International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2020 IJSRCSEIT | Volume 6 | Issue 3 | ISSN : 2456-3307
DOI : https://doi.org/10.32628/CSEIT2063146

A study On : Confidentiality Approach to Prevent Features Disclosure in IoT Situations

Frimpong Atta Junior Osei [1*], Sidique Gawusu [2], Xuezhi Wen [3], Yu Zheng [4], Daniel Appiah Kumah[1]

[1,2]Nanjing University of Information Science and Technology, Jiangsu, China

[3]School of Computer and Software, Nanjing University of Information Science and Technology, Jiangsu, China

[4]School of Computer and Software, Jiangsu Engineering Center of Network Monitoring, Nanjing University of Information Science & Technology, Jiangsu, China

*Corresponding email: 20165308007@nuist.edu.cn

ABSTRACT

This paper proposes an approach which safeguards confidentiality to avoid disclosures of features within a multiple IoT situation, that is, a setup of objects in networks that communicate with each other. Two ideas derived from the theory of databases, namely k-anonymity and t-certitude, form our basis. They are used to cluster the objects to provide a unitary view of them and their characteristics. In fact, the use of anonymity and t-closeness robustly ensures privacy for derived groups. Furthermore, description of the object grouping scheme that preserves privacy, which represents the core of our approach was studied. Eventually, we illustrated the corresponding security model and analyzed the associated properties. The study also provided important advantages for the protection of user privacy in all those situations where knowledge of object features may help an attacker to obtain information about user habits and behavior. This study prevents not only the disclosure of information but also the divulgation of features. This is a major strength of our approach as malicious analyzes of the characteristics of objects can interfere with the privacy of people.

Keywords *: Confidentiality, Preserves Privacy, Networks, Internet Of Things, User Privacy, Derived Group.*

I. INTRODUCTION

We have been assisting over the last few years with the tremendous increase in the number of sensors and apps, which are becoming increasingly ubiquitous and being used in most daily contexts. At the same time, objects are developing appallingly intelligent and social skills. All these aspects revolutionize the Internet of Things (IoT) [1, 2]. As evidence of this, more and more researchers are beginning to study the behavior of things, discuss their profiles and social interaction and manage objects almost as if they were human [3]. As a result of these investigations, several architectures were proposed in the literature implementing these ideas, and are currently being proposed. Multiple IoT Environment (MIE) [4, 5], Multiple Internet of Things (MIoT) [6, 7] and Social Internet of Things (SIoT) [8, 9] are only three of the new architectures with these features. Such an evolution of the IoT situations brings researchers in front of several problems that, if properly addressed, can become significant opportunities. A major example of this is the researchers' enormous interest in IoT security and privacy. In fact, many approaches to defining security solutions in the context of smart objects have been proposed in recent years, such as intrusion detection solutions [10], access control [11, 12] and privacy [13, 14]. Tahsien et al [15] conducted a study on Machine Learning-based Internet of Things (IoT)

security solutions as a powerful technology was used to detect attacks and identify abnormal smart device and network behaviours. Mohanty et al [16] discussed an efficient, integrated Lightweight Blockchain (ELIB) model for security and privacy in IoT. As an important illustration they presented a model to be deployed in a smart home environment to verify its applicability in different IoT situations. Based on their study in a smart home, resource-constrained resources take advantage of a centralized manager that generates shared keys to transmit data, process every incoming and outgoing request. The presented ELIB model creates an overlay network where highly equipped resources can combine into a public BC that verifies the security and privacy of dedicated resources. Mohanta et al [17] conducted an IoT security survey: challenges and solutions using machine learning, artificial intelligence and blockchain technology to study the three primary technologies Machine Learning(ML), Artificial Intelligence (AI), and Blockchain to address IoT security. In the end, an analysis of this survey mentions security issues with research challenges solved by the ML, AI, and Blockchain. Hassan et al [18] discussed on the privacy issues caused by the integration of blockchain into IoT applications by focusing on our daily use applications. In addition, they studied the implementation of five privacy conservation strategies in blockchain-based IoT systems named as anonymization, encryption, private contract, mixing, and privacy differentials. Finally, the challenges and future directions for research into preserving the privacy of blockchain-based IoT systems were also looked at. Ouaddah et al [19] investigated the limitations of the centralized model to secure IoT and suggests the blockchain approach as an example of a successful distributed system to provide IoT devices with security and privacy. In their report, they implemented Fair Access and PPDAC to ensure fine-grained access control functions for IoT devices with a clear anonymity guarantee for IoT end-users, as a lightweight and privacy-conserving access control system based on the evolving blockchain technology, primarily the permissionless and public form. As with all areas of networked computing, due to the interconnected nature of the Internet, the IoT presents particular challenges to security and privacy. It means that at any given moment Internet resources can be attacked from anywhere. There are numerous threats that can affect IoT entities, such as attacks targeting communication channels, physical threats, service denial, identity making, etc. [20]. This has prompted several researchers to develop IoT-specific countermeasures to address security and privacy issues [21, 22]. Abomhara et al [23] presented an overview of the principles of security as well as the challenges of technology and safety; then they propose countermeasures to secure the IoT. On the one hand, this technology's omnipresent nature gives its users more opportunities to enhance their interactions and have access to advanced features that foster the creation and consolidation of social relations. In contrast, however, it poses new, severe technical challenges [24]. Many researchers have adopted Blockchain-based strategies to overcome IoT resources allocation and propose security and privacy solutions [25, 26].

In this study, we aim to resolve this issue by proposing a privacy-conserving approach to prevent disclosure of characteristics in an IoT situation. Much more, as previously stated, it seeks to prevent the disclosure of a user's confidential information that can take place simply by examining the features of the devices that she is utilizing. As well taking into consideration that utility and privacy are really a major trade-off for privacy-preserving methods, our approach strives to protect all existing user-object-interaction information. In fact, this information is extremely important in assisting other applications on an IoT situation and possible analyzation. Our approach, on the other hand, consequently prevent by partially concealing the features of objects that

still allow others to exploit fully to facilitate communications with objects.

