Preserving Balance between Privacy and Data Integrity in Edge-Assisted Internet of Things

Tian Wang, Md Zakirul Alam Bhuiyan, Guojun Wang, Lianyong Qi*, Jie Wu, and Thaier Hayajneh

***Abstract*—Internet of Things (IoT) devices and the edge jointly broaden the IoT's sensing capability and the monitoring scope for various applications. Though accessing sensing data and making decisions through IoT smart devices turns out to be commonplace, it is challenging to guarantee user privacy and preserve the accuracy (integrity) of the collected data. The IoT smart devices frequently lose either IoT user's privacy or data integrity. This also makes it crucial to put a threshold on the cost of computation and load of the IoT devices, as gradually more IoT services demand access to the resources that devices offer. In this paper, we propose `BalancePIC`, a scheme that attempts to preserve a balance in the three aspects (user privacy, data integrity in edge-assisted IoT devices, and the computational cost). It achieves the balance through a balanced truth discovery approach and a proposed enhanced technique for data privacy, which are used in IoT device and edge server interactions. It authenticates the IoT user participation with privacy in the truth discovery process through a biometric-ECC based authentication algorithm. The nature of the `BalancePIC` scheme is to straightforwardly provide the likelihood for a simple amendment on the cryptography technique and weight assignment. This lessens the overall computational cost for the IoT user devices but also restricts the communications between the user devices and the edge server, which is important for data integrity. We present an enhanced technique to preserve privacy by guarding the user from potential threats and suspicious data collection parties. To achieve this, `BalancePIC` takes steps to blur the original sensory data of the device by processing results in groups called zones. Simulation result analysis provides evidence for the balance preservation in the three aspects.**

***Index Terms*—Internet of Things, data collection, security, privacy, data integrity, truth discovery, Biometric, ECC**

I. Introduction

Internet of Things (IoT) devices including smartphone, smartwatches, smartglasses, and body sensors are broadly available and interconnected by various forms of communication technologies to the Internet. There are diverse applications of IoT such as crowd sensing, smart home, smart city, body networks, and so on [1], [2]. This has led to a dramatic increase in the growth of sensory-data resources for the IoT. However, there are severe constraints in the IoT devices, including computational ability, energy, storage, and security, which degrade the performance of IoT applications. Recently, edge computing is being proposed as a new computing model in which a near-user high-end device with stronger computing power provides required resources for the applications of resource-constrained IoT devices. The edge computing-based IoT (or edge-assisted IoT) scheme is able to mitigate some challenges of communication and high computation costs, as well as low-quality of local decision-making, and low flexibility [1], [3].

One of the primary challenges with the edge-based IoT system is that the IoT sensory data is susceptible to attacks and threats, particularly, insider attacks that often happens in the IoT device tier and the network communication tier [2]–[4]. Different from insider attacks, outsider attacks can be challenged by conventional security methods, such as authentication, authorization, and auditing [5], [6]. The first priority of security is to assure the availability and functionality of IoT applications. Nevertheless, traditional security mechanisms, including AES, Blowfish, DES, RSA, ECC require a large computational cost to resist some internal attacks effectively, especially some user privacy and data integrity attacks in resource-constrained IoT [7]. There are various authentication techniques available that are designed to solve data integrity problems [8]. Though edge-assisted IoT can support security with reduced computation when suing advanced cryptography, the security aspects associated with IoT devices are still concerning. There are weaknesses in user anonymity and other ideal security functions that are seen to be vulnerable to cyberattacks [6]. More importantly, those traditional security mechanisms still consume a lot of resources of IoT devices leading to a huge influence on the IoT application performance and system lifetime. In this context, only simple security protection mechanisms, i.e., authenticated key exchange and access control, for the communications are possible for IoT applications [1], [6].

A crucial concern about the IoT applications is that the sensory data offered by different devices are frequently not accurate in terms of user privacy (anonymity or compromised sensory value) [2]. A method is to combine the likelihood of a user offering trustworthy data with the IoT user weight during the sensor data aggregation and aggregated output productions, which are supposed to be close to the data provided by trustworthy IoT users. The main difficulty is that the IoT user trustworthiness is usually anonymous a priori and can be obtained from acquired sensor data. To tackle the difficulty, the truth discovery [9]–[12] is applied to decide on true facts from untrustworthy user information.

T. Wang is with the Department of Computer Science and Engineering, Shaoxing University, Shaoxing, China 312000, and College of Computer Science and Technology, Huaqiao University, Xiamen, Fujian, China 361021.

M. Bhuiyan and T. Hayajneh are with the Department of Computer and Information Sciences, Fordham University, NY, USA 10458.

G. Wang is with School of Computer Science and Educational Software, Guangzhou University, China.

L. Qi is with the School of Information Science and Engineering, Qufu Normal University, China (corresponding author: lianyongqi@gmail.com).

J. Wu is with the Department of Computer and Information Sciences, Temple University, USA 10121.

Received on mmddyyy, Revised on mmddyyy, Accepted on mmddyyy

The objective of the truth discovery approach is to derive exact evidence from untrustworthy data of IoT devices. Three important requirements are revealed by the process of determining exact facts: user privacy, data integrity, and minimal computational cost as necessitated by IoT devices when applying for different applications in practice. Current truth discovery methods and some IoT applications such as crowdsensing [10]–[12] have a variety of outputs, from private to accurate as well as a spectrum of computation cost of the IoT devices. Most methods often dedicate at least any of the three requirements to guarantee other or straightforwardly discard requirement [6]. A current method, privacy-preserving truth discovery (PPTD) [9], [13] concentrates on maintaining user privacy of IoT devices in applications. Nevertheless, to achieve this PPTD method conceals the collected sensing data and demands that a large size of the sample before the approximated truth turns out to be exact. It happens, particularly, when the approximated ground truth is set arbitrarily. This is to make a straightforward sacrifice toward the accuracy of the collected data for user privacy.

In this paper, we propose BalancePIC, a scheme that attempts to preserve a balance in the three aspects (user privacy and data integrity in edge-assisted IoT, the computational cost). BalancePIC can overcome the limitations of the previous schemes to some extent. It achieves this through a balanced truth discovery approach and an enhanced technique for data privacy. It authenticates the IoT user participation in the truth discovery process through a biometric-ECC based cryptography algorithm. The nature of the BalancePIC scheme is to straightforwardly provide the likelihood for a simple amendment on the cryptography technique and weight allocation. It lessens the overall computation cost of IoT user devices in addition to restricting communications among the user IoT devices and the edge server. This is important to the integrity of the IoT device data.

An enhanced technique maintains user privacy by protecting the user data from potential threats and untrustworthy data collection parties. To achieve this, BalancePIC attempts to combine some functions of privacy preservation via the method of truth discovery and apply a concept of zoning and data distorting at each IoT device user level. We put a threshold on the IoT user devices' participation in the computation of the approximated ground truth. This outcome is a reduction in both the cost of computation and load on IoT user devices and the damage, which mainly occurs due to the security threats/attacks on data integrity. BalancePIC handles each user device as a database resource of sensing data. It links to the user device that requires a low cost (in terms of computation) output, and leaves the user device for other services.

