10.1109/PowerTech46648.2021.9494921}}
```

[48] Natarajan, Y., et al.: An IoT and machine learning-based routing protocol for reconfigurable engineering application. *IET Commun.* 00, 1– 12 (2021). https://doi.org/10.1049/cmu2.12266

```
@Article{Natarajan2021,
  author  = {Yuvaraj Natarajan and Kannan Srihari and Gaurav Dhiman and Selvaraj Chandragandhi and Mehdi Gheisari and Yang Liu and Cheng-Chi Lee and Krishna Kant Singh and Kusum Yadav and Hadeel Fahad Alharbi},
  journal = {{IET} Communications},
  title   = {An {IoT} and machine learning-based routing protocol for reconfigurable engineering application},
  year    = {2021},
  month   = {aug},
  doi     = {10.1049/cmu2.12266},
  publisher = {Institution of Engineering and Technology ({IET})},
}
```

[49] Mangla, Monika, et al. "A Proposed Framework for Autonomic Resource Management in Cloud Computing Environment." *Autonomic Computing in Cloud Resource Management in Industry 4.0*. Springer, Cham, 2021. 177-193.

```
@incollection{mangla2021proposed,
  title={A Proposed Framework for Autonomic Resource Management in Cloud Computing Environment},
  author={Mangla, Monika and Deokar, Sanjivani and Akhare, Rakhi and Gheisari, Mehdi},
  booktitle={Autonomic Computing in Cloud Resource Management in Industry 4.0},
  pages={177--193},
```

```
    year={2021},
    publisher={Springer}
  }
```

[50] Li, Lintao, et al. "Research on TCP Performance Model and Transport Agent Architecture in Broadband Wireless Network." *Scalable Computing: Practice and Experience* 22.2 (2021): 193-201.

```
  @article{li2021research,
    title={Research on TCP Performance Model and Transport Agent Architecture in Broadband Wireless Network},
    author={Li, Lintao and Sharma, Parv and Gheisari, Mehdi and Sharma, Amit},
    journal={Scalable Computing: Practice and Experience},
    volume={22},
    number={2},
    pages={193--201},
    year={2021}
  }
```

[51] S. Afrasiabi, B. Behdani, M. Afrasiabi, M. Mohammadi, Y. Liu and M. Gheisari, "A Comparative Analysis of Artificial Intelligence for Power Transformer Differential Protection," *2021 IEEE International Conference on Environment and Electrical Engineering and 2021 IEEE Industrial and Commercial Power Systems Europe (EEEIC / I&CPS Europe)*, 2021, pp. 1-6, doi: 10.1109/EEEIC/ICPSEurope51590.2021.9611033.

```
  @INPROCEEDINGS{9611033,
    author={Afrasiabi, Shahabodin and Behdani, Behzad and Afrasiabi, Mousa and Mohammadi, Mohammad and Liu, Yang and Gheisari, Mehdi},
    booktitle={2021 IEEE International Conference on Environment and Electrical Engineering and 2021 IEEE Industrial and Commercial Power Systems Europe (EEEIC / I CPS Europe)},
    title={A Comparative Analysis of Artificial Intelligence for Power Transformer Differential Protection},
    year={2021},
    volume={},
    number={},
    pages={1-6},
    doi={10.1109/EEEIC/ICPSEurope51590.2021.9611033}}
```

[52] M. Pazhoohesh, M. S. Javadi, M. Gheisari, S. Aziz and R. Villa, "Dealing with Missing Data in the Smart Buildings using Innovative Imputation Techniques," *IECON 2021 – 47th Annual Conference of the IEEE Industrial Electronics Society*, 2021, pp. 1-7, doi: 10.1109/IECON48115.2021.9612650.