II. METHODS AND APPROACH

Our approach uses some traditional database concepts, for example k-anonymity [27-29] and t-closeness [30], to further detail. The basic concept of both of these paradigms is to group together data in order to have at least k records contain the same piece of information. This creates a kind of blurred data cloud, in which the protected piece of information cannot be mapped to a specified record in a k-sharing environment. It is of course possible to reduce the number of candidate records associated with a specific feature when dealing with data distribution by exploiting the probability that a record contains the information. This alternative is overcome by imposing criteria based on distribution of likelihoods when selecting the allowable values for the k anonymization of a sensitive piece of information. The idea of building small conglomerates, hereafter known as community of objects, in an existing network in order to build a single view of the objects present in each of them is k-anonymity and t-closeness. The sense of self of intelligent objects is preserved from a point of view of connectivity and their features are mixed in each group. From the outside, a smart object presents itself by advertising the features available in the group it belongs to. Companies are formed through the resolution of a balance between privacy and communication performance. K-anonymity and t-closeness are combined to enhance the privacy of each party by correctly selection of features, typology and number of items in compliance with the desired degree of security as tuning parameters. The approach we take with regard to established communication channel security and the exchange of data between objects [31, 32]. In addition, while many researchers have developed mechanisms to secure object interaction from security and privacy perspectives, our approach focuses on the impact of direct viewing of the objects they employ on the privacy of users. As stated above, such strategies can be improved by using object scopes and features; therefore, enabling feature advertising is an important point and a key aspect for improving object interactions in the IoT. This consideration, combined with the observation that the knowledge of object features is an important vehicle to privacy leakage, leads to the need of a stable solution that enables these interactions in a privacy-preserving way. Our proposal refers to such a situations and presents a solution in this setting. In its design we also take into account the most recent developments on IoT research. It's been demonstrated that it is more realistic than just a unique network of objects to model an IoT situation like a set of connected networks. This is because of the number of objects involved, their intelligence and social interactions, as well as the possibility of hiding part or most of the exchange of data within every part of the object network [5]. Our proposal focuses mainly on the use of multi-network representation of our situation. (i) For each identified group, in fact, corresponds in a system 's network, (ii) each object may be modeled by means of a node, and (iii), relations between objects belonging to the same group can be modeled on arcs within the corresponding system(s), (they are called "inner arcs"). This enables us to benefit in us analyzes from the wide range of results found in previous literature for multi-network systems.

III. PROPOSED MODEL

We explain in this section our model for the actors who work on our method and interact with them. In Table 1, we list the key abbreviations used in this paper to increase the reading capacity of this section and of the next. The main concepts of our model are:
(i) Node. It represents an intelligent object and has a profile that allows it to interact anonymously with other nodes. An identifier which doesn't report any

information on the specific features of the object (to ensure anonymity) and the set of features provided by the group in which it belongs consists of a node profile. Any information necessary for communicating with other nodes (such as the Mac address, IP address, etc.), also has been associated with a node. In this study, the symbols n_i are used to indicate a node and ϕ_i is used to indicate a set of features. Furthermore, we use these two terms on an interchangeable basis since there is a bi-univocal correspondence between a clever object and the corresponding node.

Table 1. The main abbreviations used.

IoT	Internet of Things	$SIoT$	Social Internet of Things
MIE	Multiple IoT Environment	$MIoT$	Multiple Internets of Things
n_i	the ith node	P_i	the profile of n_i
$\emptyset_i$	the set of the features exposed byn_i	G_k	the kth group
min_k	the minimum number of nodes of G_k.	max_x	the maximum number of nodes of G_k.
φ	a feature	NS_k	the set of the nodes of G_k.
NS_k^P	the set of the nodes permanently associated with G_k.	NS_k^T	the set of the nodes temporarily assigned to G_k.
$\emptyset_k$	the set of the features exposed by G_k.	WZ	the Welcome Zone
$\mathcal{M}$	a MIoT	N	the set of the nodes of$\mathcal{M}$
A	the set of the arcs of $\mathcal{M}$	A_I	the set of the i-arcs of $\mathcal{M}$
A_C	the set of the c-arcs of $\mathcal{M}$	T_k	the kth IoT of M corresponding to the group G_k.
$\mathcal{T}$	the IoT of M corresponding to the Welcome Zone	$\mathcal{G}_k$	a graph representing I_K
N_k	the set of the nodes of G_k.	A_k	the set of the arcs of G_k.
σ_C	the score of the node n_C	π_C	the priority of the node n_C
τ_C	the time elapsed since n_C participated to its current group	i_C	the importance of n_C

(ii) Group. A set of intelligent objects that comply with the t-closeness principles are characterized by heterogeneous features. A group has a number of nodes minimum and maximum. We use the symbols as follows:

– G_k, to denote the kth group;

– min_k and max_k, to represent the minimum and the maximum number of nodes of G_k;

– NS_kNSk, to indicate the set of the nodes of G_k;

– ϕ_k, to denote the set of the features exposed by G_k.

- In turn, NS_k consists of two subsets, namely:

- NS_k^P i.e., the set of the nodes permanently associated with G_k;

$-NS_k^T$, i.e., the set of the nodes temporarily assigned to G_k.

(iii) Welcome area (WZ, below). Welcome area. This is a stage in which nodes are placed when they need to join our system during their start-up phase. It can be regarded as a particular group of nodes where there is no feature. In addition, it provides a connection in our program to all the other classes.

(iv) MIoT (Multifunctional-IoT). This reflects the world in which intelligent objects work and communicate. A MIoT is a network of intelligent objects which, from the physical point of view, can communicate either directly (when a direct connection exists between them), or indirectly, (if other intermediate nodes are required). There are two basic forms of contact in the network:

- Point-to-point: consists of a private message that cannot be reached from any other node between two nodes of the MIoT.
- Broadcast: consists of a public message that can be seen by all the corresponding nodes in the group or in the Welcome zone.

Logically speaking, MIoTs can be represented as an Internet of Things set (hereafter, IoTs) as a consequence of the concept proposed in [5]:

$$\mathcal{M} = (I_1, I_2 \dots\dots\dots\dots, I_m, \bar{I}) = (I_1, I_2 \dots\dots\dots\dots, I_m, I_{m+1}$$

Here, each IoT I_k, $1 \leq k \leq m$, corresponds to a group, whereas $\bar{I} = I_{m+1}$ corresponds to the welcome Zone. A graph $G_k = \langle N_k, A_k \rangle$, $1 \leq k \leq m + 1$, can be associated with each IoT of $\mathcal{M}$. In this case:

- N_k is the set of the nodes of G_k; there exists a node n_i for each smart object associated with G_k.
- A_k is the set of the arcs of G_k. Our model assumes that there always exists an arc between two nodes of the same group or between two nodes of the Welcome Zone.

Finally:

$$M = \langle N, A \rangle$$

Here:

- $N = U_{k=1}^{m+1} N_k$;
- $A = A_1 \, U \, A_c, \; where \; A_1 = U_{k=1}^{m+1} A_k \; and \; A_c = \left\{ \{(n_j, n_q) | n_j \epsilon \, N_k, n_q \epsilon \, N_l, \; k \neq 1\} \right\}$.

A_I is the set of the inner arcs (hereafter, i-arcs) of $\mathcal{M}$; they connect nodes that belongs to the same group. A_C is the set of cross arcs (hereafter, *c-arcs*) of $\mathcal{M}$; they connect nodes that belongs to different groups and play a major role in our privacy protection protocol, as is clear from the following. A node connected to at least one c-arc is called *c-node*; otherwise, it is called i- node. Actually, in our model, we can distinguish two main categories of c-nodes. The former refers to nodes that temporarily belong to a group G_k; indeed, just because they are not permanently assigned to G_k, they still continue to belong also to WZ[1]. Instead, the latter contains nodes with c-arcs to nodes that belong to certain classes. Finally, when the I are built automatically by our system, c-arcs are constructed by the knots once a group is formed. In particular, c-arcs can be created either for connecting the WZ node to the other nodes of this group temporarily, or for connecting nodes from different groups, to each group. With regard to this latter aspect, it is worth noting that in our solution nodes are still able to interact in classic IoT literature strategies such as proximity to nodes or homogeneity to nodes [45].