The contributions of this paper are four-fold.

- This paper proposes BalancePIC scheme to provide a balance in the user privacy, and data integrity and computation cost in edge-assisted IoT devices.
- It provides a biometric-ECC based authentication technique through a simple amendment on the traditional cryptography technique and weight assignment for data integrity.
- To authenticate the IoT user participation with privacy, it utilizes enhanced truth discovery technique to protect IoT device users from potential threats, such as untrusted data collection parties.
- Its performance results achieved through simulations provide evidence for the preservation of the balance in user privacy, data integrity, and the cost of computation.

The rest of the paper is organized as follows. We explain the design of the proposed work in Section II. The development methods of the scheme are described in Section III. Section IV offers the biometric-ECC based authentication algorithm, and Section V describes the enhanced technique. We conduct the performance analysis through the simulation in Section VI. Finally, the conclusion of this paper is provided in Section VII.

II. The Design of BalancePIC

In this section, we first provide the definition of the edge-assisted IoT network and then provide threat models. At the end, we provide the design overview of the proposed BalancePIC scheme.

A. Edge-assisted IoT Network Development

IoT brings auspicious solutions to develop resource consuming and computation-intensive facilities and functions in various fields, including smart-city, smart-grid, e-healthcare, and industrial automation. This revolution facilitates collaborations between things and people and new chances to change our society and enhance our life. With the growth of associated things, a large quantity of data is produced from diverse services and functions, concluding with devastating stress on data computational cost and storage, transmission, and usage. Transferring the acquired data from the IoT devices to the cloud for storage and security analysis can utilize a huge quality of costly bandwidth. 45% of generated data require to be stored and handled at the edge of IoT networks or close to IoT devices. Furthermore, all of the things produce data continuously that should be evaluated speedily to fulfill the IoT application demands. Centralized or global data storage and investigation cannot pay for the requirements of data-centric services, latency-sensitive, and security-sensitive applications. This concept is called edge-assisted IoT [3], [14].

We consider a hierarchical edge-assisted IoT network system that is partitioned into three tiers: 1) the data collection tier, 2) the processing tiers, and 3) the application service tier. As shown in Fig. 1, both the IoT network and edge network are part of the data collection tier in the architecture, while the edge server platform is part of the data processing tier and the application service tier, and the cloud services lie in the application service tier. For the data collection, a set of IoT devices such as smartphone sensors are randomly or uniformly distributed for a particular monitoring application, e.g., crowdsensing, patient e-healthcare. IoT devices are connected to one or more edge servers [3].

The IoT devices collect the application data and then forward the data to the edge server through a wireless communication channel. Normally, an IoT device has serious resource limitations, including storage, computing, and power

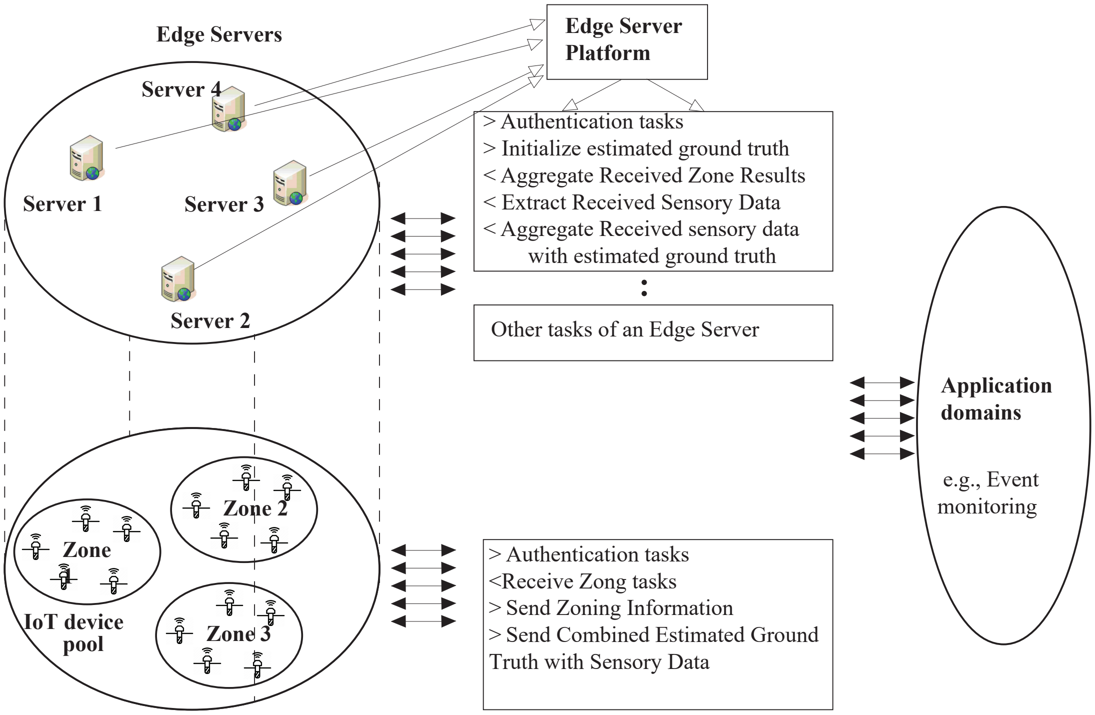

Edge Servers
Server 4
Server 1
Server 3
Server 2
Edge Server Platform
> Authentication tasks
> Initialize estimated ground truth
< Aggregate Received Zone Results
< Extract Received Sensory Data
< Aggregate Received sensory data with estimated ground truth
Other tasks of an Edge Server
Application domains
e.g., Event monitoring
Zone 2
Zone 1
Zone 3
IoT device pool
> Authentication tasks
<Receive Zong tasks
> Send Zoning Information
> Send Combined Estimated Ground Truth with Sensory Data

Fig. 1. A typical example design of `BalancePIC` scheme

resources, while edge servers are distributed computing devices usually having the more powerful capability. The edge server devices carry out data processing at the edge between the IoT network and cloud, near the IoT devices of the data. It lessens communication resources such as bandwidth required in IoT devices and Cloud data storage by carrying out analytics and knowledge generation at or near the IoT devices of the data. There are several other modules that can be in the second or third tiers, including the service access model, enterprise-level software stacks, and operating on the edge of an IoT network deployment provides the greatest basis of the edge.

A number of edge devices across the network can offload the computational load away from the Cloud, and can notably lessen the bandwidth and latency in packet exchanges. Moreover, the distributed edge servers can balance IoT traffic and avoid the traffic peaks in IoT networks, lessening the communication latency between edge server /cloudlet servers and end (application) users, as well as lessening response times for real-time IoT applications in comparison with traditional cloud services. Furthermore, by sending computation and communication overhead from IoT devices with severe energy constraints, the IoT system can extend the lifetime of the individual devices. In some applications of IoT with low latency or high timeliness, such as remote healthcare, the user needs to access the device data by using a mobile device.