```
  @INPROCEEDINGS{9612650,
    author={Pazhoohesh, Mehdi and Javadi, Mohammad Sadegh and Gheisari, Mehdi and Aziz, Saddam and Villa, Raffaella},
    booktitle={IECON 2021 – 47th Annual Conference of the IEEE Industrial Electronics Society},
    title={Dealing with Missing Data in the Smart Buildings using Innovative Imputation Techniques},
    year={2021},
    volume={},
    number={},
    pages={1-7},
    doi={10.1109/IECON48115.2021.9612650}}
```

[53] K. A. Raza, A. Asheralieva, M. M. Karim, K. Sharif, M. Gheisari and S. Khan, "A Novel Forwarding and Caching Scheme for Information-Centric Software-Defined Networks," *2021 International Symposium on Networks, Computers and Communications (ISNCC)*, 2021, pp. 1-8, doi: 10.1109/ISNCC52172.2021.9615667.

@INPROCEEDINGS{9615667, author={Raza, Khuhawar Arif and Asheralieva, Alia and Karim, Md Monjurul and Sharif, Kashif and Gheisari, Mehdi and Khan, Salabat}, booktitle={2021 International Symposium on Networks, Computers and

Communications (ISNCC)}, title={A Novel Forwarding and Caching Scheme for Information-Centric Software-Defined Networks}, year={2021}, volume={}, number={}, pages={1-8}, doi={10.1109/ISNCC52172.2021.9615667}}

[54] Yogesh Kumar, Apeksha Koul, Pushpendra Singh Sisodia, Jana Shafi, Verma Kavita, Mehdi Gheisari, Mohamad Bagher Davoodi, "Heart Failure Detection Using Quantum-Enhanced Machine Learning and Traditional Machine Learning Techniques for Internet of Artificially Intelligent Medical Things", Wireless Communications and Mobile Computing, vol. 2021, Article ID 1616725, 16 pages, 2021.

@Article{Kumar2021,
author = {Yogesh Kumar and Apeksha Koul and Pushpendra Singh Sisodia and Jana Shafi and Verma Kavita and Mehdi Gheisari and Mohamad Bagher Davoodi},
journal = {Wireless Communications and Mobile Computing},
title = {Heart Failure Detection Using Quantum-Enhanced Machine Learning and Traditional Machine Learning Techniques for Internet of Artificially Intelligent Medical Things},
year = {2021},
month = {dec},
pages = {1--16},
volume = {2021},
doi = {10.1155/2021/1616725},
editor = {Mohammad R Khosravi},
publisher = {Hindawi Limited},
}

[55]
@book{gupta2021cancer,
title={Chapter 7th, Cancer Prediction for Industrial IoT 4.0: A Machine Learning Perspective},
author={Ashish Kumar, Revant Singh Rai, Mehdi Gheisari},
isbn={9781000508581},
series={Prediction of cervical cancer using machine learning},
url={https://books.google.co.in/books?id=vDxOEAAAQBAJ},
year={2021},
publisher={CRC Press}
}

[56] Gheisari, Mehdi, et al. "A novel enhanced algorithm for efficient human tracking." *Int J Inf & Commun Technol* 11.1 (2022): 1-7.
@article{gheisari2022novel,
title={A novel enhanced algorithm for efficient human tracking},
author={Gheisari, Mehdi and Safari, Zohreh and Almasi, Mohammad and Sridharan, Abel and GK, Ragesh and Liu, Yang and Abbasi, Aaqif Afzaal},
journal={Int J Inf \& Commun Technol},
volume={11},
number={1},
pages={1--7},
year={2022}
}

[57] Abdullah Ajmal, Hamza Aldabbas, Rashid Amin, Sundas Ibrar, Bader Alouffi, Mehdi Gheisari, "Stress-Relieving Video Game and Its Effects: A POMS Case Study", *Computational Intelligence and Neuroscience*, vol. 2022, Article ID 4239536, 11 pages, 2022. https://doi.org/10.1155/2022/4239536

[58] Yongsheng Rao, Saeed Kosari, Mehdi Gheisari, "New Results in Vague Incidence Graphs with Application", Journal of Function Spaces, vol. 2022, Article ID 3475536, 7 pages, 2022. https://doi.org/10.1155/2022/3475536

```
@article{rao2022new,
  title={New Results in Vague Incidence Graphs with Application},
  author={Rao, Yongsheng and Kosari, Saeed and Gheisari, Mehdi},
  journal={Journal of Function Spaces},
  volume={2022},
  year={2022},
  publisher={Hindawi}
}
```

[59] J. A. Alzubi *et al.*, "A Dynamic SDN-based Privacy-Preserving Approach for Smart City Using Trust Technique," *2022 9th Iranian Joint Congress on Fuzzy and Intelligent Systems (CFIS)*, 2022, pp. 1-5, doi: 10.1109/CFIS54774.2022.9756458.