IV. The proposed privacy-preserving object grouping scheme

4.1. General overview of the scheme proposed

Our approach, as outlined in the introduction, aims to safeguard the privacy of smart object users with MIoT when feature guides object interactions. Our approach is based on some concepts, i.e. k-anonymity [27-29] and t-closeness [30] from databases as discussed in the Introduction. We are implementing these notions in our situation by creating groups of objects so that every object can participate in the MIoT by using its group features as a business card. If an object is interacting with one another, it can intuitively achieve the available content within a group of objects. Therefore, if all communication within the group is anonymous, observers are unable to know what nodes in the group can contain content related to a particular feature. Our scheme includes two key categories of operations, namely operations at node level and at group level. The first involves two fundamental acts within the MIoT, namely joining and leaving, that one clever entity (i.e. a node in our model) can carry out. The above applies to all operations conducted in a group to preserve the animation of the MIoT. The following measures are provided in more detail: Group formation, group restructuring and group resize. As shown in the figure. 1, by means of a join operation every node will access our network. Our system is equipped with an area where nodes are welcomed, i.e. Welcome Zone. Send hello messages to nodes that join WZ to inform other nodes of their presence in WZ.

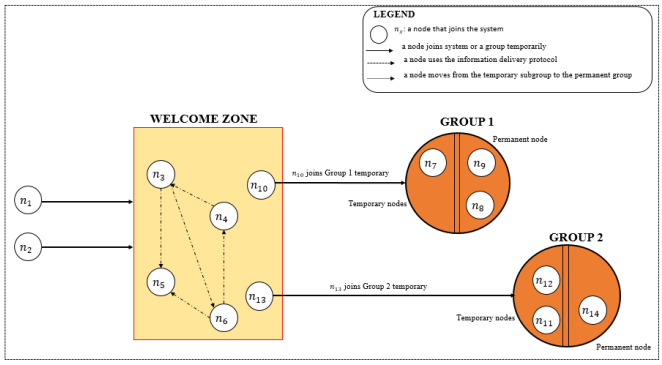

Fig. 1. A summary of our approach.

Over time, new nodes may enter and join existing groups or engage in the creation of new groups (even temporarily). In addition, its current group and system can be left by a node. Objects again communicate protocol messages (i.e. leave the current group), in which cases group-level operations (such as group restoration and group resize) are initiated. These last operations have been conceived to manage the variation of the number of nodes inside groups over time. In the final analysis our approach offers a query mechanism for ensuring the privacy that information is collected in such a complex system provided that that messages with different features as a topic often lead to a privacy failure. It is essentially made up of two types of document, intra-group queries and extra-group queries and a contact protocol. Info from your group or from the MIoT network is accessible for nodes. The first function is to use intragroup communications, but the second adopts special extra-group messages. It should be noted that the group composition is centered only on the order of arrival of nodes in WZ. This implies, of course, that a group might contain heterogeneous nodes. However, because of the requirements of our privacy model the nodes in a group have a consistent number. In reality, our goal is different and concerns to build relatively small, blurred clouds of nodes in order to protect features which each of them exposes. In other words, the node homogeneity requirements are not crucial in our context. The MIoT, which provides basic networking functionalities (private, point-to - point communication, and diffusion messages), is theoretically responsible for the connections between nodes. Whenever a node joins, the connectivity data of a system (MAC address, IP address, etc.) are actually registered with a MIoT. An important point is that we need to ensure that nodes can interact directly within the group, because we want to map every node to the features that are exposed across the entire group. For this reason, within each group we impose the complete connecting of the nodes. Again the MIoT handles all the communication (and thus the use of the associated connection links). Finally, group training is the strategy to implement our data protection model. We also maintain, however, the original nature of IoT by ensuring that nodes can still be contacted and interact with existing links and strategies [8, 9]. In fact, our solution includes non-group communication between nodes, as explained below. Thus, if two nodes are close and a link can be made between them according to [33], then there may be two situations, i.e. (a) they belong to the same group and therefore no further operation is required; ii) they belong to different groups, so that a C-arc is created between them to allow (extra-group) communication. They are not to be established. We shall provide a complete description of our protocol in the following paragraphs by examining in detail the node level operations and delivery protocol.

4.2. Node-level operations

We impose a minimum number of nodes in the WZ before group training can begin to meet the requirements of privacy. Operations at the node level describe the tasks a single node can accomplish in MIoT. There are basically two operations, namely join and leave. We describe them in the next subsections.

4.2.1. Join of a node

When a n_i node involves the joining WZ or MIoT Group G_k, an entry operation takes place. The n_i sends a "hello message" in the former case to the other nodes of the WZ. These respond by specifying the number ϵ of the nodes that have previously joined WZ but have not yet reported their features. In fact, it is necessary that at least k new nodes convey their features simultaneously in order to preserve the k anonymity property. To achieve this goal, when a node enters WZ, ϵ is increased. If $\epsilon \geq k$, the functions of all

nodes in WZ are communicated and ϵ is set to zero (0). If n i joins a G_k group, two other subsections, i.e. permanent and temporary connections, must be distinguished. The first constitutes the principal form of membership of a group node; it is a stable situation in which the node can remain in the group, and can participate, without time limitation, in all tasks involving the group members and thus, until the group no longer exists or until the node leaves it spontaneously. Last but not least, it was designed to face anomalous situations where the conditions for forming new groups are not met for a long time (in general, when an enough number of new nodes are missing). In this case objects waiting in WZ are temporarily attached to existing groups, provided the features exposed by them allow. In particular, if the crossroad between the set of its function and that of the group is not empty, a node can temporarily join a group. It is worth pointing out that in this situation, the node will dissimulate the additional characteristics that it has over those displayed by the party it belongs to. In case of a permanent join, n_i communicates the change of its state to the nodes of WZ so that they can remove it from their lists of contacts. If a temporary join occurs, n_i is G_k and WZ simultaneously. It still interacts with WZ nodes in this last case to create new groups or participate in the remediation or re-dimensioning of tasks in which existing groups already participate. As a result, n_i functions as a c-node in this situation.