Though the distributed scheme has various advantages for IoT applications, the security and privacy with the scheme is a significant concern. As edge server processes data at the edge, the privacy-sensitive information connected to application users can be compromised, as the sensed data of IoT devices is collected at the edge server, which might be more susceptible to modification than the cloud servers [15], [16]. As a result, privacy protection is usually assumed in edge devices. There are numerous privacy-preserving mechanisms, such as local differential privacy [17] and differential privacy with high utility [18]. However, many of them require significant computation and computation tasks to protect the privacy of application users in the edge-based IoT environment.

The idea of *BalancePIC* is to maintain a balance between privacy-preserving and data integrity regarding computation cost bandwidth, etc. `BalancePIC` includes a balanced truth discovery regarding the serious limitations of the previous work in terms of user privacy, collected data integrity, and low computational costs, as demanded by the natural growth of IoT applications. The main idea is to limit the participation of IoT devices in the computation of the approximated truth (finding the true data), we attempt to reduce both the cost and burden placed onto the application user devices, as well as the damage caused by an active attack on data integrity. *BalancePIC* aims to satisfy these and treats user devices as if they were a database resource of IoT device sensory data. It connects to the device, demands a low-cost result and gets out, leaving the user device for other services to use.

B. Threat Models

One of the primary challenges with the edge-based IoT system is that the sensory data in IoT is susceptible to different security threats/attacks, particularly. For example, internal attacks regularly happen in the IoT device tier and the network communication tier. Different from these attacks, external attacks would be challenged by conventional security protocols, such as encryption, authorization, and auditing. Whenever IoT devices, IoT users, and edge servers exchange information that can be sensitive information, the receiver definitely has the guarantee that the data has come originally from the expected sender and is not alerted unintentionally or otherwise. Regarding the situations, there can be different kinds of active and passive data integrity threats. We assume a small set of sophisticated threat models for the edge-assisted IoT network, which are shortly explained as follows.

- *Collusion attacks.* Numerous existing works propose security protocols [10], [19]–[22]. In most protocols, every IoT device is assumed to be authentic. These protocols apply various methods for secure communications. These include authentication, authorization, hardware-based cipher. However, there remain concerns with many of them, including collusion attacks. This can be a type of attacks, which conveys the risks of the important data if an IoT device intentionally establishes communication with an unknown device. Such an unknown device might be compromised by an attacker. He can gain the essential information from the application [10].
- *Eavesdropping.* It is a type of threats/attacks, which carries security risks to the user data privacy (such as patient's sensing data privacy). It contains snuffling significant data sent by the IoT device, which yields the data privacy risks in communication.
- We also consider several attacks related to the integrity and authentication, including *resist replay attack*, *resist impersonation attacks*, *resist sensor node capture attack*, and *resist desynchronization attack*

There is no same secret data stored in the user and the server, and they do not need to update any information when one session is completed. So this attack could not occur. In terms of data privacy, we assume that an attacker may try to get user and devices' traceability and data secret.

C. The Basic Process of BalancePIC

The process in BalancePIC starts with setting the approximate ground truth with an arbitrary value. The arbitrarily adjusted ground truth is transmitted to k user IoT devices; we assume that this set of k devices are in a group named a zone. An IoT device gets the truth value and unites it along with its personal sensing information. Next, the IoT device sends its outcome to the edge server. The device encodes the information together with our suggested lightweight biometric based authentication technique. This concludes the user device's involvement in the IoT-edge based scheme. Next, the edge server gets the k outcomes from k devices and measures the mean. By this mean value, the edge server mines the unique arbitrarily adjusted ground truth through an extraction method. The approximated ground truth that the edge server is left with is a precise match to the mean of the unique sensing information of the user IoT devices.

The process of concealing a user device's sensing information with a united mean, adding the outcomes of a zone, subsequently eliminating so-called "mask" to be left with a accurate mean would be replicated with every zone being managed. The results from each zone are aggregated with the current approximated ground truth. This method prevents individual data (maybe personal data) from being sent to the edge server and solely representing the currently approximated ground truth. This prevents personal information from being acquired through alteration, eavesdropping, or the same types of attacks.

In the occurrence that the data-collecting party is not trusted, BalancePIC offers an enhanced technique for privacy. The enhanced technique for data privacy permits user devices to use an arbitrary weight when computing the mean of their individual sensing data and the approximate ground truth transmitted by the edge server. This blocks the edge server from being capable to excerpt the user device's sensing information with around 100% accuracy by applying a proposed extraction method. The scale of this weight would be offered to the user by the edge server, to best fit the context of the ground truth, or by the user device for maximum privacy security. It is presumed that the user device chooses its individual scale relying on its assessment of the data-collection party (i.e. by using zero weight variance with trusted sites, +/- v% with unknown/untrusted sites).

The BalancePIC also leaves the capability to enhance alterations. Existing light-weighted authentication is supposed to have the capability to balance the dependability of user devices is also in the hands of the user of this scheme. Some weighting methods and algorithms may be applied for this purpose [9], [10], [13], [23].

D. Design Objective

The objective of the BalancePiC design is to provide a balance among the privacy of the user, integrity of the gathered sensing data, and cost of computation of the cryptography methods applied, for example, the suggested biometric-ECC based authentication algorithm. Especially, it is aimed to guarantee the privacy of the IoT device user at the time when the user needs access to the IoT device, the dependability of the IoT device (no privacy information is leaked by this device), and integrity of the data during the data exchange between the IoT device and the edge server, and low-cost during the authentication time among the IoT device and the edge server.

III. Zone Processing for the Edge-assisted IoT

In this section, we explain the zone development process of the BalancePIC scheme. At first, we explain the zone initialization. Then we discuss the zone processing. Finally, we describe the extraction methods.

A. Zone Initialization

The overview of functions for interactions between edge servers and IoT devices is demonstrated in Figure 1. The scheme constitutes of the following missions:

1) **Edge Server:** Arbitrarily initialize an approximated ground truth.
2) **Edge Server:** Transmit the approximated ground truth to k devices (a zone).
3) **IoT device (s)**: Through formula (1), IoT device's sensory data and the average of the projected ground truth are computed.
4) **IoT device (s):** The result is delivered to the server.
5) **Edge Server:** From a zone, the mean of all k results is calculated.
6) **Edge Server:** By using formula (2), IoT device sensory data is extracted to eliminate the data transmitted in function 2.
7) **Edge Server:**
   - In the case that it appears as the first zone, the approximated ground truth is set to the outcome obtained from function 6
   - In the case that it is not the first zone, through the formula (3), the aggregation of the currently approximated ground truth is combined with the output of function 6

B. Zone Processing

In the following subsection, we elaborate on the details of functions 1-5. These functions help to calculate zone information.

To begin with, the `BalancePIC` scheme initializes the approximate ground truth to an arbitrary value [9]. Within the edge server, the initialization takes place through a data collection entity. When using the `BalancePIC` scheme, the arbitrary value may have no impact on the approximate ground truth. In spite of this, it is still recommended to use an arbitrary value that makes it contextually related, particularly when applying the enhanced technique elaborated in Section V. The purpose of using the adjusted value is to ensure that compromised or distinct sensing data is transmitted to the edge server. In a specific zone, Algorithm 1 and Algorithm 2 show the zone processing technique and users compute in a particular zone, respectively.