```
@INPROCEEDINGS{9756458,
  author={Alzubi, Jafar A. and Movassagh, AliAkbar and Gheisari, Mehdi and Najafabadi, Hamid Esmaeili and Abbasi, Aaqif Afzaal and Liu, Yang and Pingmei, Zhou and Izadpanahkakhk, Mahdieh and Najafabadi, AmirHossein Pourishaban},
  booktitle={2022 9th Iranian Joint Congress on Fuzzy and Intelligent Systems (CFIS)},
  title={A Dynamic SDN-based Privacy-Preserving Approach for Smart City Using Trust Technique},
  year={2022},
  volume={},
  number={},
  pages={1-5},
  doi={10.1109/CFIS54774.2022.9756458}}
```

[60] Yongsheng Rao, Saeed Kosari, Mehdi Gheisari, "New Results in Vague Incidence Graphs with Application", *Journal of Function Spaces*, vol. 2022, Article ID 3475536, 7 pages, 2022. https://doi.org/10.1155/2022/3475536

[61] Moshayedi, Ata Jahangir et al. "Automation Attendance Systems Approaches: A Practical Review." *BOHR International Journal of Internet of Things Research* (2021): n. pag.

```
@article{Moshayedi2021AutomationAS,
  title={Automation Attendance Systems Approaches: A Practical Review},
  author={Ata Jahangir Moshayedi and Atanu Roy and Liefa Liao and Mehdi Gheisari and Aaqif Afzaal Abbasi and Seyed Mojtaba Hosseini Bamakan},
  journal={BOHR International Journal of Internet of Things Research},
  year={2021}
}
```

[62] Mehdi Gheisari, et al. "An efficient cluster head selection for wireless sensor network-based smart agriculture systems". Computers and Electronics in Agriculture, Elsevier, 198, 107105, 2022.

```
@article{gheisari2022efficient,
  title={An efficient cluster head selection for wireless sensor network-based smart agriculture systems},
  author={Gheisari, Mehdi and Yaraziz, Mahdi Safaei and Alzubi, Jafar A and Fern{\'a}ndez-Campusano, Christian and Feylizadeh, Mohammad Reza and Pirasteh, Saied and Abbasi, Aaqif Afzaal and Liu, Yang and Lee, Cheng-Chi},
  journal={Computers and Electronics in Agriculture},
  volume={198},
  pages={107105},
  year={2022},
  publisher={Elsevier}
}
```