4.2.2. Leave of a node

When a node, n_i requires to leave WZ or a MIoT group G_k, a leave operation is performed. In the former case, it's enough that, n_i informs WZ's other nodes to remove the arcs that link them to, n_i. In the latter case, n_i will notify both G_k and WZ nodes which will eliminate all the arcs that connect them to it. The cycle ends after this function if, n_i is an i-node. On the other hand, i.e. , n_i is a c-node, it is necessary to handle the arcs between it and the nodes of the other groups of the MIoT. For each arc between , n_i and a node , n_I of another group G_q, two cases might happen: (a) the arc is recent and has been rarely used; in this case, it can be removed; (b) the arc is old and has been frequently used; in this case, it should be ‘‘inherited’’ by another node of G_k. To distinguish these two cases, it is possible to introduce a parameter ρ measuring the relevance of an arc ρ is defined as;

On the other hand, i.e., n_i is a c-node, the arcs between it and the nodes of the other MIoT groups must be handled. For each arc between, n_i and a node, n_I of another G_q group , two cases could occur: (a) the arc is recent and has rarely been used; in this case, it can be removed; (b) the arc is old and has been frequently used; in this case, it should be "inherited" by another G_k node. In order to differentiate between these two instances, it is possible to add a parameter ρ which measures the significance of an arc is defined as

$p = \frac{v}{\lambda}$, where ν is the number of times the arc was used for communication, whereas λ is the arc used for lifetime. If ρ is less than a threshold $th\ \rho$, the arc can be removed; otherwise, another node of G_k will "inherit" it. In this latter case the node that inherits the arc must be chosen. To this end, the of G_k candidate nodes set $CSetk$ is determined first. This package contains all of the separate of G_k c-nodes than n_i. Then, each CSetk node nc has to calculate a score σ_c, which takes into account both its πc priority and the compatibility between its and G_q features. Formal spoken word:

$$\sigma_C = \omega \,.\pi_C + (1-\omega).J(\emptyset_C, \emptyset_q)$$

Here, ω is a weight that belongs to the actual interval [0, 1] used to weigh against compatibility the importance of priority. The π_c priority is a real number that takes into account the time that has elapsed since n_c took part in G_k and the importance l_c of n_c in the MIoT:

$$\pi_C = \tau_C \,.l_C$$

The value of l_c belongs to the real interval [0 , 1] and is set in a friendly fashion by the human expert. For example, a system that measures a critical parameter (e.g. pulse or blood glucose) is typically more important than one that measures the brightness. The above strategy seeks to assign the arcs with a higher priority to the nodes; it helps to reduce the possibility of potential new reassignments of the same arc. As matter of facts, since a node's priority is determined as a combination of both the time elapsed from the time it joined

G_k and its importance (in terms of the features offered), a high-priority node is less likely to leave G_k J is the Jaccard coefficient between the characteristics of n_C and those of group G_q, which belongs to n_1. We remember that the coefficient Jaccard tests the similarity between two sets and returns a value in the real interval [0, 1]; the higher the similarity [34]. The Leaving node initializes the competition to inherit the arc. After all G_k candidate nodes have determined their score, they communicate it anonymously using the anonymous broadcast communication from the information delivery protocol. Therefore the node with the highest score is chosen to inherit the arc left by n_i. This arc will be inherited in anonymous manner. When this happens, the reset value for this arc will be the value of π, and consequently of ρ. As pointed out earlier, n_i leaves G_k. And the MIoT, WZ nodes must also be informed. In fact, all nodes belonging to WZ, or temporarily assigned to other groups, must know all the changes in each group because those changes can activate resize or remediation operations that might involve them.

4.3. Information delivery protocol

In fact, anonymous broadcasting can be seen as a hybrid approach consisting of a preliminary set of point-to - point exchanges of the message to be delivered, handled in a manner analogous to what happens in mix-net networks [35], followed by the delivery of the same message through broadcast [36]. As follows, a naive (but at the same time effective and effective) way of proceeding is. Using point-to - point mode, when a node n_i receives a message m, it forward m to another node n_i with a given probability ρ. Instead, it forward m in broadcast mode to all the nodes of its group (or to WZ) with a probability equal to $1 - p$. The value of p must be chosen to ensure a trade-off between the need to distribute m to all community nodes quickly (so as to prevent m being obsolete) and the need for privacy protection. If m is received by a node n_i of a group in broadcast mode, if n_i has arcs toward nodes of other groups that reveal features characterizing m, it may use these arcs to transmit m in point-to - point mode to the respective groups. After illustrating the three possible message modes, we are now looking at the possible types of messages provided by our protocol for the delivery of information. They can be divided into three categories: entering, leaving and querying. We illustrate all of them in the following subsections.

V. SECURITY MODEL

5.1. Attack model

As a preliminary assumption, we find a practical situation in which there is a sufficient number of nodes available for effective implementation of our approach. Therefore, we will not consider anomalous situations where the number of nodes available in the system is less than the minimum number required to ensure, at least in principle, privacy (i.e., $k \cdot \eta$).

In addition, our approach focuses on node information protection and does not address protocol attacks, such as sinkhole attacks or DoS attacks [57,58]. Indeed, for most communication protocols, these risks are normal and the methods to avoid them are orthogonal to our proposition. In our case, some of these approaches, such as those mentioned in [59–61], can be applied in such a way as to make our strategy resilient to these kinds of attacks as well. In light of this basic assumption, we now identify our approach's security properties. They are as follows:

- SP1-Definition of group characteristics ensures node privacy.
- SP2-Our approach is resistant to group resize operations exploiting attacks.
- SP3-Our approach is resistant to timing attacks that exploit interviews with cross-functions.

We will consider the following assumptions in the analysis of the safety properties described above:

- A1-An attacker can't control a whole node group.
- A2-The underlying network provider does not wish to violate the privacy of the node.
- A3-The basic features of the MIoT system (point-to - point communication, etc.) are resistant to attacks.

We'll investigate the above mentioned security properties in the following. A prototype model was constructed to test the approach. The ideas expressed in the simulator design, and in

the next construction of the MIoTs to be used for the experiments, in which the authors emphasize that one of the main factors used to build links in an IoT is node proximity. Our simulator, as mentioned above, associates an object with a given route recorded in the dataset. It also creates an arc between two nodes if the distance between the corresponding routes for a predefined time interval th_t is less than a certain threshold th_d . The thd and tht values can be specified through the interface of the constructors. Clearly the higher this value, the more the IoT that was designed associated. As far as the MIoT construction is concerned, since group creation depends on the sequence of subscriptions of the nodes to our system (which, for simplicity's sake, can be assumed to be random) and on their features, we reproduce it by simulations, as is clear below. When defining the distribution of the features among the nodes, we leveraged scientific literature and used the corresponding results to tune our simulator correctly. We particularly adopted the values stated in [62]. Table 2 provides some information about our dataset.

Table 2. Parameter values for our simulator.