Based on the edge server's utilization preference, arbitrary ground truth is directly transmitted to k IoT devices. By signifying this set of k devices, a zone is processed together, so that the edge server does not handle any individual IoT device sensory data. The size of the zone is denoted by the k. The data-collection party is the one who can select the value of k. If the data-collection party uses a small amount of IoT devices, it proposes that a tiny value for k be used. The benefit of a tiny value for k is that it makes sure that the approximate ground truth is often renewed. k's value can additionally be ascertained in the context. It is completely based on the data-collection party to determine the way the set of k devices is selected for a specific zone. In order to ensure contextual relevance, a region or crowd of devices can be divided into n number of zones with size k on the basis of device specifications, location or merely its availability to the edge server. Depending on the context, the extent of anonymity required varies.

The functions 6-7 are elaborated in the following. Every k user devices compute the total amount of the approximate ground truth passed on by the edge server and their own sensory data. The summation is arrived at based on the assumption that there are only two portions, the edge servers and their own are weighted equally. The equation is as follows:

$$x_k = SensoryData * 0.5 + x * 0.5 \tag{1}$$

Once the individual calculations are over for every one of the set of k user IoT devices, these return the information to the edge server. The outputs are then aggregated by the edge server. The `BalancePIC` scheme that has been simulated for the purpose of analysis simply calculates the mean of the results, without taking into consideration the weighted dependability. The overall zone processing align with functions 1-7 are simply described in Algorithm 1.

At an individual level, although the use of zone processing complicates data, the larger image (one of k devices) still maintain unambiguous. For example, for a batch of people in New York City, it is possible to monitor the location and the change of location. However, if the objective is to find the habits of a person and the individual location, the data becomes insufficient and incomprehensible with respect to the group. On the other hand, additional information can be derived to solve the following problems: which locations people stay at in New York City during the day versus in the evening, which areas have the most vigorous nightlife, what is the origin or demographic of citizens who visit a special site at a particular time, and so on.

Algorithm 1: Zone Development

```
Input: A set of $k$ user IoT devices: device $[k]$
Result: Approximate ground truth: $x$
Initialization;
Arbitrarily adjusted the ground truth for each object;
repeat
    for every $k$ do
        Transmit ground truth to a user IoT device;
        Get aggregation of the device results;
    end
    if This zone is the first one then
        Extract the arbitrary value;
        $x$ = remainder of the IoT devices of the network;
    else
        Extract the value;
        Get the aggregation of the remainder of the
          devices and $x$;
    end
until All of the zones are processed;
return $x$;
```

Algorithm 2: User Computation

```
Input: A set of $k$ user IoT devices: device $[k]$
Result: User Calculation Result $(y)$
for every edge server do
    Get IoT device sensing data and $x$ ;
    Transmit ground truth to a user IoT device;
    $y$ = Aggregate sensing data and $x$ (e.g., formula (1));
end
return $y$;
```

C. Extraction Method

In the following part, functions 6-7 are discussed regarding the extraction. The arbitrary initialization of ground truths (in a range according to context) gives a data accuracy problem if not correctly resolved. From the accumulated sensory data, the BalancePIC scheme resolves the issue through an approach that extracts the approximated ground truths transmitted to k users in the zone. To be sure, the user calculations aggregate the sensory data of users' devices, along with the approximated ground truths supplied by edge servers, as two equal portions. From k user devices within a zone, the sensory data is accumulated. Therefore, it represents half of the device sensory information plus half approximated ground truths. The formula below derives approximated ground truths and leaves edge servers with the accumulated sensory data:

$$s^z = x^z * 0.5 + [x^z - 2(xx^z)] * 0.5 \tag{2}$$

wherein s^z denotes the sensory data accumulated in zone z, x^z denotes the accumulated results provided by the IoT devices (i.e. pre-extraction is denoted by s^z), and x denotes the presently approximated ground truth. In the one hand, this technique of extraction is applied to excerpt the randomized values which the approximated ground truth is adjusted to; and on the another hand, in order to update ground truths, in combination with the following expression:

$$x = s_z * k/c + x * (c - k)/c \tag{3}$$

where k denotes the amount of IoT devices in the zone, whereas c denotes the amount of IoT devices, which engage in the group-based sensing system that includes k user devices within the zone being presently handled. The technique of extraction applied in combination with arbitrarily adjusted values and the concept of masking sensing data from user IoT devices, enable the privacy-protections without sacrificing the integrity of data. The outputs of this approach are comprised of precise copies of all sensory data aggregated from all c devices, theoretically.

IV. Biometric-ECC based Algorithm for Data Integrity

We describe the authentication feature for data integrity features of the BalancePIC scheme in this subsection, including cryptography.

A. Cryptography Techniques

BalancePIC scheme needs to rely on any concrete cryptography technique. Nevertheless, it is recommended to implement cryptosystems with BalancePIC schemes in order to properly guard the privacy of all parties involved. Possible threats would arise if third parties were able to intercept the data being transmitted from edge servers to user IoT devices plus any data being transmitted from IoT devices to the edge servers. If an attacker who captured the data understands the nature of this BalancePIC scheme, he may use the technique of extraction to acquire the individual's IoT sensory data (although the enhanced technique presented in Section 5 protects against this possibility). It is just as critical to realize that such approximated ground truths that are being accumulated by data-collection parties might not be information that those parties wish to disclose to third parties.

Traditional cryptography techniques, including well-known cryptosystems such as Blowfish, DES, RSA involve a lot of computations. A crucial aspect with IoT-based sensing applications is that the sensing data offered by individual participants is normally not trustworthy in terms of user privacy (anonymity or compromised sensory value). To satisfy the need for low-cost computation tasks in user IoT devices, it is recommended that low computational cost cryptosystem needs to be utilized. The cryptosystem utilized in PPTD is highly complicated and necessitates device contributions to a great extent. We attempt to avoid such a cryptosystem and utilize a lightweight one. We consider a light-weight version of the cryptographic algorithms.

B. Biometric-ECC based Authentication Algorithm

We present a combined biometric-ECC based authentication algorithm with user privacy (anonymity) for before data exchange amongst the devices and edge servers in BalancePIC. We omit the basic information of the ECC here due to space limitation; however, interested reader may refer to [24] for further study. At the beginning of the data integrity verification, the ES (ES for an edge server) selects an elliptic curve E_c over a prime finite field denoted by FF_p, and selects an extra subclass G of E_c. This is produced by P by taking a large prime number order n. Hence, an ES produces the private/public key pair $\{x, X\}$ for itself (here, $x \in Z * n$ and $X = xP$. In addition, the ES selects a master secret key denoted by ω. ES issues the key parameters $\{E_c, G, n, P, X\}$. This algorithm includes 3 levels, and the explanation of the levels can be simply given in the following.

1) Enrolment Level: We divide the enrolment level into two parts, i.e., IoT device enrolment and IoT user enrolment, and these are both performed securely.

