IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

SPECIAL SECTION ON RECENT ADVANCES IN COMPUTATIONAL INTELLIGENCE PARADIGMS FOR SECURITY AND PRIVACY FOR FOG AND MOBILE EDGE COMPUTING

Received October 5, 2016, accepted October 13, 2016, date of current version January 4, 2017.

Digital Object Identifier 10.1109/ACCESS.2016.2631546

A Fog Based Middleware for Automated Compliance With OECD Privacy Principles in Internet of Healthcare Things

AHMED M. ELMISERY[1], SEUNGMIN RHO[2], AND DMITRI BOTVICH[3]

[1]Department of Electronics Engineering, Universidad Tecnica Federico Santa Maria, 1680 Valparaiso, Chile
[2]Department of Media Software, Sungkyul University, Anyang, South Korea
[3]Gaspard Monge Computer Science Laboratory, Université Paris-Est Marne-la-Vallée, Paris, France

Corresponding author: S. Rho (smrho@sungkyul.ac.kr)

This work was supported in part by the Dirección General de Investigación, Innovación y Postgrado of Federico Santa María Technical University- Chile, in the Project Private and Secure Mobile Cloud Framework for Medical IoT Devices (UTFSM-DGIP 116.23.3), in part by the Basic Science Research Program through the National Research Foundation of Korea Funded by the Ministry of Education under Grant 2013R1A1A2061978.

ABSTRACT Cloud-based healthcare service with the Internet of Healthcare Things (IoHT) is a model for healthcare delivery for urban areas and vulnerable population that utilizes the digital communications and the IoHT to provide flexible opportunities to transform all the health data into workable, personalized health insights, and help attain wellness outside the traditional hospital setting. This model of healthcare Web services acts like a living organism, taking advantage of the opportunities afforded by running in cloud infrastructure to connect patients and providers anywhere and anytime to improve the quality of care, with the IoHT, acting as a central nervous system for this model that measures patients' vital statistics, constantly logging their health data, and report any abnormalities to the relevant healthcare provider. However, it is crucial to preserve the privacy of patients while utilizing this model so as to maintain their satisfaction and trust in the offered services. With the increasing number of cases for privacy breaches of healthcare data, different countries and corporations have issued privacy laws and regulations to define the best practices for the protection of personal health information. The health insurance portability and accountability act and the privacy principles established by the Organization for Economic Cooperation and Development (OECD) are examples of such regulation frameworks. In this paper, we assert that utilizing the cloud-based healthcare services to generate accurate health insights are feasible, while preserving the privacy of the end-users' sensitive health information, which will be residing on a clear form only on his/her own personal gateway. To support this claim, the personal gateways at the end-users' side will act as intermediate nodes (called fog nodes) between the IoHT devices and the cloud-based healthcare services. In such solution, these fog nodes will host a holistic privacy middleware that executes a two-stage concealment process within a distributed data collection protocol that utilizes the hierarchical nature of the IoHT devices. This will unburden the constrained IoHT devices from performing intensive privacy preserving processes. Additionally, the proposed solution complies with one of the common privacy regulation frameworks for fair information practice in a natural and functional way—which is OECD privacy principles. We depicted how the proposed approach can be integrated into a scenario related to preserving the privacy of the users' health data that is utilized by a cloud-based healthcare recommender service in order to generate accurate referrals. Our holistic approach induces a straightforward solution with accurate results, which are beneficial to both end-users and service providers.

INDEX TERMS Internet of healthcare things, cloud based healthcare services, holistic privacy.

I. INTRODUCTION

The Internet of Things (IoT) is evolving into an extensive network of small and specific-purpose objects with low power consumption that represent the latest phase in evolution of the Internet. International Data Corporation (IDC) predicted in a recent report, in 2020, the market for IoT would reach

$1.7 trillion (from $655.8 billion in 2014) [35]. Research firm Gartner forecasts that the current 4.9 billion connected ''things'' in 2015 will expand to 25 billion by 2020 [46], while the Harvard Business Review predicted that the IoT is expected to connect 28 billion ''things'' to the Internet by 2020 [36]. These connected things will be ranging from wearable devices, such as smart watches to automobiles, electric appliances, smart homes, smart cities, cameras and industrial equipment. While there is a swing in the estimates in the number of ''things'' that will be connected to the Internet, this evolution is bigger than refrigerators planning ahead our grocery shopping. The IoT is going to have a positive profound impact to the world with expected repercussions span various industries and domains; one of the sectors which leads this impressive growth is the healthcare field. In fact, a new acronym has emerged as part of this movement: IoHT, which stands for ''Internet of Healthcare Things''- that reflects the identification of the healthcare field as a subsector of IoT [12]. Approximately 65% of enterprises already utilize IoT solutions for business purposes, according to a recent survey conducted by 451 Research [29] The healthcare industry is among the fastest to embrace the Internet of things, as reported by the survey projected in the report, healthcare organizations collect 49 per cent of data from IoT medical devices. The reason for this trend is that embedding IoT features into healthcare devices considerably enhances the quality and efficacy of healthcare services, delivering greater value for patients requiring constant supervision. The research firm ''MarketsAndMarkets'' [44] claims that the healthcare segment of IoT will be worth $163.2B by 2020, while a new mind commerce report [43] predicts healthcare IoT spending of $117B for that year. Additionally, a recent report from McKinsey [42] estimates that IoHT could have an economic impact of more than $170 billion to $1.7 trillion a year. By 2025, FierceHealthIT report estimates that the IoHT will potentially attain a ''total economic impact'' of almost $4 trillion up to possibly $11.1 trillion per year. This projected figure is based on ''cost savings in treatment and the value of longer lives and improved quality of life that patients with chronic conditions could enjoy if IoT monitoring helps them avoid disease complications [15]. It is expected that more organizations will adopt the IoT to cut costs in the future [29]. Finally, McKinsey report [42] demands the healthcare industry to make significant reforms for IoHT to have full impact by increasing the acceptance of wellness and health devices among various patients' groups and properly addressing challenges related to privacy, security and compliance.

With the increasing demands for a greater focus on health and wellbeing and recent advances in digital communications, patients now have the ability to connect with remote healthcare services whereever they may be, taking a greater sense of empowerment and choice, and impelling the ''customization of healthcare''. Different healthcare services have been developed since the last decade and they have had a profound effect on today's society. With the emergence of Internet of healthcare things and the spread of software-as-a-service and cloud computing technologies, there has been a growing demand of providing services that support IoHT devices. Internet of healthcare things can be most simply defined as a large network of physical devices encompassing software, sensors and connectivity, which allows the exchange of data with external cloud based service in order to provide greater healthcare value and service. The future of care delivery in typical IoHT paradigm centers on a networked devices utilizing both wired and wireless technologies, a personal gateway capturing health data and cloud based healthcare services in which patients can securely share their health related data to obtain highly personalized, accessible, and on-time healthcare services. IoHT paradigm will fundamentally enhance healthcare delivery models in our society especially for elderly, disabled and those with chronic conditions by minimizing their need for direct patient-specialist interaction and allowing the remote healthcare services to deliver more personalized health insights, using health data from wearables and implants in a secure and trustworthy manner. However, the current spread of IoHT enlarges the attack surface to a scope that have never been achieved before, according to a recent report [52], IoT devices are coming with severe security flaws that no longer exist in modern computing systems, and the only reason for not exploiting these flaws is hackers have not been interested in exposing such systems till now. At the same time, additional computing resources are required to satisfy the overhead introduced by various security functions; nevertheless, IoT devices pose constraints on computation and communication resources due to the limited energy budget. This poses significant challenges in terms of security as it adds constraints to the types of security functions that should be deployed on such system. Designing a secure IoHT system in such conditions is problematic. In order to mitigate these limitations, one of the most favorable perspectives is to integrate IoT devices with the cloud environments 'thus' these devices will benefit from a general utility providing on demand computing resources.