Parameter	Value
Nodes number	1000
Relationships Number	6763
Out-degree mean	6.994
In-degree mean	7.001
Distinct features number	20
Maximum number of equivalence class functions	10
Maximum number of functions per node	3

5.2. Security analysis

5.2.1. SP1 - Defining the group functions ensures node privacy

This property is essential in our approach, as it guarantees that nodes within a group are safeguarded against privacy attacks. To ensure this property, our approach utilizes a combination of k-anonymity and t-closeness. Indeed, k-anonymity fails alone because features aren't evenly distributed among smart objects in real life. So an attacker near a node can take advantage of the function of probability distribution to perform a statistical attack and improve the probability of guessing. Therefore, the distribution of the functions that characterize a new group when selecting k features is taken into consideration in our algorithm. According to the t close-up paradigm, when it comes to their probability distribution, the characterizing features of a group shall belong to an equivalence class. This makes sure that an attacker cannot manipulate the historical information about the popularity of features among intelligent objects in such a way that the least likely is removed. In addition, our protocol once again uses a principle of k anonymity when it relates to group creation, which enables nodes to share information on features freely without being recognized. Indeed, before anonymous broadcast protocol to communicate its functions, each node within the WZ will wait until $\epsilon > k$ nodes become available. Now ϵ can be set to k in the absence of collusion attacks. An attacker can therefore only observe some features of these k nodes, without having any additional advantages when mapping them to the appropriate objects. Furthermore, t-closeness is not required here because the attacker has the same likelihood that each of the k nodes possesses the specified properties. In conclusion, an attacker can only control t nodes simultaneously in accordance with assumptions $A1$ and $A5$. Thus, it is possible to set $\epsilon = k + t$ to preserve the k-anonymity property to block a collusion attack.

5.2.2. SP2 - Our approach is resistant to attacks exploiting group resize operation

The purpose of this property is to protect our system against attacks based on resize observations. Indeed, the

configuration of groups that change with regard to both the number of nodes involved and perhaps the number of features that are available during each resize process. An intruder can test the features of a group by interacting close to the group node or as part of the group. The solution to these attacks takes two countermeasures. The first is to force the resize algorithm so that it can only be activated when k leave is recorded. As a result of Assumption A1, the attacker is unable to control a group and, as a result, is unable to control which nodes leave the system. In addition, we require that η nodes be at least possessed as a further safety measure for each feature. The combination of such counter-measures prevents the assailant from detecting which feature is owned by the nodes left (the likelihood that the characteristics of any other node in the group will be the same). This prevents the attacker from detecting a reduction in the number of features that are available in the group.

5.2.3. SP3 - Our approach is timely and resistant to interviews using cross-functions.

The statistical observation of the node response time in relation to external events provides a common situation attack similar to the one proposed in this paper. In our case, a node for information about predefined features and the time of response can be used to perform this attack. Fast responses may be related to node-owned features while slow (or empty), features owned by the nodes of that same group must also be mapped in order to give a response to the attacked node. Every node uses a pattern recognition algorithm to prevent this type of attack, and enters a protective way each time a suspect querying pattern is recognized. Essentially, when a target node gets a suspicious sequence of consecutive cross-feature queries from a source node, say n_a, a random delay in its responses begins with n_a na. This delay varies from 0 to the average time of response observed in prior communications [4]. In addition, if the node cannot answer two consecutive cross-functional inquiries, it will for a certain time interval no longer answer any next queries from n_a. When coupled with the Assumption $A4$, these two countermeasures prevent the attacker from gaining advantage by interviewing our system node maliciously. Even so, Assumption A4 says the assailant cannot leverage information on certain geographical positions when it makes queries (e.g. to isolate a small set of devices). An attacker can build and submit queries without this assumption which can only be answered by equipment placed in a certain geographic position. This is, of course, a local attack that requires the malicious user to isolate a small number of devices to detect features that belong to them in order to be successful.

VI. Solving the trade-off between privacy requirement and network performance

This section examines the configuration of data protection parameters (k and η) to ensure the desired level of confidentiality. In fact, the higher the demand for privacy, the greater the impact on network performance. Our protocol states that a more demanding requirement for privacy would lead to a group size development. communication among nodes is influenced by both the presence of groups and the anonymous broadcast protocol, which requires the involvement of a random number of nodes inside each group before reaching the desired destination. As a result, both intra-group and inter-group communications are strongly dependent on the size of the group; specifically, the larger the groups, the higher the number of nodes involved. The network 's performance has two direct effects: I the overall network load is increased; (ii) the average trajectory between nodes is increased (which leads to a higher average delays in communications). That's why a first experiment was conducted to simulate our system's behavior and to monitor the group creation. The measurements we have adopted for this study are: (i) the change in the size of the group to the different privacy settings (i.e. the different configurations of k and η); (ii) the change in the length of the communication paths between the nodes after the application of our privacy model. For simulation, we considered the different values of both k and η. Specifically, in the case of k, we selected the range [37], with a step of 1; in the case of η, instead, we considered a multiple of k; in particular, its range was [k, 2k].

We measured the metric I as the first investigation. For this purpose, we simulated a random subscription to our system (i.e. a random arrival order in the Welcome Zone) of the 1000 nodes of the original IoT graph considered in this experiment. We used our algorithm for group formation and measured the average number of nodes within each group, as well as the average number of nodes not participating in the group and therefore waiting in the WZ. In this experiment, we did not consider temporary joints that could be used to minimize the number of nodes not assigned (either temporarily or permanently) to any group. In order to consider the different configurations of the node arrivals, we repeated the experiment 250 times and averaged the corresponding results. It's in Fig. 2, we report the average percentage of all the nodes of the MIoT that are present in the group against the increase of k and η.

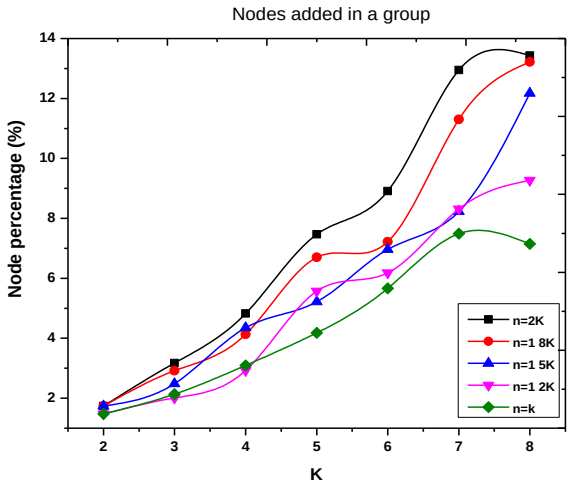

Fig. Fig. 2. Percentage of nodes present in a given group against increase of k and η

Rather than that, Fig. 3 shows the average percentage of all MIoT nodes remaining in WZ compared to the increase of k and η.

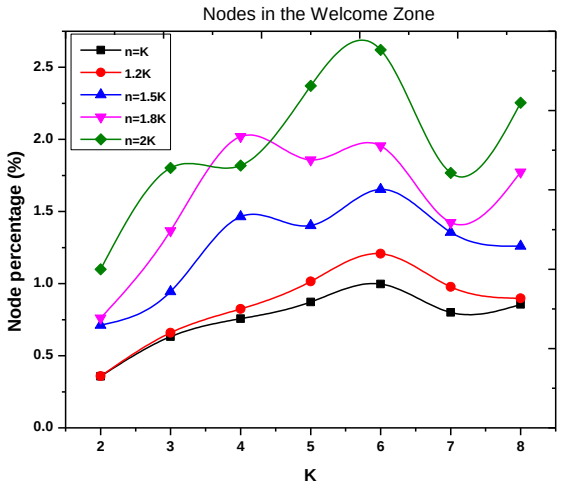

Fig. 3. Percentage of nodes waiting in the Welcome Zone against an increase of k and η.