2) IoT Device Enrolment: For each IoT device (IoT_D) with its identity denoted by IoT_{Did}, ES chooses a sole identity and computes a private key $K_{sk} = h(IoT_{Did}||\omega)$. Once this is done, the ES saves the identity of the IoT device IoT_{Did} in its storage and (IoT_{Did}, K_{sk}) in the device. Then, the IoT device can be placed in a particular area to construct a network.

3) IoT User Enrolment: An IoT user IoT_U chooses an identity and a password pw_u, and obtains biometric information in an IoT device with fuzzy extractor $Gen(B_U)$, where $Gen(B_U) = (P_U, Q_U)$. We utilize a fuzzy extractor technique for Biometrics [25]. It is a fuzzy extractor tool that uses a fixed-length string to recover the biometric information. The biometric information distribution W on M for B_U is given with a minimum entropy threshold e_m. Multiple-tuple $\{M, e_m, l, \tau, \epsilon\}$ is used to symbolize the string with two algorithms: *Gen* and *Rep*. BIOU is the acquired biometric data distribution W on M with a threshold of min-entropy. The Gen algorithm produces two strings: a private string $P_U \in \{0, 1\}$ for user IoT_U, and a helper string Q_U.

Then, the IoT user produces a random number and calculates its key. Finally, the user submits the registration request to ES securely. When ES gets a request of the registration, it validates whether the user id is in the storage. If it finds, the IoT user is requested to select a new id. Else, ES computes a secret code (SC) for the user and sends it in a secure manner. Finally, upon getting the secret codes, the IoT user saves the code in the IoT device.

C. Authentication & Key Agreement Level

At any time, the IoT_U needs to get access to the sensory data of IoT devices with the identity of the devices, the authentication processes in the following can be carried out among the IoT user, ES, and the IoT device, and in the end, the IoT user and IoT device can agree in a session key for further interaction. The procedures of this level are as follows:

- Proc1: An IoT user produces a login request M_1 with inputting identity and password, and imprints its biometric information in the IoT device and fuzzy extractor is used in this case. The IoT device computes the secret string and checks secret code. If this code is not satisfied, the login request is declined by the IoT device, as one factor of authentication, id, password, or the biometric is unacceptable. Else, the user produces an arbitrary number and calculates a string. In the end, the login request is sent to the ES.
- Proc2. When ES receives the login request, it calculates user login information and validates whether or not the user id is from the storage. If it is found, the ES computes associate security verification for the IoT device. The request is dismissed by the ES if verification does not go through. Otherwise, the ES can calculate a secret code M_2 with the random number and forwards the code to the IoT device.
- Proc3. When the IoT device receives the message M_2 from the ES, it computes id verification and checks the secret code. The session is dismissed if the secret code does not match. Otherwise, the IoT device computes a code for ES (M_3) and send it to ES.
- Proc4. Once the ES receives the message M_3 , it computes a further verification code (M_4) for the IoT device and sends it to the IoT user.
- Proc5. When the IoT device receives message M_4, it computes the code and verifies it. The session is dismissed if the code is unmatched. Else, the ES can be authenticated by the user. Hence, the IoT device computes the private key and checks. The session is dismissed if the key does not match. The IoT device is then authenticated by the user, and the user shares a session key with the device. A further detail of the authentication procedure can be found in our previous work [26].

Security Feature Analysis. In the above authentication, to maintain anonymity and untraceability, a dynamic id is considered in the login request $M_1 = \{IoT_{Did}, S_1, S_3, S_4\}$ as a substitute of real id. Here, $S_1 = aP$, $S_2 = aX$, $IoT_U = IoT_{Uid} \oplus h(S_2)$ $S_3 = IoT_{Did} \oplus B2 \oplus h(S_2)$, and $S_4 = h(B2, S_2, IoT_{Did})$. Finally, the login request $M_1 = IoT_{Uid}, S_1, S_3, S_4$ is yielded to the ES. In order to attain user id identity IoT_{Did} from the login request, x is important info for an attacker to calculate S_2. Nonetheless, x can be a private key, which is only known to the ES. In contrast, ES can attain IDU from login request by computing $D2 = xD_1, IDU = IoT_U \oplus h(S2)$. As a result, the proposed algorithm obtains the feature of the anonymity of the IoT user, and also facilities the identity validation of the IoT user. In addition, IoT device's id should not be sent via a public communication or common method, and the ES can attain the IoT device id from the login request by computing $S2 = xS_1$, $IoT'_{Uid} = IoT_{Did} \oplus h(S2)$, $B2 = h(IoT'_{Uid}||\omega)$, and $IoTD'_{id} = S_3 \oplus B2$.

As a result, the protocol confirms the IoT device anonymity. Besides, every element of login request $M_1 = \{IoT_{Uid}, D_1, D_3, D_4\}$ dynamically changes with the arbitrary number. Therefore, an attacker is not able to track a particular IoT user through snooping the login information. The advantage of untraceability is confirmed.

D. Data Integrity Checking with Weighted Reliability

With the authentication algorithm above, the user IoT device's reliability can be computed based on the data integrity. The `BalancePIC` scheme contains a truth detection technique for weighing the reliability of each IoT user device and for establishing the truth through every device, in order to determine if the data had an integrity problem (data compromise happened). This is to validate whether any data is modified or not. All IoT devices have equal value (decision input) regarding ground truth aggregation. Weighted reliability, in theory, guards the data integrity. Classic weighting techniques are available [9], [11]–[13], [27]. For instance, [9] provides a weighted dependability technique of calculation in that every device's weight information is transmitted to the user devices, whereas the `BalancePIC` scheme necessitates that such technique will be computed and used only at the edge server-side. With the `BalancePIC` scheme, we calculate IoT device's status values in order to determine if the private information was modified during transmission. The fundamental principle is that the status value of a device could be assigned a high value, where data from the transmitted device is set to be approximate ground truths. The following equation is used to calculate IoT device's status values.

$$S_k = \log(\frac{\sum_{k'=1}^{K} \sum_{m=1}^{M} d(x_m^{k'}, x_m^*)}{\sum_{m=1}^{M} d(x_m^k, x_m^*)}) \tag{4}$$

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2019.2951687, IEEE Internet of Things Journal

where $x_m^{k'}$ be the observation values and x_m^* be the approximated ground true facts. There is distance function denoted by $d(.)$ used to determine the difference between sensor devices $x_m^{k'}$ and x_m^* [27].

The value of $d(.)$ is due to a specific sensing application situation. The presented scheme BalancePIC is envisioned to handle structural health event identification of SHM applications. In the case of SHM applications, where the sensor devices' signals are continuous (e.g., structural vibration response), we adopt a standardized squared distance function, which is in the following:

$$d(x_m^k, x_m^*) = \frac{\left(x_m^k - x_m^*\right)^2}{std_m} \tag{5}$$

When functions (2-3) work together, base the weights of the user devices in terms of the standard deviation as well as the normalized squared-distance function. It would be just as critical to realize that device reliability can vary between contexts [12]. For the highest possible integrity of the data, it can be recommended that the weighted dependability can be computed by the edge servers for all user IoT devices in regard to all particular contexts (wherever the edge server finds at least 2 ground truths through various sensors).