The integration of cloud computing paradigm and Internet of healthcare things are reshaping the healthcare domain. The spread of chronic diseases around the world sweeping amendments ushered in by an affordable care act and a public acceptance to restrain rising healthcare costs mean that healthcare providers must find new ways to become precise and more impactful especially for urban areas and vulnerable population without renouncing quality of care. Cloud based healthcare services with Internet of healthcare things is a model for healthcare delivery that utilizes digital communications and the IoHT devices to provide flexible opportunities for quality healthcare outside of the traditional hospital setting, connecting patients and providers anywhere and anytime, and patient experience. Cloud-based healthcare services are perpetually being deployed, where an increasing volume of personal health data is being processed in return for personally tailored health insights for wellness and

preventive services that will help the end-users to perform personalized life-style that will improve their health. This personalization task is performed by a health recommender service, which might be running as part of the healthcare web service or as a third party service. In the first case, healthcare service providers are required to buy, build, train, and maintain their health recommender system infrastructures despite exponential costs. Moreover, in order to run this service well, providers need to recruit a highly specialized team to tune and handle ongoing problems that arise once the service runs. However, in the second case, the healthcare service providers could opt for the outsource service model as it enables them to overcome their lack of computational power or expertise. They can plug in and subscribe to a cloud based healthcare service provider running the health recommender service built on shared infrastructure via the Internet, where user's health data is outsourced to this health recommender service to perform the desired processing thereon. The recognition of the outscore service model is steadily increasing because it simplifies deployment and reduces client acquisition costs. Multitenancy feature of those online services permits cloud-based healthcare service providers to scale as quick and as much as needed without replacing costly infrastructures or adding IT staff. However, such outsource service model raises privacy issues as cloud based healthcare service providers might be situated abroad with totally different legal structures and data privacy laws.

Privacy violations are prohibited in many countries. However, there is an absence of effective methods to enforce the law. This downside is exacerbated once information is used about individuals without their knowledge. As it should, if the customer has the proof that his/her privacy has been violated by the provider, he/she could complain to the proper authorities, so that justice might be served. However, no amount of ''justice'' can fully restore his/her privacy. Two common means can be utilized for guaranteeing the privacy, technological, and legislative solutions. The former approach refers to technical methods and tools that are integrated into systems or networks to reduce the collection of accurate personal health data. Such methods and tools are referred to as privacy enhancing technologies (PETs). One example of such PETs, which will be mentioned during this paper, is a holistic privacy middleware that executes topological formation for data collection along with a two-stage concealment process that aims to control the amount of information that end-users reveal in the initial contact, eliminates the necessity to release personal health data in the raw form, and permits the end-users to act anonymously. As for privacy legislation, it refers to data protection legislation restricting the gathering and usage of private health data by data processors in order to define the best practices for the protection of personal health information. Five examples for such privacy guidelines are the EU Directives 95/46/EC [14] and 2002/58/EC [10], UK's Data Protection Act, The health insurance portability and accountability act (HIPAA) [49], and OECD privacy principles [11]. Despite the fact that several nations have developed privacy protection laws and regulations to guard against the secret use of personal health information, the present laws and their conceptual foundations have become outdated because of the continuous changes in technology [8]. As a result, these personal health data reside on databases of service providers, largely beyond the control of existing privacy laws, leading to a potential privacy invasion on a scale never before possible. It is commonly believed that privacy is most successfully protected by a holistic solution that combines both technological and legislative efforts.

Among several existing approaches to recommender services that pride themselves in providing accurate recommendations, only a few tackle the privacy issues and aim to manage privacy risks of recommender systems as addressed by [56]. Most of the ''privacy-concerned'' recommender services developed nowadays are either based on a trusted third-party model or on some generalized architecture. In order to use the recommender service, the end-users have to divulge their personal health data to the remote recommender service and expect that the service providers will not use it in a malicious manner. Moreover, other systems address this problem with techniques to protect the processing of data stored on untrusted providers' systems. Besides, several of the existing recommender services that are based on multi-party recommendation protocols did not take into consideration the privacy issue. Therefore, our main challenge in this paper is to design an efficient privacy enhancing framework that shields against unauthorized access to the user's personal health data, while at the same time exposing a sufficient amount of information to the cloud based healthcare recommender service in order to extract useful recommendations.

This paper presents holistic privacy middleware for IoHT based healthcare services using fog nodes (personal gateways) as a privacy enforcement points. Counting on this, a novel approach where sensitive health data has two copies a concealed version, which is located on the cloud based healthcare recommender service side and a plain version that is stored on the user's side or in his/her fog node. More precisely, our approach for enhancing the user's privacy is to utilize the personal gateways at the end-users side as intermediate fog nodes between IoHT devices and cloud based healthcare services. These fog nodes will host the proposed holistic privacy middleware and user's health profiles. The user's health data can be either kept private on his/her side, or released in a concealed form. The latter implies that health data is shared in a private manner after concealing it using a two-stage concealment process. The non-resource constrained feature of these fog nodes will unburden the constrained IoHT devices from performing intensive privacy preserving processes. Additionally, the proposed holistic middleware that takes into consideration the topological formation of IoHT devices when collecting users' health data for these services. This holistic middleware can be utilized for cloud based healthcare services to facilitate access to a wealth of users' health data in a privacy-preserving manner. Our aim is not only limited to preventing the disclosure of sensitive

health data but also preserving the usefulness of health data as much as possible to be only effective for the required healthcare decision making process. Employing IoHT based healthcare services promotes quality life and health to its patients, by providing freedom to live a normal life like any healthy person with the trust that a caregiver is following their health states continuously. This gives the opportunity to boost patients' healthcare within any location by continuous monitoring and reduces the inpatient load on schedule at health care organizations. The rest of this paper is organized as follows. In Section 2, related works are described. Section 3 introduces OECD privacy principles and their implication in designing an efficient privacy enhancing frameworks. The proposed solution based on our holistic privacy middleware entitled EMCP (Enhanced Middleware for Collaborative Privacy) is introduced in Section 4. In Section 5, motivations and restrictions of the various prospective parties in our holistic privacy approach are depicted in detail. Possible scenarios for the holistic privacy middleware were demonstrated in Section 6. In Section 7, the middleware prototype is presented. Finally, the conclusion and future research are given in Section 8.

II. RELATED WORK

Recently, there has been an emerging trend in the usage of wearable healthcare sensors that come in different sizes and forms, such as auto-injectors, wearable imaging machines,[1] brainware wireless EEG,[2] cardiac pacemakers, continuous glucose monitoring sensors, and myriad of healthcare sensors that are currently being integrated into smart phones [60]. These devices enable their owners to smoothly collect a broad range of vital sign parameters such as their personal life-style (e.g., diet particulars and physical daily activities), physiological data (e.g., blood pressure (BP), heart rate (HR), electrocardiogram (ECG), blood glucose (BG), respiratory rate (RR), and brain activities), and contextual related data (e.g., locations and time). Following the same trend is the proliferation of cloud based health and wellness applications [9] that enable patients to track and share their health data with other patients. For example, Health devices such as Garmin Connect[3] or Fitbit[4] allow the users to upload and share their physiological data while doing exercises on purpose driven social networks such as Strava.[5] In such case, the users will be able to regularly track their physiological data along with their daily physical activities. Other devices such as Hexoskin smart shirt[6] have their own online web dashboard service that enable the users to monitor their physiological data and diet particulars while sleeping. Leading enterprises are currently turning toward the provision of healthcare services on their platforms. For example, Apple® has lately reported the release of the HealthKit APIs on iOS platform,[7] which enables health and fitness applications to communicate and share health data with each other or across various devices via iCloud. It also enables the end-users to monitor their aggregated health data collected from miscellaneous devices or applications they are using, and then perform statistical analysis on it. Moreover, Apple® is currently cooperating with diverse healthcare providers to offer online health insights for its registered customers. Similarly, Alphabit® recently released Google fit SDK[8] for android[9] operating system which will allow its registered customers to store their health data on Google cloud storage service. In return, customers will be rewarded discount coupons or cash.