Analyzing the results obtained, we can observe that the percentage of nodes in a group grows linearly with an increase of both k and η. Interestingly, even with the most demanding privacy requirement (i.e., k = 8 and η = 2 k), it does not exceed 12.5 per cent of the total number of nodes. Of course, as demonstrated in [63], higher values of k do not provide additional benefits once the desired privacy requirement has been met. With regard to this reasoning, we would like to point out that there is no best practice in estimating the right value of k. Typical values in the literature range from 2 to 5. Even then, since our approach to group resize is carried out every time k permanent nodes leave a group, in order to maintain their robustness, we need to have the k-anonymity property guaranteed at the time of departure from the first node to the departure of the kth one (after which the size of the group will be determined by our approach). In the first analysis, we can confirm that, if η is equal to 2 k, no problems will arise before the re-size procedure is carried out. This setting is the most conservative of all but, in contrast, requires a very high number of nodes for each feature. However, if we take into account a limited case in which all leave operations involve nodes possessing only one of the features available without repetition, we could safely set η = k+1 to ensure the k-anonymity property and the operability of the group during leave operations. These considerations are crucial to the proper alignment of η. Indeed, we can conclude that its correct value should range

from k + 1 to 2 k. As a further observation, keeping η to the minimum values significantly reduces the number of nodes still waiting in WZ after group formation. In fact, if we set k = 4 and k < η = 1.2 k, the average percentage of nodes waiting in WZ after the group formation algorithm is about 0.08 per cent. The number of nodes in each group is also low and on average equal to 2.2% of the nodes in the original graph. The objective of the second experiment is to measure the metric (ii). In order to perform this measurement, we applied the same logic adopted in the previous experiment to simulate the formation of groups, but preserved the original links in the graph built from our data set for intergroup connections. Note that this choice is consistent with what should happen in a real-life situation because intergroup connections are increasing in line with the proximity events between nodes belonging to different groups, which is exactly how the links were established in the original IoT graph. Now, given a pair of nodes ($n_{i,}$ n_j) such that $n_{i,} \in G_i$, $n_j \in G_j$, $G_i \neq = G_j$, and there is a path from n_i to n_j in the original graph, Fig. 4 shows the ratio of the length of the path between n_i and n_j in our system to the length of the path between the same nodes in the original graph. This parameter is called "Cost of the Protocol" (hereafter, CoP). The results observed in this figure are averaged over 1,000 pairs of nodes meeting the above requirements. The results obtained show that, if we keep k ≤ 4 and η = 1.21 k, CoP reaches a maximum value of 1.273, which means that the length of the path between the pairs of nodes obtained by applying our approach increases to a maximum of about 26.1% with respect to the length of the original path.

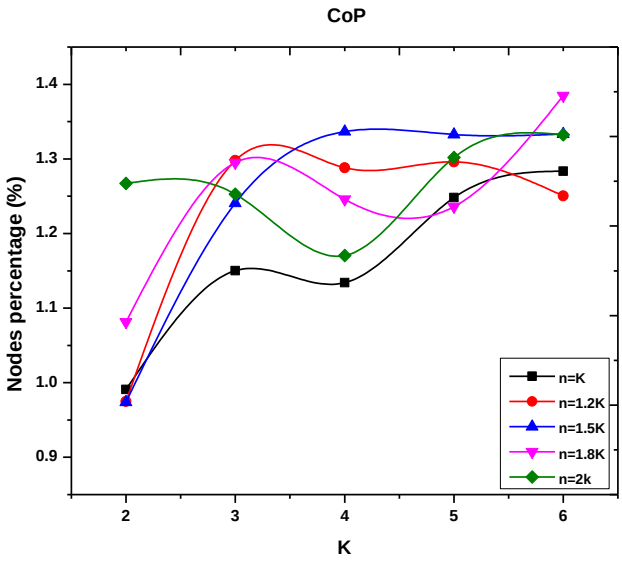

Fig. 4. Value of the COP against the increase of k and η.

VII. DISCUSSION

6.1. Privacy features

We shall begin by analyzing the two features adopted in this paper, namely: (i) k-anonymity and (ii) t-proximity. K-anonymity is a very old notion that, in principle, disclosure of information in a database can be avoided as long as sufficient "noisy" tables (i.e., tables guaranteeing k collisions) can be generated [38]. However, it has also been shown that when dealing with value distributions of attributes, an attacker can take advantage by comparing the distribution in the noisy dataset with the distribution of the real-world attribute to bypass such a privacy mechanism [39]. Consequently, even if k-anonymity can protect against identity disclosure, it cannot protect against attribute disclosure attacks. In this last case, an attacker may use the disclosure of the value of a confidential attribute associated with an external identified individual to infringe k-anonymity features. In real-life situations, the risk of such an attack is very high and therefore the only application of k-anonymity appears to be inadequate for our privacy objectives. T-closeness has been widely studied in scientific literature [30]. It was conceptualized as an evolution of k-anonymity that also protects against the disclosure of attributes. The situation of interest for this paper is very close to those for which t-closeness was designed. Indeed, our aim is to hide the

features (or attributes) of an object behind a group of heterogeneous and equivalent objects (in terms of probability distributions). For this reason, in our approach, we leverage t-closeness to enhance k-anonymity with the ability to protect against attribute disclosure, assuming that object attributes (or features, in our case) have specific and measurable distributions. Interestingly, our solution also recalls the concept of differential privacy [40]. The aim of this kind of privacy solution is to limit knowledge gains between datasets that differ from one individual to another. It initially focused on protecting the results of queries made in the database. Other papers then extended this concept to non-interactive situations (i.e. cases where it is not necessary to protect a specific query or set of queries). These solutions often deal with specific classes of generic queries (usually count ones) [41]. Interestingly, it has been shown that closeness and differential privacy are somehow related to each other [42]. In review the results of Domingo-Ferrer [43] have shown that, in a dataset in which t-closeness is held, differential privacy is guaranteed by projection over confidential attributes.

6.2. Applicability and limitations

With regard to the applicability of our proposal to real-world situations, we stress that our strategy is in line with the new trend of improving the independence of IoT nodes. Our solution finds direct application in this context, because knowledge of the features that characterize objects and the services they provide is essential for improving the efficiency of IoT links. For this reason, it is important to filter the contacts of the object according to the usefulness of the information that the contacts may provide. Of course, as stated throughout this paper, knowledge of the features of an object has a serious impact on the privacy of the user. Clearly, due to the extremely high dynamics of the situation under consideration, our approach has some limitations that need to be taken into account. Indeed, as stated in Assumption A4, our solution does not cover the protection of features related to specific geographical locations. Indeed, without this assumption, the security property SP3 cannot be guaranteed. Consider the case in which an attacker can isolate a node in a given location to clarify this concept. Furthermore, assume that some of the exposed features may be related to the position of the object; consider, for example, the temperature of the room. In this case, the attacker can evaluate whether the node is capable of responding correctly to a question about the temperature of the zone under control. Either a positive or a negative response results in a privacy leak, as the attacker is able to identify one of the features of the object to reduce the allowable set. This security property, in addition to Assumption A4, also requires a pattern recognition solution to detect anomalous interviews with cross-functions. Of course, it is possible to obtain a naïve and very conservative solution by forcing each node to label as suspect each direct interaction with a node that submits queries relating to more than two features. A more sophisticated and refined solution can be obtained by adopting any existing approach to anomalous pattern recognition [71]; however, modeling the normal behavior of nodes requires a base knowledge.