```
@article{GHEISARI2022107105,
title = {An efficient cluster head selection for wireless sensor network-based smart agriculture systems},
journal = {Computers and Electronics in Agriculture},
volume = {198},
pages = {107105},
year = {2022},
}
```

[63] Gheisari, M., Javadpour, A., Gao, J. *et al.* PPDMIT: a lightweight architecture for privacy-preserving data aggregation in the Internet of Things. *J Ambient Intell Human Comput* (2022). https://doi.org/10.1007/s12652-022-03866-1

[1] A. Javadpour, G. Wang, and S. Rezaei, "Resource Management in a Peer to Peer Cloud Network for IoT," *Wirel. Pers. Commun.*, 2020.

[2] M. Badra and S. Zeadally, "Lightweight and efficient privacy-preserving data aggregation approach for the smart grid," *Ad Hoc Networks*, vol. 64, pp. 32–40, 2017.

[3] A. Javadpour, G. Wang, S. Rezaei, and S. Chend, "Power Curtailment in Cloud Environment Utilising Load Balancing Machine Allocation," in *2018 IEEE SmartWorld, Ubiquitous Intelligence Computing, Advanced Trusted Computing, Scalable Computing Communications, Cloud Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI)*, 2018, pp. 1364–1370.

[4] Z. Guan *et al.*, "APPA: An anonymous and privacy preserving data aggregation scheme for fog-enhanced IoT," *J. Netw. Comput. Appl.*, vol. 125, pp. 82–92, 2019.

[5] J. Rachels, "Why privacy is important," in *Privacy*, Routledge, 2017, pp. 11–21.

[6] Q. Liu, G. Wang, F. Li, S. Yang, and J. Wu, "Preserving privacy with probabilistic indistinguishability in weighted social networks," *IEEE Trans. Parallel Distrib. Syst.*, vol. 28, no. 5, pp. 1417–1429, 2016.

[7] M. C. Lee, R. Mitra, E. Lazaridis, A.-C. Lai, Y. K. Goh, and W.-S. Yap, "Data privacy preserving scheme using generalised linear models," *Comput. Secur.*, vol. 69, pp. 142–154, 2017.

[8] T. Peng, Q. Liu, D. Meng, and G. Wang, "Collaborative trajectory privacy preserving scheme in location-based services," *Inf. Sci. (Ny).*, vol. 387, pp. 165–179, 2017.

[9] E. Aïmeur, S. Gambs, and A. Ho, "UPP: User Privacy Policy for Social Networking Sites," *2009 Fourth Int. Conf. Internet Web Appl. Serv.*, pp. 267–272, 2009.

[10] M. Slimp and R. Bartels, *How the Internet of Things is Changing Our Colleges, Our Classrooms, and Our Students*. Rowman & Littlefield Publishers, 2019.

[11] B. U. I. Khan, R. F. Olanrewaju, F. Anwar, R. N. Mir, and A. R. Najeeb, "A critical insight into the effectiveness of research methods evolved to secure IoT ecosystem," *Int. J. Inf. Comput. Secur.*, vol. 11, no. 4–5, pp. 332–354, 2019.

[12] Beecham, "IoT security threat map,Online Report Beecham research," *online Rep. , http//www.beechamresearch.com/download.aspx?id=43*, 2021.

[13] X. Ding, Q. Yu, J. Li, J. Liu, and H. Jin, "Distributed anonymization for multiple data providers in a cloud system," in *International Conference on Database Systems for Advanced Applications*, 2013, pp. 346–360.

[14] Y. A. A. S. Aldeen, M. Salleh, and M. A. Razzaque, "A comprehensive review on privacy preserving data mining," *Springerplus*, vol. 4, no. 1, p. 694, 2015.

[15] M. Martonosi, "Keynotes: Internet of Things: History and hype, technology and policy," in *2016 49th Annual IEEE/ACM International Symposium on Microarchitecture (MICRO)*, 2016, pp. 1–2.

[16] H. Zhu, X. Meng, and G. Kollios, "Privacy Preserving Similarity Evaluation of Time Series Data.," in *EDBT*, 2014, vol. 2014, pp. 499–510.

[17] S. Ruj and A. Nayak, "A decentralized security framework for data aggregation and access control in smart grids," *IEEE Trans. Smart Grid*, vol. 4, no. 1, pp. 196–205, 2013.

[18] R. Raju, R. Komalavalli, and V. Kesavakumar, "Privacy maintenance collaborative data mining-a practical approach," in *2009 Second International Conference on Emerging Trends in Engineering & Technology*, 2009, pp. 307–311.

[19] R. Mukkamala and V. G. Ashok, "Fuzzy-based methods for privacy-preserving data mining," in *2011 Eighth International Conference on Information Technology: New Generations*, 2011, pp. 348–353.

[20] P. Kamakshi and A. V. Babu, "Automatic detection of sensitive attribute in PPDM," in *2012 IEEE international conference on computational intelligence and computing research*, 2012, pp. 1–5.

[21] J. Lai, Y. Li, R. H. Deng, J. Weng, C. Guan, and Q. Yan, "Towards semantically secure outsourcing of association rule mining on categorical data," *Inf. Sci. (Ny).*, vol. 267, pp. 267–286, 2014.