In practice, end-users have shown an increasing concern for sharing their private health data, especially in the case of untrusted parties [51]. This occurs due to the following reasons: First, the health data collected by IoHT devices is personal by nature, e.g., patients might choose not to disclose their physical daily activities, stress levels or the location and time where they perform workout. Second, in spite of the ostensibly innocuous nature of collected vital signs, they can be utilized to infer further private and sensitive health related problems, physical activities or emotions that could be deliberately kept hidden. For example, it is possible to deduce sensitive personal information from the brainwave data of users wearing popular brainwear wireless EEG headsets [45], such as digits of PIN numbers, credit card data, birth months, areas of residence and other private information. Third, the automated nature of data capture raises concerns over personal information privacy as various private data could be gathered without their consent/knowledge by malicious attackers or third party service providers. Thereby, the unintentional disclosure of their health data might be embarrassing or employed to discriminate against the users. Additionally, the lack of transparency in the way service providers manage data breaches and mishandling issues due to malicious or criminal attacks based on lapses in their security deployments. For example, security experts managed to remotely exploit vulnerabilities in drug infusion pumps to tweak drug amount to fatal dose that would harm any patient [58]. In most cases, these issues can forestall the wide-scale acceptance and viability of cloud based healthcare services with Internet of healthcare things. As a result, the need to protect users' sensitive health data is more crucial than ever as the end-users of these services have shown an increasing concern for exposing their personal health data to untrusted entities so as to receive value-added services [51]. They need to realize full control over their sensitive health data collected by these services and cannot accept a compromise that their health data might be fully accessible to an external party.

For the description and review of related work, we identify three fundamental research categories. First Pervasive

[1] https://pristine.io/
[2] http://emotiv.com
[3] http://connect.garmin.com
[4] http://www.fitbit.com
[5] http://www.strava.com
[6] http://www.hexoskin.com
[7] https://developer.apple.com/ios
[8] https://developers.google.com/fit
[9] https://www.android.com

healthcare systems are discussed. Depending on this, IoT-based healthcare security solutions are reviewed. Finally, Privacy-enhanced recommender systems are shortly surveyed.

A. PERVASIVE HEALTHCARE SYSTEMS

Existing literature contain solutions for e-health systems to offer remote patient care through continuous monitoring. These solutions have been promoted to improve quality of life of patients with different types of diseases. The embedding of networked sensors in pervasive healthcare devices assist in creating a smart healthcare environment, where patients' health states can be monitored in an inconspicuous way [61]. M-Psychiatry is a psychiatric health monitoring system that offers enhanced healthcare service for patients with affective disorders [3]. Patients can control the m-psychiatry monitoring system via their handled devices that act as a gateway to relay health data from the body sensor network and the Internet to communicate with healthcare providers. The M-psychiatry system consists of three primary components: a body sensor network that is composed of different types of sensors, which are varying from patient to patient, a network gateway that connects the sensors network to a wide area network and query stations which are back-end servers used by healthcare professionals to alter and query the sensed data stored in the m-psychiatry's data store. The m-psychiatry system allows the registration and substitution of a wide variety of sensors. Additionally, the system allows the patients to control the monitoring process and gives them the ability to stop it whenever they want. The collection of data via m-psychiatry system is preferable to paper-based collection for a number of reasons, such as responsiveness, time, labor and cost savings, clinician data entry reduction, prevention of data entry errors, reduction of missing information, and standardized data collection.

A similar system that offers the same functionality was proposed in [4]. The C-SMART is a mobile health platform for continuous real time remote monitoring. The platform covers the communication between a set of sensors on patient's body, a mobile phone, and a centralized healthcare server. The main advantage of C-SMART is that it is implemented on application layer and thus can be compatible to different existing telemedicine and medical database standards with minimal overhead. The C-SMART is working in a plug and play manner but yet to give the user maximum control on the system operation. This property facilitates interfacing to a wide variety of vendors' devices and sensors and it is attained by forming a dedicated remote control and installation center and by using an operation menu on the mobile phone. The authors in [1] presented a completely distributed approach to help in medical diagnosis of disease propagation using wireless body area networks. Additionally, they discussed the basic building blocks of mobile wireless body area network platform. The architecture of this platform usually consists of three-tier as follows:

- 1st Tier is client (Sensor Node), which is wearable, or implantable sensor device placed on patient body.
- 2nd Tier is middleware (Personal Server), which is the personal server, with its computer software could be installed on a personal computer or smartphone.
- Finally, the 3rd Tier is back-end server (Database Server), which is the database server located in the medical institution.

With this architecture, the healthcare monitoring system can detect some diseases indoor and outdoor, and also investigate people who may have a disease, who may propagate epidemic diseases and who move in an urban region. The personal server in their system is implemented by using Java programming language and has a direct connection with the sensor nodes and the back-end server to be able to receive and forward the medical data in a real-time. Once the personal server receives event messages from the sensor nodes, a local reasoning is executed to determine the user's health status and present the feedback through an efficient graphical interface user.

Provisioning quality of service support for wireless sensor networks in e-Health services was discussed in [57]. This work goes further and studies the QOS aspects of e-health wireless networks. The authors have compared recent significant works in this topic regarding QoS requirements that the particular authors of these works have considered significant to incorporate on their research. In their perspective, QoS in the context of e-health wireless networks can be considered as the degree to which the system executes its intended functions and mechanism exists to support this performance. First, The QoS requirements of the system and the users must be examined, before the implementation of relevant QoS mechanisms and protocols. Hence, their work mainly focused on three layers, the data link layer which is utilized for media access control, the network layer that is responsible for scheduling and discovering the best path available, and finally, the transport layer provides an end-to-end communication services. According to the surveyed work in [57], They underlined the need for e-health wireless networks to provide quality of service support such guarantee for latency, aside from congestion control, reliability, service differentiation, and throughput. The e-health wireless network must prioritize the delivery of vital data when unexpected change occurs in patients' health states, therefore, it is important to differentiate all the collected health data. Since all network layers are interacting with each other, multiple layers affect the features which are previously mentioned. Accordingly, there is a need for a framework considering all these features to provide a cross layer optimization. Given the limited resources of nodes, the complexity of such framework has to be simple. In our work, quality of service has not been considered. However, given its importance, it is planned as a future work to implement a model to monitor some quality of service while preserving privacy and security of patients.

Another system has been proposed in [48]. Healthopia is a full-fledged health-monitoring platform that enables the

development of various mobile healthcare applications over smartphones and wearable sensor devices. This integrated platform manages all the health-monitoring requests from these applications, which liberate them from several complicated service issues. Healthopia takes charge of underlying issues for health monitoring; from accurate health data analysis and inferring, to resource optimization, and to private data management and delivery. With the novel resource-efficient sensor control technique in Healthopia platform, the mobile healthcare applications can specify their monitoring queries in the conjunctive form of multiple contexts, which achieves a high level of resource efficiency without the sacrifice of application quality. Healthopia has four components, which are essential to support mobile healthcare applications. The health monitor is responsible for health information monitoring. It continuously processes sensor data and recognizes the health information. The resource efficient sensor controller manages the resources of the sensors. It selects the essential sensors for monitoring the queries and resolves the conflicts of the applications for a shared resource. The privacy controller preserves the privacy of user's health information. It enables the user to select the trusted applications and prohibits untrusted applications from accessing his/her health information. Finally, the sensor broker manages wearable health sensors. By periodically broadcasting the beacon message, it dynamically discovers available nearby sensors. It also interprets sensor data and sensor control messages. Application developers can easily develop diverse mobile healthcare applications while utilizing Healthopia platform to handle monitoring requests, taking care of complicated underlying issues in sensor data processing and resource management, and automatically capture the requested health information e.g., calorie consumption, heart condition, pollution level.