V. Proposed Enhanced Technique for Data Privacy

When we need to manage the device users privacy, it is crucial for us to consider all of the potential risks to data privacy. It can also involve the likelihood of data collection parties, which even looks untrustworthy. If an edge server notifies that it is sending a message about the truth information, but in reality, it is a phishing scam about privacy-related data and also the individual sensory information of the user IoT device can be acquired through extraction technique; in this situation, we assume that the edge server message falls short of aggregating the information amongst this k users' IoT devices in a particular zone. To properly conserve discretion, the privacy should be safeguarded against all possible threats from all data collection parties that are the outside ones and eavesdropping ones.

Algorithm 3: Enhanced Technique for User Data Privacy (calculated by the user)

```
Input: Approximate ground truth: $x$, variance $v$
Result: Result
if the value of $v$ is not expected (enough) then
    Do the replacement of $v$ with a desirable value;
else
end
Get weight = a random value between $50 - v$ & $50 + 5$;
Result = (sensing data $\cdot \frac{weight}{100}$) + (x$\cdot$100 $- weight/100$);
return $Result$;
```

The enhanced technique considers this type of situations by distorting the individual sensory information further. The technique enables the user IoT devices to employ an arbitrary weight (inside a threshold regarding particular context), especially, when we integrate the device sensory information with approximate ground truth values obtained from the edge servers. It will stop the edge server from obtaining the precise particular IoT device sensory data. Our extraction technique is simply set with high integrity when the result that is passed to the edge server from the user IoT devices is half of the device sensing information and also half of the approximate ground truth. It may affect the integrity of the data negatively. Nonetheless, as data is tackled within k IoT user devices inside a zone each with a small variation on the calculated weight, and the cumulative consequence is correct. The integrity of the data becomes inaccurate, however, the effect is negligible within certain situations considering the contexts. We provide an enhanced technique in Algorithm 3.

When we apply the enhanced technique, we can have several ways to designate appropriate variance on the weight. A weight variance might be obtained from the edge server, with the aim to meet the needs in a particular situation in context or can be stored in an IoT device. A good idea is to think of a combined algorithm. We enable the edge server to decide the condition and provide definitions of the context. However, if an edge server announces a variance that is too small, which could be a risk to the user IoT device privacy, the user IoT device may employ a value of the variance confirmed by itself within a particular range of harmless variance values.

VI. Performance Studies

The detailed performance evaluation of BalancePIC scheme is studied in this section regarding its claim of preserving the balance among data privacy, data integrity, and computational load. We have conducted the evaluation of BalancePIC through simulations.

A. Simulation Settings

We utilize a Windows 64-bit computer with Intel Core i7 version, 8 GB of RAM. We use Python to manage the programs. The BalancePIC scheme is implemented as an extension of the Wireless Network Simulation tool (OMNeT++) that is compatible with multi-radios for every IoT device node [28]. Even though OMNeT does not support Bluetooth yet, Bluetooth has been emulated through the Zigbee IEEE 802.15 WPAN scheme, with the communication range, which is set to 10-12m.

We considered 3 classes in the simulations: 1) the IoT device class, 2) the simulation class, and 3) the edge server class. The edge server class has an object for the edge servers, which contains the essential techniques that are used for imitating the operations of the edge server running the BalancePIC scheme, as it was explained in this paper. Similarly, the actions are imitated by the device class that is expected of an IoT user device. The experimental class supplies edge servers together with the required IoT devices to organize zones and compute the ground truth.

In the three classes, the experimental setting consists of 20 zones of IoT devices and 20 edge servers, and every zone has up to 100 IoT devices with +/- 0.5% of the variance. The edge server is located at a random location around the zone;

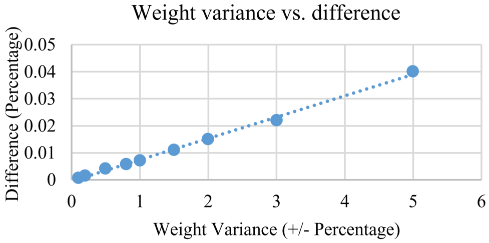


Fig. 2. The percentage of weight variance vs. the difference

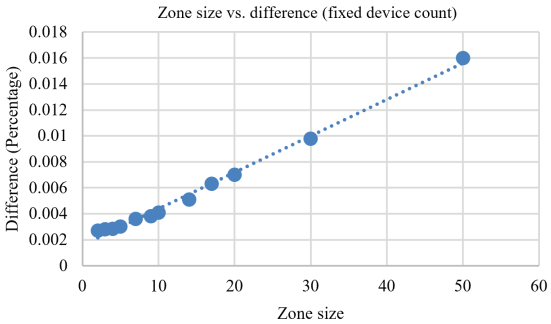


Fig. 3. The size of the zone vs. difference (percentage) with the fixed amount of device pool

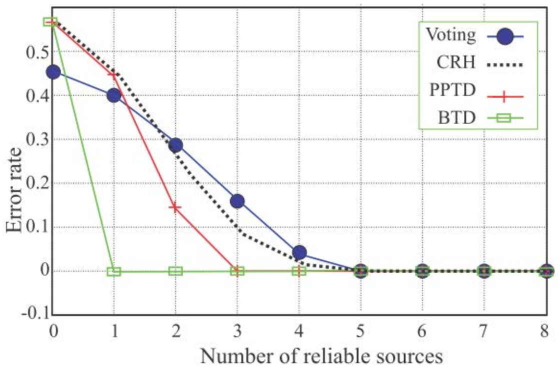


Fig. 4. Comparisons regarding error rate (in maintaining the privacy) vs. reliable data sources (that provided data without any data compromise.

however, each edge server is set to be up to 50 meters away from each other. Every simulation is repeated for 30 times and is executed for 500 virtual minutes. Furthermore, as we target the mobile devices and the sensors (regarding a crowd of mobile devices), all of the simulated IoT sensor devices have been configured to change arbitrarily 4m/s in one minute. Experimental findings are gathered based on real-world data traces of a sensing network system [13].

B. Comparisons

In the simulations, for the discovery of the status value truth as a baseline setting, the traditional techniques of truth discovery have been employed, i.e. the conflict resolution on data, which is heterogeneous (CRH for short) [11], [27], which have not done anything to break IoT device security protection during the entire process. The cryptosystem of a $(p, \lfloor \frac{p}{2} \rfloor)$-threshold Paillier has been employed in our simulations (http://cs.utdallas.edu/dspl/cgi-bin/pailliertoolbox/). This is with the Paillier Threshold Encryption Toolbox, which we carry out with the discovery of the status value truth [9], [13].

C. Simulation Results

The objective of the first set of the simulations is to compute the influence that the size of the zone has on the accuracy of data while employing the enhanced technique. The sizes of zone ranging from 3 to 20 are utilized in the experiment and the pool of the devices is kept static. The value of weight variance is measured against its effect on data accuracy (without integrity problem). As shown in Fig. 2, the result represents the difference between the approximated ground truth as calculated by the edge server vs. the average truth of the sensory data from devices.