[22] R. Lu, K. Heung, A. H. Lashkari, and A. A. Ghorbani, "A lightweight privacy-preserving data aggregation scheme for fog computing-enhanced IoT," *IEEE Access*, vol. 5, pp. 3302–3312, 2017.

[23] C. A. Melchor and P. Gaborit, “A fast private information retrieval protocol,” in *2008 IEEE international symposium on information theory*, 2008, pp. 1848–1852.
[24] T. Tassa, “Secure mining of association rules in horizontally distributed databases,” *IEEE Trans. Knowl. Data Eng.*, vol. 26, no. 4, pp. 970–983, 2013.
[25] Ashourian, Mohsen, et al "An Improved Node Scheduling Scheme for Resilient Packet Ring Network." Majlesi Journal of Electrical Engineering 9.2 (2015): 43
[26] Kannan, S.; et al, M. Ubiquitous Vehicular Ad-Hoc Network Computing Using Deep Neural Network with IoT-Based Bat Agents for Traffic Management. *Electronics* 2021, *10*, 785. https://doi.org/10.3390/electronics10070785
[27] U. M. Aïvodji, S. Gambs, and A. Martin, “IOTFLA : AA secured and privacy-preserving smart home architecture implementing federated learning,” *Proc. - 2019 IEEE Symp. Secur. Priv. Work. SPW 2019*, pp. 175–180, 2019.
[28] X. Zhang, C. Liu, S. Nepal, C. Yang, W. Dou, and J. Chen, “Combining top-down and bottom-up: scalable sub-tree anonymization over big data using MapReduce on cloud,” in *2013 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications*, 2013, pp. 501–508.
[29] Gheisari, Mehdi, et al . "Data Storages in Wireless Sensor Networks to Deal With Disaster Management." Emergency and Disaster Management: Concepts, Methodologies, Tools, and Applications. *IGI Global*, 2019. 655-682.
[30] Noor, F, Sajid, et al, V. Bayesian estimation and prediction for Burr-Rayleigh mixture model using censored data. I*nt J Commun Syst*. 2019;e4094. https://doi.org/10.1002/dac.4094
[31] Natarajan, Y., et al.: An IoT and machine learning-based routing protocol for reconfigurable engineering application. *IET Commun*. 00, 1– 12 (2021). https://doi.org/10.1049/cmu2.12266
[32] Mangla, Monika, et al. "A Proposed Framework for Autonomic Resource Management in Cloud Computing Environment." *Autonomic Computing in Cloud Resource Management in Industry 4.0. Springer, Cham*, 2021. 177-193.
[33] Li, Lintao, et al. "Research on TCP Performance Model and Transport Agent Architecture in Broadband Wireless Network." Scalable Computing: Practice and Experience 22.2 (2021): 193-201.
[34] P. P. Jayaraman, X. Yang, A. Yavari, D. Georgakopoulos, and X. Yi, “Privacy preserving Internet of Things: From privacy techniques to a blueprint architecture and efficient implementation,” *Futur. Gener. Comput. Syst.*, vol. 76, pp. 540–549, 2017.
[35] P. Zheng and J. Huang, “An efficient image homomorphic encryption scheme with small ciphertext expansion,” in *Proceedings of the 21st ACM international conference on Multimedia*, 2013, pp. 803–812.
[36] F. Mendel, C. Rechberger, and M. Schläffer, “MD5 is weaker than weak: Attacks on concatenated combiners,” in *International Conference on the Theory and Application of Cryptology and Information Security*, 2009, pp. 144–161.
[37] Gheisari, Mehdi, et al. "MAPP: A Modular Arithmetic Algorithm for Privacy Preserving in IoT." Ubiquitous Computing and Communications (ISPA/IUCC), *2017 IEEE International Symposium on Parallel and Distributed Processing with Applications and 2017 IEEE International Conference on. IEEE*, 2017.
[38] Gheisari, M., Najafabadi, H. E., Alzubi, J. A., Gao, J., Wang, G., Abbasi, A. A., & Castiglione, A. (2021). OBPP: An ontology-based framework for privacy-preserving in IoT-based smart city. *Future Generation Computer Systems*.
[39] N.-S. Jho, J. Y. Hwang, J. H. Cheon, M.-H. Kim, D. H. Lee, and E. S. Yoo, “One-way chain based broadcast encryption schemes,” in Annual International Conference on the Theory and Applications of Cryptographic Techniques, 2005, pp. 559–574.
[40] Porkar, Payam, et al. "A Comparison with Two Sensor Data Storages in Energy." International Conference on Computer and Computer Intelligence (ICCCI 2011). ASME Press, 2011.
[41] P. Erdos and J. Schönheim, “On the set of non pairwise coprime divisors of a number,” in *Combinatorial theory and its applications, I (Proc. Colloq., Balatonfüred, 1969)*, 1969, pp. 369–376.