B. IoT-BASED HEALTHCARE SECURITY SOLUTIONS

The CodeBlue project has been proposed in [62]. The basic idea for the CodeBlue approach is to place multiple medical sensors on a patient's body (e.g., pulse oximeter, EMG, EKG, and SpO2 sensor board onto the Mica2 motes) within in-hospital environment in order to aid in rehabilitation and disaster response for stroke patients. The developers of CodeBlue intentionally left security and privacy aspects as a future work to exploit both opportunities and challenges. However, they stress on the need to develop general security solutions for IOT based healthcare application. The authors in [40] propose to employ cryptography tools such as TinyECC for the key generation and TinySEC for symmetric encryption in the CodeBlue project. Another research project called PAM (personal ambient monitoring) was proposed in [3], which is concerned with mental health monitoring. The project aims to develop a sensor network infrastructure for mobile phones and a rule-based paradigm for monitoring the activity signatures of individuals with bipolar disorder. PAM system consists of two parts: firstly, a network infrastructure (PAM-I) composed of off-the-shelf wireless medical sensors, mobile phones and personal computers, and secondly a programming architecture (PAM-A) that utilizes rule-based paradigm to control monitoring settings and the processing of stream data. PAM-I employs the Bluetooth protocol to connect between wireless medical sensors and mobile phones. Aside from multiple communications standards such as IEEE 802.11b/g and X10, the Bluetooth protocol can also be used to connect mobile phones with personal computers. The wireless medical sensors are equipped with computing and communication capabilities to collect and transmit the sensed health data to mobile phones. These sensors might be located in one fixed location with a stable power supply (environmental sensors) or might be attached to a patient's body with a battery power supply (wireless medical sensors). The mobile phones are used to aggregate the sensed health data and send it to the personal computers for further storage and analysis. Moreover, the mobile phones are hosting the rule-oriented applications, which are used to control the collection of sensed health data. Finally, the personal computer receives the environmental sensor data along with the data aggregated from the medical sensors. The personal computer utilizes its Internet connection for secure back-up and off-site data storage. Regarding the PAM-A part, it consists of a set of customized applications written in java and prolog to manage inter-device network connections, control the monitoring settings, store and transfer the sensed health data offsite for further analysis and long-term storage. The PAM system is the first research attempt to extract activity signatures from patients with bipolar disorder. The authors in their article mainly focused on reliability and acceptability issues in mental health monitoring using wearable and environmental sensors networks. However, they did not address patients' privacy and security issues, which are indispensable requirements for such healthcare applications. In [30], the SATIRE system has been proposed. SATIRE is a wearable personal health monitoring service transparently embedded in patient garments. SATIRE allows the patients to archive a private searchable record of their normal daily activities. This personal archive can later be searched to answer queries regarding present and past user behavior patterns and locations. When the user who uses a SATIRE moves into proximity of an access mote, the logged data stored in the SATIRE system is transmitted to the private personal archive for this individual user. This data can later be used to reconstruct an activity map of all the activities performed in the past. The authors of this work have properly discussed security and privacy issues in detail. However, they did not consider the implementation of any real solution to preserve security and privacy of the personally collected data. Another architecture was proposed in [41] called SNAP (Sensor Network for Assessment of Patients). SNAP was mainly designed to address security challenges in wireless healthcare monitoring systems. In spite of that, there are two problems associated with SNAP architecture: firstly, the data is collected from wireless medical sensors in a plain-text form, hence, it could be modified or interrupted by

attackers, and secondly, SNAP does not verify the identity of the users who are forwarding their data to the system. Finally, in [59] the IBE-Lite scheme (lightweight identity-based cryptography) was proposed for a patient-doctor environment. Different protocols based on the IBE-Lite solution were present in their work, with the aim to balance security and privacy with accessibility. The IBE-Lite depends on the isomorphism between the ECC group and the integer group where public and private keys are in, respectively. Hence, if the new public key is a combination of the previously used public keys, then the new private key associated with this new public key will also be a combination of the previously used private keys. On the sensor node, a pool of public keys is generated and saved. Additionally, the key generator is responsible for storing a pool of private keys that have been used to generate these public keys. A cryptographic hash function running on the sensor node utilizes a pre-calculated ID string to generate a bit string of length n. The value of n equals to the number of public keys in the pool. Moreover, the value and position of the bits in this bit string determines which public keys have been used in the addition. However, several security and privacy issues have been identified in IBE- [33], such as, the exposure of a master key, lack of data authentication between sensor to base station/user data, partial heath data decryption problem after rekeying, failure to detect node replication attacks, and lack of adequate privacy preserving technique.

C. PRIVACY-ENHANCED RECOMMENDER SYSTEMS

There are many solutions in the literature that were proposed to achieve privacy in recommender systems. The work in [6] was the first proposal to attain this; it considers a scenario in which a centralized recommender system generates recommendations using the collaborative filtering approach. End-users remove some selected parts from their profiles before sending them to the recommender. The recommender is able to attain recommendations because it was able to predict to some extent the missing parts. Attackers cannot learn the original ratings from the protected ones, but end-users can decide if their original ratings are included in the model using zero knowledge protocols. In this way, there is no external entity that has access to the private profile of a user. In [7] a privacy preserving approach is proposed based on peer to peer techniques using users' communities, where the community will have an aggregate user profile representing the group as a whole but not individual users. Personal information will be encrypted and the communication will be between individual users but not servers. Thus, the recommendations will be generated at the client side. In [28] a theoretical framework is proposed to preserve the privacy of customers and the commercial interests of merchants. Their system is a hybrid recommender system that uses secure two party protocols and public key infrastructure to achieve the desired goals. In [54] and [55] another method is suggested for privacy preserving on centralized recommender systems by adding uncertainty to the data using a randomized perturbation technique while attempting to make sure that necessary statistical aggregates such as the mean don't get disturbed much. Hence, the server has no knowledge about the true values of the individual rating profiles for each user. They demonstrate that this method does not essentially decrease the obtained accuracy of the results. But recent research work in [34] and [37] pointed out that these techniques do not provide the levels of privacy as was previously thought. In [37] it is pointed out that arbitrary randomization is not safe because it is easy to breach the privacy protection it offers. They proposed random matrix based spectral filtering techniques to recover the original data from perturbed data. Their experiments revealed that in many cases random perturbation techniques preserve very little privacy. Similar limitations were detailed in [34] Storing the users' rating profiles on their own side and running the recommender system in a distributed manner without relying on any server is another approach proposed in [47], where authors proposed transmitting only similarity measures over the network and to keep users' rating profiles secret on their side to preserve privacy. Although this method eliminates the main source of threat against the user's privacy, it requires higher cooperation among users to generate useful recommendations.

III. THE OECD PRIVACY PRINCIPLES

The organization for economic co-operation and development (OECD) [11] formulated sets of principles for fair information practice that can be considered as the primary components for the protection of privacy and personal data. A number of countries have adopted these principles as a statutory law, in whole or in part in order to govern the data that customers outsource for cloud based services operating at remote sites. These principles can be described as follows:

- **Collection limitation**: Data collection and usage for a remote service should be limited only to data that is required to offer an appropriate service.
- **Data quality:** Data should only be used for the relevant purposes for which it is collected.
- **Purpose specification:** Remote services should specify up front how they are going to use the data and end-users should be notified in advance when a system will use it for any other purposes.
- **Use limitation:** Data should not be used for purposes other than those disclosed under the purpose specification principle without end-user consent.
- **Security safeguards:** Data should be protected with reasonable security safeguards (encryption, secure transmission channels, etc.).
- **Openness:** The end-user should be notified upfront when the data collection and usage practices started.
- **Individual participation:** End-users should have the right to insert, update, and erase data in their profiles stored on remote services.
- **Accountability:** Remote services are responsible for complying with the principles mentioned above.

A. THE IMPLICATIONS OF OECD PRINCIPLES IN DESIGNING EFFICIENT PRIVACY ENHANCING FRAMEWORKS

In this section, the research work in [50] is presented that classifies the implications of the OECD principles with respect to designing efficient privacy frameworks. Their suggestions will be used in order to state which of these principles should be considered as a norm in designing the holistic privacy framework:

- **Collection Limitation**: This principle is too general to be applied in our holistic privacy framework. The boundaries and content of what is considered private differ among cultures and individuals, but share basic common themes. Inspired from the work in [32], we summarized the challenges for this principle as boundaries and for each boundary, we describe a tension which the boundary has to face. These boundaries are as follows:
  - The Disclosure boundary (privacy and publicity) - this can be defined as a tension between data points that are private and public. The end-user has to decide what to keep private and what to make public.
  - The Identity boundary (self and other) - the end-users need to decide which identity to disclose to whom. This is a tension between different identities a user might have.
  - Temporal boundaries (Past, Present, and Future) – this is a tension on the time aspect. What is not private in the past might become so in the future and vice versa, and when the information is being persistent, many of the actions done in the past cannot be undone.

Our contributions in this research address the first two boundaries. As a result, we decided to leave this task for the end-users to determine a sensible realization for the notion of very sensitive data. Moreover, the end-users are responsible for making their data public or private by employing privacy preferences languages to specify rules or levels for releasing their data such that a conscious automatic choice can be made about which group gets to see what. Also, catering to the second boundary, it gives the end-users the choice to join a recommendation request, using an anonymous network or leaving the recommendation process, where the end-users can join recommendation requests only with a trusted cloud based service providers. The temporal boundary was partially addressed in this paper, where the fog node has the choice to share outdated measurements and results with external fog nodes, in order to compute the trust level with the cloud based service provider. However, we plan to fully address the temporal boundary in future research.