In Fig. 3, the findings of the experiment show that the difference (reduction in accuracy) increases while keeping the device count fixed when the size of the zone rises. The extent of the influences is minor (with a size of zone = 30, the accuracy is around +/- 0.01%), but nonetheless, some context situations may need higher accuracy or fewer devices in the pools.

Our next objective of the simulation is to measure accuracy (data integrity). Computation cost on user devices, relative to PPTD, is assumed to be less, regarding simplification of authentication algorithms, zone processing, and system development. The experiments are not equivalently performed for examining the BalancePIC simulations and PPTD [13], which were analyzed previously. Findings from both cannot be directly compared. Nonetheless, deductions can be composed of the findings of simulations of BalancePIC, the PPTD experiment as well as the assessment of CRH [11], [27], which is a crowd-based IoT sensing scheme applied within the PPTD. The results of the comparison between PPTD, BalancePIC, voting, and other studies are displayed in Figure 3.

We can see that a minimum error rate is about 0.70-0.71, which is illustrated in Fig. 3. The error curve in the figure implies that the error found in maintaining the user privacy and collected data that is without any data compromise, i.e., which is with high data integrity. In the error calculation, the rounding factor L is irrespective [13] when the absolute error average (calculated by using the average of absolute distance between approximated outcomes and the ground truths) applied in PPTD scheme is united with CRH with the expression of the dotted blue line, and the error is found to be 0.70-0.71. It displays that as far as there is a single data reliable source of data (see Fig. 4), BalancePIC has a rate of error close to 0 (with the illustration of the black line). It demonstrates that the PPTD generates an error of about 0.71 without any of the additives for maintaining privacy. The simulations confirm that BalancePIC contains an error of 0.05 at the time of its "worst case", and a high variance of weight +/- 5% scenario while employing the enhanced technique. Nonetheless, the value of weight can result in a much lower error of about 0.001 using a lower variance.

As mentioned previously, it is not possible to compare directly the findings of PPTD experiments with `BalancePIC` simulations. The importance of the errors generated by using PPTD is to provide evidence of the enhancement incorrectness of data provided by `BalancePIC`. It is noteworthy that `BalancePIC` also performs actions to certify the integrity of data by safeguarding the users having the intention of altering the approximated ground truth.

VII. Conclusions

We have presented `BalancePIC`, a novel scheme to provide a balance between the data security tasks and computational efforts for performing security tasks. `BalancePIC` advances the previous schemes by fulfilling three requirements of IoT network: preserving the privacy of the device users whenever a user attempts to login in or gets involved in the data collection; the data integrity, such as integrity of the data at the data collection party; and the low-cost of computation in the edge-assisted IoT networks. To achieve this, in `BalancePIC`, we have presented a system design. This includes an extraction method, a biometric-ECC based authentication algorithm and the reliability weight based on the enhanced truth discovery. Simulations running the `BalancePIC` scheme show that accurate data within a few thousands of the percentage can be achieved whilst preserving the privacy of the device user. We believed that the proposed scheme can be applied to many existing works with a modification for better performance and molded to serve a particular context.

References

[1] R. Hsu, J. Lee, T. Q. S. Quek, and J. Chen, "Reconfigurable security: Edge-computing-based framework for iot," *IEEE Network*, vol. 32, no. 5, pp. 92–99, 2018.

[2] T. Wang, G. Zhang, A. Liu, M. Z. A. Bhuiyan, and Q. Jin, "A secure iot service architecture with an efficient balance dynamics based on cloud and edge computing," *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 4831–4843, 2019.

[3] Y. Liu, C. Yang, L. Jiang, S. Xie, and Y. Zhang, "Intelligent edge computing for iot-based energy management in smart cities," *IEEE Network*, vol. 33, no. 2, pp. 111–117, 2019.

[4] J. Zhou, Z. Cao, X. Dong, , and A. V. Vasilakos, "Security and privacy for cloud-based iot: Challenges," *IEEE Commun. Mag*, vol. 55, no. 1, pp. 26–33, 2017.

[5] Kim and Y.-S. Jeong, "Secure authentication-management human-centric scheme for trusting personal resource information on mobile cloud computing with blockchain," *Human Centric Comput. Inf. Sci*, vol. 8, no. 11, pp. 26–33, 2018.

[6] F. Meneghello, M. Calore, D. Zucchetto, M. Polese, and A. Zanella, "Iot: Internet of threats? a survey of practical security vulnerabilities in real iot devices," *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 8182–8201, 2019.

[7] A. Ahmed, K. Abu Bakar, M. I. Channa, K. Haseeb, and A. W. Khan, "A trust aware routing protocol for energy constrained wireless sensor network," *Telecommunication Systems*, vol. 61, no. 1, pp. 123–140.

[8] W. Jiang, G. Wang, M. Z. A. Bhuiyan, and J. Wu, "Understanding graph-based trust evaluation in online social networks: Methodologies and challenges," *ACM Comput. Surv.*, vol. 49, no. 1, pp. 10:1–10:35, May 2016.

[9] C. Miao, W. Jiang, L. Su, Y. Li, S. Guo, Z. Qin, H. Xiao, J. Gao, and K. Ren, "Privacy-preserving truth discovery in crowd sensing systems," *ACM Trans. Sen. Netw.*, vol. 15, no. 1, pp. 9:1–9:32, 2019.

[10] M. Z. A. Bhuiyan and J. Wu, "Trustworthy and protected data collection for event detection using networked sensing systems," in *2016 IEEE 37th Sarnoff Symposium*, 2016, pp. 148–153.

[11] Q. Li, Y. Li, J. Gao, B. Zhao, W. Fan, and J. Han, "Resolving conflicts in heterogeneous data by truth discovery and source reliability estimation," in *Proceedings of the 2014 ACM SIGMOD International Conference on Management of Data*, ser. SIGMOD '14, 2014, pp. 1187–1198.

[12] F. Ma, Y. Li, Q. Li, M. Qiu, J. Gao, S. Zhi, L. Su, B. Zhao, H. Ji, and J. Han, "Faitcrowd: Fine grained truth discovery for crowdsourced data aggregation," in *Proceedings of the 21th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, ser. KDD '15, 2015, pp. 745–754.

[13] C. Miao, W. Jiang, L. Su, Y. Li, S. Guo, Z. Qin, H. Xiao, J. Gao, and K. Ren, "Cloud-enabled privacy-preserving truth discovery in crowd sensing systems," in *Proceedings of SenSys '15*, 2015, pp. 183–196.

[14] J. Ni, X. Lin, and X. S. Shen, "Toward edge-assisted internet of things: From security and efficiency perspectives," *IEEE Network*, vol. 33, no. 2, pp. 50–57, 2019.

[15] W. Yu, F. Liang, X. He, W. G. Hatcher, C. Lu, J. Lin, and X. Yang, "A survey on the edge computing for the internet of things," *IEEE Access*, pp. 6900–6919, 2018.

[16] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao, "A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications," *IEEE Internet of Things Journal*, vol. 4, no. 5, pp. 1125–1142, 2017.