VIII. CONCLUSION

In this study, we proposed a privacy-preserving approach capable of preventing the disclosure of features (and, consequently, information) in an IoT situation. Our approach also ensures privacy in dynamic contexts where many smart objects are highly interconnected to form a collection of (partially overlapping) networks that communicate with one another. We've illustrated the proposed model after studying related literature. Then, we described the object grouping scheme that preserves privacy, which represents the core of our approach. Eventually, we illustrated the corresponding security model and analyzed the associated properties. Our approach provides important advantages for the protection of user privacy in all those situations where knowledge of object features may help an attacker to obtain information about user habits and behavior. As a first research direction, we plan to improve our approach by enhancing group formation, using the likelihood that the associated nodes will be good contacts for each other (i.e. sharing common interests and,

therefore, exchanging valuable information with the other nodes in their group). Indeed, currently, we consider only the features available and the time of arrival in WZ to be the trigger for group creation. It would be useful to understand whether an improved algorithm can be designed in such a way that membership of a group can also be preferred when it leads to an increase in the information available for its nodes. In addition, we plan to include a security mechanism in our approach that prevents malicious nodes from being able to join a group to acquire a given set of features. Although this has no impact on the privacy of other nodes within the group being attacked, it can lead to performance detriment. Solutions based on models of trust and credibility can be implemented to avoid this kind of attack. Empowering our reputational model solution will allow for another future growth. Indeed, our privacy model currently includes some static node protection countermeasures, based on the features involved in the received queries (cross-function interview). The fundamental idea is that an attacking node changes its normal behaviour, by cutting its response rate; nevertheless, no action against the suspected attacker is taken. It may be useful to exploit information about the suspected attacker to train a reputation model, so that nodes can share information about the attacking node if this type of attack happens, thus updating their trust in it and its overall credibility. Finally, a possible attack in our situation could involve a malicious node distributing fabricated information within a group (i.e. handling the messages exchanged). Blockchain can be used as a public directory to avoid such an attack, as any message within it can be securely traced. This enables the analysis of the digest reported in the Blockchain public ledger detect each modification to the messages generated.

IX. REFERENCES

[1]. C. Zhang, L. Zhu, C. Xu, K. Sharif, X. Du, and M. Guizani, "LPTD: Achieving lightweight and privacy-preserving truth discovery in CIoT," Future Generation Computer Systems, vol. 90, pp. 175-184, 2019.

[2]. A. I. Khan and A. Al-Badi, "Open Source Machine Learning Frameworks for Industrial Internet of Things," Procedia Computer Science, vol. 170, pp. 571-577, 2020/01/01/ 2020.

[3]. E. Curry, W. Derguech, S. Hasan, C. Kouroupetroglou, and U. ul Hassan, "A real-time linked dataspace for the internet of things: enabling “pay-as-you-go” data management in smart environments," Future Generation Computer Systems, vol. 90, pp. 405-422, 2019.

[4]. G. Baldassarre, P. L. Giudice, L. Musarella, and D. Ursino, "A paradigm for the cooperation of objects belonging to different IoTs," in Proceedings of the 22nd International Database Engineering & Applications Symposium, 2018, pp. 157-164.

[5]. K. Skiadopoulos, K. Oikonomou, M. Avlonitis, K. Giannakis, D. Kogias, and I. Stavrakakis, "Multiple and replicated random walkers analysis for service discovery in fog computing IoT environments," Ad Hoc Networks, vol. 93, p. 101893, 2019/10/01/ 2019.

[6]. G. Baldassarre, P. L. Giudice, L. Musarella, and D. Ursino, "The MIoT paradigm: main features and an “ad-hoc” crawler," Future Generation Computer Systems, vol. 92, pp. 29-42, 2019.

[7]. X. Lu, J. Liu, W. Qi, and Q. Dai, "Multiple-target tracking based on compressed sensing in the Internet of Things," Journal of Network and Computer Applications, vol. 122, pp. 16-23, 2018/11/15/ 2018.

[8]. L. Atzori, A. Iera, G. Morabito, and M. Nitti, "The Social Internet of Things (SIoT) – When social networks meet the Internet of Things: Concept, architecture and network characterization," Computer Networks, vol. 56, pp. 3594-3608, 2012/11/14/ 2012.

[9]. R. M.S, S. Pattar, R. Buyya, V. K.R, S. S. Iyengar, and L. M. Patnaik, "Social Internet of Things (SIoT): Foundations, thrust areas, systematic review and future directions," Computer

Communications, vol. 139, pp. 32-57, 2019/05/01/ 2019.

[10]. M. Aloqaily, S. Otoum, I. Al Ridhawi, and Y. Jararweh, "An intrusion detection system for connected vehicles in smart cities," Ad Hoc Networks, vol. 90, p. 101842, 2019.

[11]. Y. Zhang, R. H. Deng, G. Han, and D. Zheng, "Secure smart health with privacy-aware aggregate authentication and access control in Internet of Things," Journal of Network and Computer Applications, vol. 123, pp. 89-100, 2018/12/01/ 2018.

[12]. S. Munirathinam, "Chapter Six - Industry 4.0: Industrial Internet of Things (IIOT)," in Advances in Computers. vol. 117, P. Raj and P. Evangeline, Eds., ed: Elsevier, 2020, pp. 129-164.

[13]. S. Sicari, A. Rizzardi, and A. Coen-Porisini, "5G in the Internet of Things era: an overview on security and privacy challenges," Computer Networks, p. 107345, 2020/06/02/ 2020.

[14]. D. Mocrii, Y. Chen, and P. Musilek, "IoT-based smart homes: A review of system architecture, software, communications, privacy and security," Internet of Things, vol. 1-2, pp. 81-98, 2018/09/01/ 2018.

[15]. S. M. Tahsien, H. Karimipour, and P. Spachos, "Machine learning based solutions for security of Internet of Things (IoT): A survey," Journal of Network and Computer Applications, vol. 161, p. 102630, 2020/07/01/ 2020.

[16]. S. N. Mohanty, K. C. Ramya, S. S. Rani, D. Gupta, K. Shankar, S. K. Lakshmanaprabu, et al., "An efficient Lightweight integrated Blockchain (ELIB) model for IoT security and privacy," Future Generation Computer Systems, vol. 102, pp. 1027-1037, 2020/01/01/ 2020.

[17]. B. K. Mohanta, D. Jena, U. Satapathy, and S. Patnaik, "Survey on IoT security: Challenges and solution using machine learning, artificial intelligence and blockchain technology," Internet of Things, vol. 11, p. 100227, 2020/09/01/ 2020.