- **Data Quality Principle**: Most of the privacy enhancing frameworks assume that the data is in an appropriate form to be processed by the current concealment techniques. However, data cleaning methods could be utilized locally to handle imprecision and errors in data before any concealment process. We mitigated this principle in the holistic privacy framework by selecting two common types of erroneousness in the users' health data, which are incomplete users' health profiles and outliers. We then proposed a two-stage concealment process, which take into consideration pre-processing the incomplete user health profiles and handling outliers on these profiles. Other types of deviations should be investigated in future research. Meanwhile, we left the task of handling other erroneousness to the end-user, in order to maintain an accurate health profile for the recommendation process and to facilitate a straightforward concealment process.
- **Purpose Specification Principle:** This principle is relevant for our holistic privacy framework. End-users should be well informed at the outset prior to the collection and the processing of their health information.
- **Use Limitation Principle**: This principle is relevant for our holistic privacy framework and related to the previous principle. The collected health information from end-users must be used only for the purpose that was disclosed at the time of collecting this information.
- **Security Safeguards Principle**: This principle is relevant for our holistic privacy framework but is related in general to data security. We have mitigated this principle by proposing a middleware that runs at the end-user's side and assures the anonymity and privacy of each individual user. Within this approach, the middleware assigns two profiles for each user, one is a local profile in a plain form that is stored locally on the user's fog node and the other is a public profile that represents the local profile in a concealed form that is stored remotely at the cloud based service provider. This ensures that the personal user's health data is protected from malicious/unauthorized users.
- **Openness Principle**: This principle is relevant for our holistic privacy framework. End-users should know the data that have been gathered about them and processed. However, most of the cloud-based services do not disclose the logic behind the scene due to intellectual property issues. Our holistic privacy framework enables each end-user to decide either to join or not a certain type of recommendation process and also to control what data to be released for this recommendation process.
- **Individual Participation Principle**: This principle is relevant for our holistic privacy framework. End-users are aware that the generated referrals are related to their released data. End-users can challenge the value of the generated referrals and decide whether to participate or not. Therefore, there should be a certain mechanism to carefully outline the weight of this principle to the end-users.
- **Accountability Principle**: This principle is irrelevant for our holistic privacy framework. Cloud based services should inform end-users about the policies related to the usage of the generated recommendation model including the consequences of abusing the collected data. This

principle is too general in scope or area to be utilized for privacy-enhancing frameworks.

Based on the outline we declared above, we categorized the OECD principles into two groups according to their influence on the context of designing the proposed holistic privacy framework:

- **Relevant Group**: Consists of those principles that should be considered as design principles in the holistic privacy framework, such as data quality, purpose specification, use limitation, security safeguard, openness, and individual participation.
- **Irrelevant Group**: Involves some principles that are too general or irrelevant to the proposed holistic privacy framework. Some of those principles depend on the applications where the privacy-enhancing frameworks are needed, and their effects should be understood and carefully evaluated depending on these applications.

The principles categorized in the first group are relevant in the context of our holistic privacy approach and are fundamental for further research, development, and deployment of privacy enhancing frameworks in general.

B. UTILIZING CLUSTERING ANALYSIS IN BUILDING PETs

In this research work, clustering algorithms were used as the basic building block for the pattern preservation task within the proposed two-stage concealment process. The collected vital measurements is pre-processed with the clustering algorithm introduced in [20] in order to extract essential patterns needed for the recommendation techniques and then after the local concealment process is adjusted to keep these patterns analogous to the ones in the original data. Utilizing cluster algorithms enables the off-the-shelf recommendation techniques to extract these useful patterns directly from the concealed health data without the need to modify these techniques to work the concealed data.

Data Clustering is an ideal pattern preserving method since it can extract regularities from the health data. These regularities can be realized in the form of putting sets of similar data points into clusters, where each cluster has a representative or exemplar to it. An ideal clustering algorithm seeks to attain two objectives: (1) minimizes the inter-cluster similarity and (2) maximizes the intra-cluster similarity. Choosing the *LLA* clustering algorithm introduced in [25] for this task has been done for three reasons:

1. *LLA* algorithm has a predicative capability, where similarities between a new data point and existing clusters can be utilized to identify the type of the data point based on which cluster it belongs to.
2. *LLA* algorithm can reduce computation costs, since the whole cluster's data points can be represented by an exemplar, which is enough to describe the whole cluster structure.
3. *LLA* algorithm extracts groups of data points that deserve attention while cleaning the data from outliers and errors.

IV. HOLISTIC PRIVACY FRAMEWORK USING EMCP FOR CLOUD-BASED HEALTHCARE SERVICES

The proposed solution is deployed over three primitive usage layers. The first is the data collection layer: consists of various IoHT devices and a mobile application that capture vital sign measurements from the user's body/home during various physical activities. Additionally, the mobile application collects other externally available data related to these performed activities (e.g. location and time). The collected data from this layer is used for recommendation purposes. The second is the intermediate layer: consists of a set of fog nodes where each node hosts a holistic privacy middleware, which will execute the second stage of the two-stage concealment process within a distributed data collection protocol that utilizes the hierarchical nature of IoHT devices. The third is the service layer: consists of various healthcare web services hosted on cloud platforms that allow greater voluminous of data, inclusive analysis and satisfying reliability of the proposed solution. The healthcare information system is managing one or more of these services, where the healthcare recommender services are used to monitor the user's health condition and offer recommendations on how to improve it in accordance with the caregiver's perspectives. Additionally, this layer facilitates different collaborations between various service providers.

To mitigate privacy risks in cloud based healthcare service with Internet of healthcare things, strong cryptographic algorithms are needed to be utilized. Traditional cryptographic solutions are not precisely appropriate for such services due to the computational complexity of cryptographic protocols together with the limited energy budget of such devices, which make privacy provisioning in such devices a problematic mission. Additionally, due to the constrained resources of IoHT devices, it is unattainable to employ traditional cryptography solutions in these services. Hence, there is a need to develop lightweight cryptographic primitives that can be executed on IoHT devices with low computational power as discussed in [38]. As an alternative solution, the fog nodes residing at the user's side have become relatively powerful due to a vast advance in their processing, networking and storage capabilities, until recently, the tasks designated to these devices were initially limited to trivial operations such as data accumulation and forwarding. With the advance of fog computing paradigm, these devices have become more divergent and computationally intensive. The benefits of utilizing Fog Computing for IoT applications have been discussed in [5]. According to our approach, privacy assurance will be moved from IoHT devices to the personal gateways (called fog nodes). The end-users will need to configure the desired privacy preferences only once (what purposes their health data will be released for, what data from their health profiles gets collected at each concealment level, etc.), and the fog nodes will have the burden to apply them automatically to any health data released for the cloud based healthcare services, regardless of the physical IoHT device in use. This approach has various advantages: first, establishing a user-centered privacy by transforming the execution of intensive privacy

preserving processes from an IoHT device to the fog node; secondly, obtaining a personalized privacy assurance independent from the IoHT devices while reducing their power consumption, which occurs as a consequence of unburdening the IoHT devices from performing these complex processes; thirdly, simplifies adding management and re-configuration of privacy preferences for any released health data and all the IoHT devices; and finally, empowering resource-constrained IoHT devices with the same level of privacy assurance of more secure systems.