[17] Z. Qin, Y. Yang, T. Yu, I. Khalil, X. Xiao, and K. Ren, "Heavy hitter estimation over set-valued data with local differential privacy," in *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, ser. CCS '16, 2016, pp. 192–203.

[18] X. Yang, T. Wang, X. Ren, and W. Yu, "Survey on improving data utility in differentially private sequential data publishing," *IEEE Transactions on Big Data*, pp. 1–10, 2018.

[19] E. Luo, Q. Liu, and G. Wang, "Hierarchical multi-authority and attribute-based encryption friend discovery scheme in mobile social networks," *IEEE Communications Letters*, vol. 20, no. 9, pp. 1772–1775, 2016.

[20] T. Wang, J. Zhou, A. Liu, M. Z. A. Bhuiyan, G. Wang, and W. Jia, "Fog-based computing and storage offloading for data synchronization in iot," *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 4272–4282, 2019.

[21] J. Shen, Z. Gui, S. Ji, J. Shen, H. Tan, and Y. Tang, "Cloud-aided lightweight certificateless authentication protocol with anonymity for wireless body area networks," *Journal of Network and Computer Applications*, vol. 0, pp. 1–15, DOI: 10.1016/j.jnca.2018.01.003, 2018.

[22] T. Wang, Y. Li, G. Wang, J. Cao, M. Z. A. Bhuiyan, and W. Jia, "Sustainable and efficient data collection from wsns to cloud," *IEEE Transactions on Sustainable Computing*, pp. 1–12, 2017.

[23] S. Wang, D. Wang, L. Su, L. Kaplan, and T. F. Abdelzaher, "Towards cyber-physical systems in social spaces: The data reliability challenge," in *2014 IEEE Real-Time Systems Symposium*, 2014, pp. 74–85.

[24] D. Hankerson, A. J. Menezes, and S. Vanstone, *Guide to Elliptic Curve Cryptography*. Berlin, Heidelberg: Springer-Verlag, 2003.

[25] Y. Dodis, L. Reyzin, and A. Smith, "Fuzzy extractors: How to generate strong keys from biometrics and other noisy data," in *Advances in Cryptology - EUROCRYPT 2004*, C. Cachin and J. L. Camenisch, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2004, pp. 523–540.

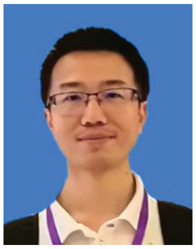
[26] X. Li, J. Niu, M. Z. A. Bhuiyan, F. Wu, M. Karuppiah, and S. Kumari, "A robust ecc-based provable secure authentication protocol with privacy preserving for industrial internet of things," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 8, pp. 3599–3609, 2018.

[27] Y. Li, Q. Li, J. Gao, L. Su, B. Zhao, W. Fan, and J. Han, "Conflicts to harmony: A framework for resolving conflicts in heterogeneous data by truth discovery," *IEEE Transactions on Knowledge and Data Engineering*, vol. 28, no. 8, pp. 1986–1999, 2016.

[28] O. Helgason and S. T. Kouyoumdjieva, "Enabling multiple controllable radios in omnet++ nodes," in *Proceedings of the 4th International ICST Conference on Simulation Tools and Techniques*, ser. SIMUTools '11, 2011, pp. 398–401.

Acknowledgment

This work is supported by the Fordham University Faculty Research Grant, in part by the National Key Research and Development Program of China (No. 2017YFB1001800), in part by the National Science Foundation of China under Grant No. 61872219, and in part by the Natural Science Foundation of Shandong Province (ZR2019MF001)..



Tian Wang received his BSc and MSc degrees in Computer Science from the Central South University in 2004 and 2007, respectively. He received his PhD degree in City University of Hong Kong in 2011. Currently, he is a professor at the College of Computer Science and Technology, Huaqiao University, China and a guest professor at the Department of Computer Science and Engineering, Shaoxing University, Shaoxing, China. His research interests include internet of things, edge computing and mobile computing.

Md Zakirul Alam Bhuiyan , PhD (M'09-SM'17), is currently an Assistant Professor of the Department of Computer and Information Sciences at the Fordham University, NY, USA, the Founding Director of Fordham Dependable and Secure System Lab (DependSys). Earlier, he worked as an Assistant Professor at the Temple University. His research focuses on dependability, cybersecurity, big data, and IoT/CPS Applications. His work (including 40+ JCR Q1 papers) in these areas published in top-tier venues. Several research work of Dr. Bhuiyan have got recognition of ESI Highly Cited Papers. He has received numerous awards, including the IEEE TCSC Early Career Researcher, the IEEE Outstanding Leadership Award, and IEEE Service Award. He is a senior member of IEEE and a member of ACM.

Guojun Wang , received BSc in Geophysics, MSc in Computer Science, and PhD in Computer Science from Central South University, China. He is currently the Pearl River Scholarship Distinguished Professor at Guangzhou University, China. He was a Professor at Central South University, China; a visiting scholar at Temple University and Florida Atlantic University, USA; a visiting researcher at the University of Aizu, Japan, and a research fellow at Hong Kong Polytechnic University. His research interests include cloud computing, trusted computing, and information security. He is a distinguished member of the CCF, and a member of IEEE, ACM, and IEICE..

Lianyong Qi , received his PhD degree from the Department of Computer Science and Technology from Nanjing University, China, in 2011. In 2010, he visited the Department of Information and Communication Technology, Swinburne University of Technology. Now, he is a professor in the School of Information Science and Engineering, Qufu Normal University, China. He has chaired two NSFC projects and has published over 40 research papers in international journals (e.g., IEEE TCC, IEEE TBD, IEEE TCSS, IEEE JSAC) and international conferences (e.g., ICWS, ICSOC, HPCC, TRUSTCOM). His research interests include big data and services computing.

Jie Wu is the Director of the Center for Networked Computing and Laura H. Carnell professor at Temple University. He also serves as the Director of International Affairs at College of Science and Technology. His research interests include mobile computing and wireless networks, routing protocols, cloud computing, and network trust and security. Dr. Wu publishes in scholarly journals, conference proceedings, and books. He serves on several editorial boards. Dr. Wu was general co-chair for MASS 2006, IPDPS 2008, ICDCS 2013, MobiHoc 2014, ICPP 2016, and CNS 2016, as well as program chair for INFOCOM 2011 and CNCC 2013. Dr. Wu is a Fellow of the IEEE.

Thaier Hayajneh Ph.D. is the founder and director of Fordham Center for Cybersecurity, University Professor, and director of the cybersecurity programs at Fordham University, New York. Prior to joining Fordham, he was a full-time faculty of computer science at New York Institute of Technology and founding director of NYIT Center of Excellence in Cyber Security (2014-2016). He received his Ph.D. and M.S. degrees in Information Sciences with specialization in cybersecurity and Networking from the University of Pittsburgh, PA. He also received his MS and BS in Electrical and Computer Engineering from Jordan University of Science and Technology, Irbid, Jordan, in 1999 and 1997, respectively.