[18]. M. U. Hassan, M. H. Rehmani, and J. Chen, "Privacy preservation in blockchain based IoT systems: Integration issues, prospects, challenges, and future research directions," Future Generation Computer Systems, vol. 97, pp. 512-529, 2019/08/01/ 2019.

[19]. A. Ouaddah, "Chapter Eight - A blockchain based access control framework for the security and privacy of IoT with strong anonymity unlinkability and intractability guarantees," in Advances in Computers. vol. 115, S. Kim, G. C. Deka, and P. Zhang, Eds., ed: Elsevier, 2019, pp. 211-258.

[20]. H. HaddadPajouh, A. Dehghantanha, R. M. Parizi, M. Aledhari, and H. Karimipour, "A survey on internet of things security: Requirements, challenges, and solutions," Internet of Things, p. 100129, 2019/11/09/ 2019.

[21]. R. Hou, G. Ren, C. Zhou, H. Yue, H. Liu, and J. Liu, "Analysis and research on network security and privacy security in ubiquitous electricity Internet of Things," Computer Communications, vol. 158, pp. 64-72, 2020/05/15/ 2020.

[22]. F. Allhoff and A. Henschke, "The Internet of Things: Foundational ethical issues," Internet of Things, vol. 1-2, pp. 55-66, 2018/09/01/ 2018.

[23]. G. K. M. Abomhara, "Security and privacy in the internet of things: Current status and open issues," Proc. of the International Conference on Privacy and Security in MMbile Systems, PRISMS'14, IEEE, Aalborg, Denmark,, pp. 1-8, 2014.

[24]. A. A. A. Ari, O. K. Ngangmo, C. Titouna, O. Thiare, Kolyang, A. Mohamadou, et al., "Enabling privacy and security in Cloud of Things: Architecture, applications, security & privacy challenges," Applied Computing and Informatics, 2019/11/22/ 2019.

[25]. D. Minoli, "Positioning of blockchain mechanisms in IOT-powered smart home systems: A gateway-based approach," Internet of Things, p. 100147, 2019/11/27/ 2019.

[26]. R. Shrestha and S. Kim, "Chapter Ten - Integration of IoT with blockchain and homomorphic encryption: Challenging issues and opportunities," in Advances in Computers. vol. 115, S. Kim, G. C. Deka, and P. Zhang, Eds., ed: Elsevier, 2019, pp. 293-331.

[27]. M. Amiri-Zarandi, R. A. Dara, and E. Fraser, "A Survey of Machine Learning-based Solutions to Protect Privacy in the Internet of Things," Computers & Security, p. 101921, 2020/06/01/ 2020.

[28]. S. Zhang, X. Li, Z. Tan, T. Peng, and G. Wang, "A caching and spatial K-anonymity driven privacy enhancement scheme in continuous location-based services," Future Generation Computer Systems, vol. 94, pp. 40-50, 2019/05/01/ 2019.

[29]. Y. Wang, Z. Cai, Z. Chi, X. Tong, and L. Li, "A differentially k-anonymity-based location privacy-preserving for mobile crowdsourcing systems," Procedia Computer Science, vol. 129, pp. 28-34, 2018/01/01/ 2018.

[30]. T. L. N. Li, S. Venkatasubramanian, "t-closeness: Privacy beyond kanonymity and l-diversity," Proc. of the International Conference on Data Engineering, ICDE'07, IEEE, Istanbul, Turkey, pp. 106–115, 2007.

[31]. M. Quwaider and Y. Shatnawi, "Congestion Control Model for Securing Internet of Things Data Flow," Ad Hoc Networks, p. 102160, 2020/05/19/ 2020.

[32]. H. S. Trivedi and S. J. Patel, "Design of secure authentication protocol for dynamic user addition in distributed Internet-of-Things," Computer Networks, vol. 178, p. 107335, 2020/09/04/ 2020.

[33]. H. Elazhary, "Internet of Things (IoT), mobile cloud, cloudlet, mobile IoT, IoT cloud, fog, mobile edge, and edge emerging computing paradigms: Disambiguation and research directions," Journal of Network and Computer Applications, vol. 128, pp. 105-140, 2019/02/15/ 2019.

[34]. A. Alnaied, M. Elbendak, and A. Bulbul, "An intelligent use of stemmer and morphology analysis for Arabic information retrieval," Egyptian Informatics Journal, 2020/03/07/ 2020.

[35]. R. I. Meneguette, A. Boukerche, F. A. Silva, L. Villas, L. B. Ruiz, and A. A. F. Loureiro, "A novel self-adaptive content delivery protocol for vehicular networks," Ad Hoc Networks, vol. 73, pp. 1-13, 2018/05/01/ 2018.

[36]. C. Borrego, J. Borrell, and S. Robles, "Efficient broadcast in opportunistic networks using optimal stopping theory," Ad Hoc Networks, vol. 88, pp. 5-17, 2019/05/15/ 2019.

[37]. J. Sengupta, S. Ruj, and S. Das Bit, "A Comprehensive Survey on Attacks, Security Issues and Blockchain Solutions for IoT and IIoT," Journal of Network and Computer Applications, vol. 149, p. 102481, 2020/01/01/ 2020.

[38]. M. Ehara, H. Samejima, M. Yamanoshita, Y. Asada, Y. Shogaki, M. Yano, et al., "REDD+ engagement types preferred by Japanese private firms: The challenges and opportunities in relation to private sector participation," Forest Policy and Economics, vol. 106, p. 101945, 2019/09/01/ 2019.

[39]. S. Nicolazzo, A. Nocera, D. Ursino, and L. Virgili, "A privacy-preserving approach to prevent feature disclosure in an IoT scenario," Future Generation Computer Systems, vol. 105, pp. 502-519, 2020/04/01/ 2020.

[40]. S. Zapechnikov, "Privacy-Preserving Machine Learning as a Tool for Secure Personalized Information Services," Procedia Computer Science, vol. 169, pp. 393-399, 2020/01/01/ 2020.

[41]. Y. Li, D. Yang, and X. Hu, "A differential privacy-based privacy-preserving data publishing algorithm for transit smart card data," Transportation Research Part C: Emerging

Technologies, vol. 115, p. 102634, 2020/06/01/ 2020.

[42]. P. Wang and H. Zhang, "Differential privacy for sparse classification learning," Neurocomputing, vol. 375, pp. 91-101, 2020/01/29/ 2020.

[43]. J. Domingo-Ferrer and J. Soria-Comas, "From t-closeness to differential privacy and vice versa in data anonymization," Knowledge-Based Systems, vol. 74, pp. 151-158, 2015/01/01/ 2015.

Cite this article as :

Frimpong Atta Junior Osei, Sidique Gawusu, Xuezhi Wen, Yu Zheng, Daniel Appiah Kumah, "A study On : Confidentiality Approach to Prevent Features Disclosure in IoT Situations", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 6, Issue 3, pp.616-632, May-June-2020. Available at
doi : https://doi.org/10.32628/CSEIT2063146
Journal URL : http://ijsrcseit.com/CSEIT2063146