EMCP has been proposed to satisfy the privacy requirements of privacy aware users. Our earlier work presents a holistic privacy framework that implements a two-stage concealment process, where each stage utilized a set of clustering analysis based stochastic techniques that introduce carefully-chosen artificial noise in the data so as to retain its statistical content while concealing all the private information. In that way, privacy is achieved for each user. The following terms will be used during the remaining parts of this paper:

1. User's health profile refers to the personal information, measurements for different vital signs and personal life-style. The personal information corresponds to any personally identifiable information such as name, gender, zip code, age, address, etc., while measurements correspond to the parameters for different vital signs such as blood pressure, heart rate, electrocardiogram, blood glucose, and respiratory rate, etc. Finally, the personal life-style refers to the diet particulars and physical daily activities.
2. An individual user is a registered patient for the cloud based healthcare service.
3. The third party entity that offers the recommendations/ referrals was referred to as the cloud based healthcare service.
4. The end-users and the cloud based healthcare service can be called clients for the cloud based healthcare service, where each cloud service provider can serve multiple cloud based healthcare services with their end-users using a service-oriented infrastructure.
5. Fog nodes refers to the personal gateways at the end-user's side that act as intermediate nodes between IoHT devices and cloud-based healthcare services

Each individual user who utilizes the recommendation of the cloud based healthcare service is hosting and running the *EMCP* middleware within his/her fog node. *EMCP* is the main architectural element of our holistic privacy framework, since it is responsible for executing the topological formation protocol for data collection and providing controlled access over what personal information is to be released with a different degree of granularities to external cloud based healthcare services. The cloud based healthcare service uses *EMCP* to manage and store the users' health profiles. The main characteristics of the *EMCP* middleware architecture are:

- Form the cloud based healthcare service's point of view, *EMCP* is a decentralized system for the storage and management of users' health profiles.
- Form the user's point of view, *EMCP* is a centralized system where all his/her health profile is stored locally on his/her personal gateway.

As we mentioned earlier, the proposed holistic privacy framework was implemented using the *EMCP* middleware, which combines all of these techniques to make it possible to efficiently take advantage of this work. The proposed middleware enables IoHT devices to be organized in a distributed topology during data collection to achieve privacy for the recorded data of each IoHT device with relatively low accuracy loss. IoHT devices are organized into a VPN coalition and each coalition contains a reliable node to act as a trusted aggregator that is entitled fog node, which will be responsible for anonymously sending the aggregated health data of IoHT devices to the cloud based healthcare service. Additionally after receiving the referrals list, the fog node will be responsible for distributing this list back to its end-user. Electing a trusted cloud based healthcare service is based on negotiations between fog nodes and a trusted third party; this trusted third party is responsible for generating certificates for all end-users, and managing these certificates. In addition, it is responsible for making assessments on those fog nodes according to other fog nodes' reports and periodically updates the reputation of those fog nodes.

Utilizing topological formation within our holistic privacy framework attains privacy for users with relatively low accuracy loss. It also prevents the cloud based healthcare service from creating a centralized database with a raw health data for each user. Additionally, it permits a decentralized execution of a two-stage concealment process on the users' health data. The topological execution in the proposed middleware satisfies the requirements of high scalability and reduces the risk of privacy breaches. The formation of this VPN coalition is done through a specific virtual topology in order to create an aggregated profile (group profile). This topology might be simple like a ring topology or complex like a hierarchical topology (see Figure 2). This ordering enables IoHT devices to attain privacy by collaboration between them. The VPN coalition also attains a secure transmission channel to protect all the traffic between the IoHT devices and the fog node. Health data is shared between various IoHT devices within the same coalition after it is locally concealed. The fog node will be responsible for executing a global concealment process on the aggregated profile (group profile) before delivering it to the cloud based healthcare service. In this approach, the notion of privacy surrounding the disclosure of the users' health profiles and the protection of trust computation between different fog nodes are together the backbone of this framework. A trust based concealment mechanism was applied at the fog node side such that trust computation is done locally over the concealed user's data. Utilizing trust heuristic as an input for the global concealment process has been of great importance in mitigating some of the malicious insider attacks described in [26] and maintains an optimized utility for the concealed health data [21].

The proposed holistic privacy framework attains anonymity and privacy. The anonymity is achieved either by utilizing pseudonyms, by running the communication through an anonymity network like Tor or by a topological formation that divides IoHT devices into a VPN coalition. Each coalition is to be treated as one entity by aggregating its devices' local data into one aggregated health profile at the fog node. This fog-node will then handle the interaction with the cloud based healthcare service. If health profiles cannot be identified or traced back, the framework protects the privacy of the end-users even if their profiles are sent in clear. However, the privacy of the locally recorded data of IoHT devices is achieved as each device within the coalition performs at least one stage in the two-stage concealment process. The IoHT devices perform a local concealment process before releasing their data to external entities. Local concealment is a pre-processing step that is based on clustering the sensitive vital sign measurements. It then applies a concealment algorithm on the extracted partitions, so as to take into consideration the correlations and the range of different data points within sensitive measurements. The fog nodes of every coalition aggregate the health data received from traditional members to form a group health profile. The fog node then executes a global concealment process on the group profile before releasing it to the cloud based healthcare service. This sort of two-stage concealment process enforces anonymity for participants' identities and privacy for their data. Data privacy in the two-stage concealment process was achieved by using a set of newly proposed stochastic techniques for concealing users' health data within their released profiles for recommendation requests. This is not a straightforward task since the two-stage concealment process should make sure that the concealed data is still useful for the recommendation phase, which usually requires that changes on the users' health data be as limited as possible. However, users' health profiles are complicated and are an interrelated structure. Making small changes in it could cause an unexpected influence on the overall recommendation process. The proposed techniques combine approaches from the clustering analysis that consider knowledge representation in the domain of data privacy in order to preserve the aggregates in the dataset to maximize the usability of this data, with a view to accurately perform the desired recommendation process. The validity of the framework is demonstrated by the implementation and evaluation of the proposed solution within a set of important innovative applications. A general overview on the proposed framework is shown in Figure 1.

A. DESIGN OF EMCP MIDDLEWARE

The fog node is a network edge device that can be depicted as an enhanced access point such as a switch or router operating at the indoor environment of the end-user. The fog node is equipped with networking and computing capabilities to facilitate the execution of dynamic run-time self-reconfiguration mechanism that automatically adjusts the concealment level of released data based on data collection and usage practices of the cloud based healthcare service (e.g.: P3P policies which are answering questions concerning the purpose of collection, the recipients of these profiles, and the retention policy), and user's privacy preferences. The fog node can be considered as the most critical component in the proposed framework as it is responsible for ensuring privacy and anonymity for the end-user. Moreover, this component must be trusted for delegation, as the end-user must be assured that the fog node will implement the global concealing process (the second stage of the two-stage concealment process) on his/her released health data and will not trigger any malicious activities. Nevertheless, if the end-user does not trust the fog node, he/she is not forced to give up the execution of the first-stage of the two-stage concealment process on any released health data. In other words, the end-user can always execute the local concealing process on the released health data before forwarding it to fog node. However, if the end-user prefers a double line of privacy preservation to perform privacy guardianship in depth, the fog node can be used as a complement to standard privacy protection measures. Finally, secure transmission channels protect all the traffic between the IoHT devices and the fog node, such that the user's released data cannot be eavesdropped or altered by an external attacker before the fog node implements global concealing process

Figure 3 illustrates the proposed enhanced middleware for collaborative privacy (*EMCP)* components running inside the user's fog node. *EMCP* consists of different cooperative agents. A learning agent explicitly captures vital sign measurements from the user's body/home during various physical activities to build three databases, the first one is the vital sign measurements database, and the second one is the metadata database that contains the feature vector for data related to the measurement of the vital. Finally, the last one is the realized activities database. The manager agent is responsible for coordinating between requests and different agents in *EMCP*, such that, the manager agent receives the recommendation requests and the P3P policies from the cloud based healthcare services. It then forwards them to the involved agents. It also ensures that the group profile contains the health data required for this particular recommendation process. The local concealment agent implements the local concealment process to achieve user privacy while sharing his/her health data with fog nodes or the cloud based healthcare service (CHS). The trust agent calculates the approximated interpersonal trust between the fog node and the cloud based healthcare service. The trust computation is done in a decentralized fashion using the entropy definition proposed in [39]. The global concealment agent is only exists in the fog node. It executes the global concealment process on the aggregated health profile. The two-stage concealment process acts as wrappers to conceal health data before they are shared with any external cloud based healthcare service.

Since the database is dynamic in nature, the local concealment agent periodically conceals the updated vital measurements, and then the synchronize agent forwards them to the

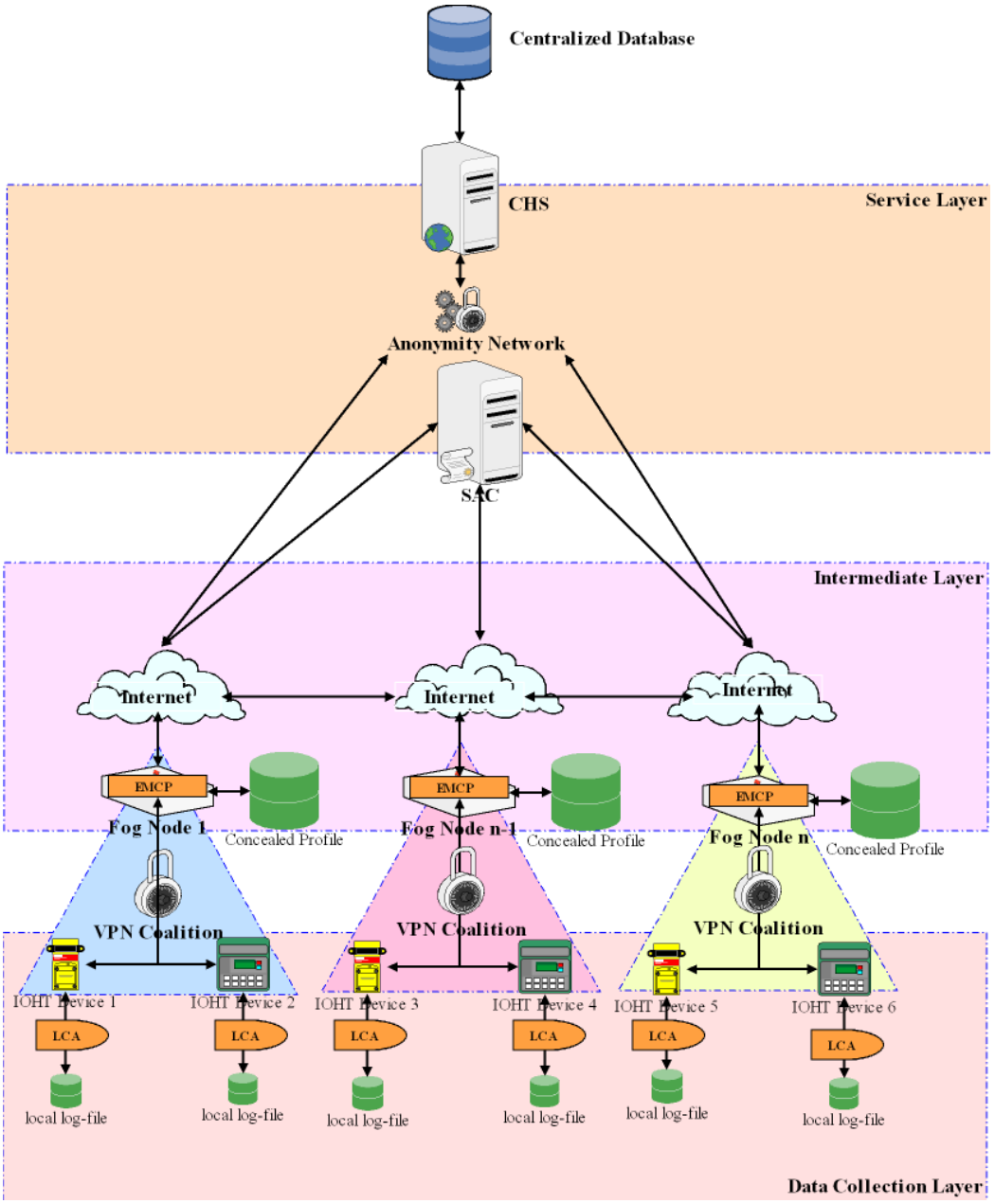

FIGURE 1. EMCP Middleware in Third-Party Cloud based Healthcare Service.

cloud based healthcare service (CHS) or the fog node upon owner permission. Thus, recommendations can be made on the most recent health data. The synchronize agent is also responsible for calculating and storing parameterized paths in the anonymous network that attains high throughput, which in turn can be used in submitting the group profile anonymously. These parameterized paths are stored in a database called ''nodes store''. The policy agent is the entity in *EMCP* that has the ability to encode privacy preferences and privacy policies as XML statements. It also has the responsibility to encode data collection and data usage practices as P3P policies via XML statements which are answering questions concerning the purpose of collection, the recipients of these health profiles, and the retention policy. In order to do so, the policy agent needs to acquire the user's privacy preferences and express them using APPEL as a set of preferences rules which are then decoded into a set of elements that are stored in a database called ''privacy preferences'' in the form of tables called ''privacy meta-data''. These rules contain both privacy policy and an action to be taken for such privacy policy, in this way, it will enable the preference checker to make self-acting decisions on data points that are encountered during the data collection process regarding different P3P policies (e.g.: privacy preferences could include: certain

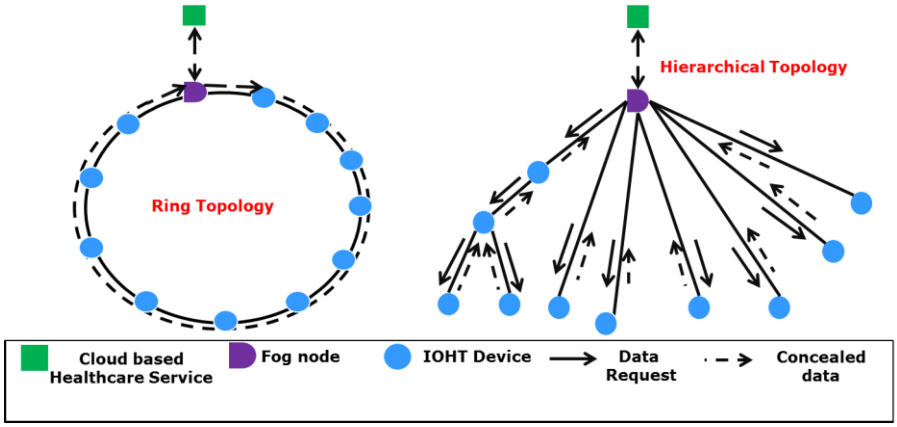

FIGURE 2. Topology for creating aggregated health profile in IoHT coalition.

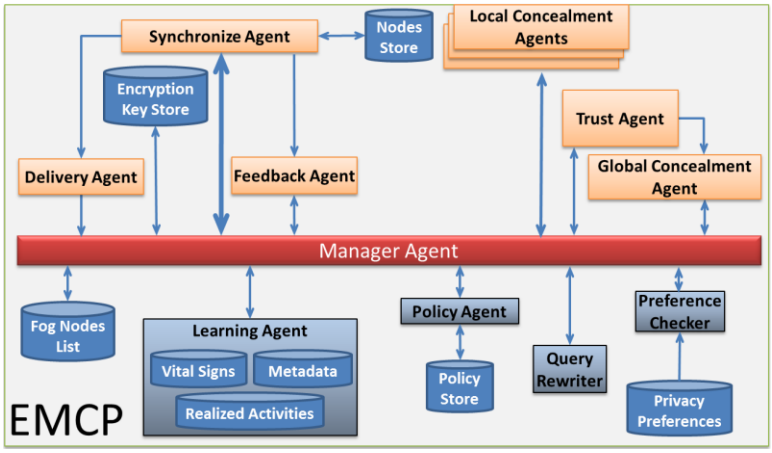

FIGURE 3. Inside *EMCP* Components.

categories of data points should be excluded from health data before submission, refresh rate of vital sign parameters, usage of data points that have been captured during sensitive activities/locations, generalize certain data points in user's health profile according to defined taxonomy, using synonyms for certain terms or names in user's health profile, suppressing certain data points from the extracted data and insert dummy data points that have the same feature vector like the suppressed ones as described in [20], limiting the potentially output patterns from extracted health data etc. in order to prevent the disclosure of sensitive data points in user's health profile). Query Rewriter rewrites the received request constrained by the privacy preferences for its host. The feedback agent is responsible for anonymously submitting the user's feedback about the referrals list and recommendation process to the cloud based healthcare service. The feedback agent also reports scores about the different fog nodes and the cloud based healthcare service to the security authority center. Finally, the delivery agent is the entity which is responsible for communicating with the external third-party providers in order to provide or fetch meta-data related to the personal life-style to be performed or already performed.

B. THE INTERACTION SEQUENCE BETWEEN PARTIES WITHIN HOLISTIC PRIVACY FRAMEWORK

Figure 4 shows the participants' interactions with fog nodes and a cloud based healthcare service. A general overview of the recommendation process in the proposed framework operates as follows:

1. The manager agent within the fog node broadcasts a message to various IoHT devices placed on the surrounding environment of the patient requesting recommendations for a personalized life-style that could potentially improve the health condition of the patient. This ''fog node'' which will act as a communication gateway between the cloud based healthcare service and the IoHT devices.
2. Thereafter, the manager agent broadcasts a message to other manager agents hosted on the external fog nodes to demand the computation of a trust level with a specific cloud based healthcare service provider.

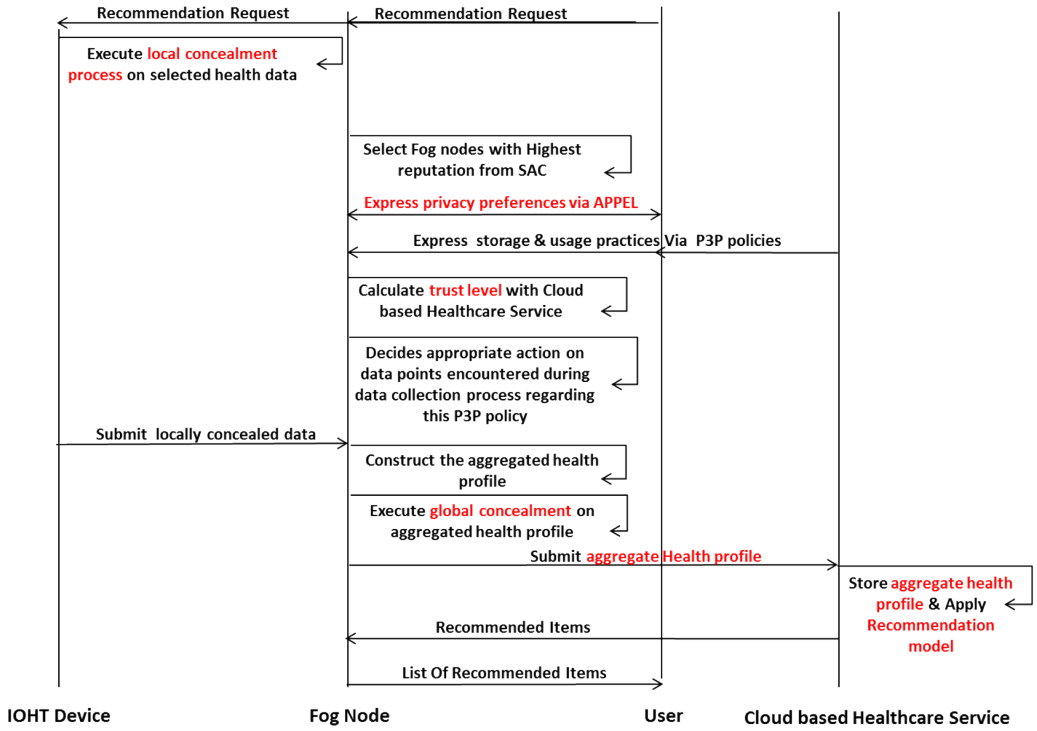

FIGURE 4. Interaction sequence diagram for holistic privacy framework.

Additionally, it selects a set of its outdated measurements and recommendations' results to be shared later with external fog nodes, in order to compute the trust level. The local concealment agent is employed to execute the local concealment process on any released data. Finally, the manager agent dispatches this data to the individual fog nodes that have decided to participate in the computation of the trust level.

3. Upon receiving replies from different fog nodes, the manager agent negotiates with the security authority center (SAC) to select the fog nodes with the highest reputation to act as members in the trust computation. The reputation score for each fog node is calculated as a resultant of the trust ratings assigned to it. The reputation score of each fog node serves as a weight for any evaluation that this fog node assigns to each contribution in the trust computation. SAC is a trusted third party responsible for making an assessment on those fog nodes according to the fog nodes' reports. Moreover, SAC records the calculated reputation scores for various fog nodes and trust levels for different cloud based healthcare service providers.
4. The manager agent negotiates with the cloud based healthcare service to express its privacy policies for the data collection and usage process via P3P policies.
5. When the manager agent receives the P3P policy from the cloud based healthcare service, it forwards the received P3P policy and the patient's request to the preference checker and the query rewriter respectively. The preference checker ensures that the extracted health measurements do not violate the privacy of its host which was previously declared by the use of APPEL preferences. The query rewriter rewrites the received request based on the feedback of the preference checker. The modified request is directed to the learning agent to start the collection of health measurements that could satisfy the modified query and forwards it to the local concealment agent. Finally, the policy agent stores in its internal store the original and modified requests along with the estimated trust level and the received P3P policy. This will empower the policy agent to execute multiple auditing insights to define the conflicting requests, which could be used to extract the sensitive health measurements.
6. The trust agent calculates the approximated trust level with the designated cloud based healthcare service provider based on the replies given by different fog nodes. The trust computation is done in a decentralized fashion using the entropy definition proposed in [39] at each node side. The trust agent sends the calculated trust value to the requester fog node. The estimated trust value is also forwarded to both the participating fog nodes and the SAC. Then after, the locally concealed health data from each IoHT device is sent to the fog node of their pre-specified health IOT network.

7. Upon receiving the locally concealed health data from each IoHT device, the fog node builds a group profile (aggregated profile) in order to perform the global concealment process on this profile. The fog node can seamlessly interact with the cloud based healthcare service (CHS) by posing as an end-user and has a group profile as its own profile.
8. The cloud based healthcare service (CHS) runs the recommendation algorithm on the received aggregated profile then forwards the generated referrals list along with the predicted personalized life-style that could potentially improve the health condition of the patient to the requester fog node. The fog node publishes the final list to the mobile phone of its end-user. Finally, the fog nodes that contributed in this process report scores about the requester fog node and the cloud based healthcare service provider to SAC, which helps to determine the reputation of each entity involved in the referrals generation.

In order to demonstrate the applicability of this framework, this research presented a case study focusing on cloud based healthcare recommender service. This scenario is motivated by protecting the privacy of users' health profiles while utilizing the cloud based healthcare recommender service and its implications. A typical end-user health profile with this service contains the user's vital measurements along with his/her personal data and personal life-style. The reason for selecting this case study was due to the fact that it represents the more pressing issue on privacy research and we hoped to enable the deployment of privacy-aware healthcare recommender service using the holistic privacy approach. Obviously, other practical scenarios still exist for the proposed framework. However, in this research we are unable to address all of them.

C. THE ROLE OF OECD PRINCIPLES IN THE HOLISTIC PRIVACY FRAMEWORK

OECD principles rely on the commitment of cloud based healthcare services on revealing their data handling practices accurately. However, the current perspective illustrates that it is likely for them to not follow these principles in full. We have utilized the OECD principles as design guidelines for our holistic privacy framework. The role of OECD principles in designing the proposed holistic framework will be outlined in this subsection, where we have termed the proposed framework in this research as an enhanced middleware for the collaborative privacy framework, which is abbreviated as *EMCP*. The proposed framework reduces privacy risks and facilitates privacy commitment. The proposed solution realizes privacy aware healthcare recommender service while complying with the current business model of third-party cloud based service provider.

The privacy obtained through the proposed holistic privacy approach is as follows:

- **Collection Method:** The proposed solution attains an explicit data collection mode. End-users are aware that a data collection within a recommendation process is happening and they can make a wise decision about whether or not to provide their health data in this recommendation process. Privacy policies such as P3P are utilized to explain to the users how their health data is going to be used. End-users utilize privacy preferences in order to control what health data from their profiles gets collected at each concealment level. However, formalizing such privacy preferences is not an easy task. End-users need to realize various privacy issues. End-users also need to deduce future recommendation requests that might raise privacy concerns for their collected health data. The end-user can employ an anonymous network while sending this locally concealed health data to either the fog node or the cloud based healthcare service.
- **Duration:** The proposed solution attains a session-based collection that allows for a simpler service that does not need the storage and retrieval of users' health profiles. The data related to the recommendation process is collected from users' health profiles in a concealed form. This concealed data is only feasible for the recommendation purposes. This reduces privacy concerns since minimal data to be collected and also ensures compliance with privacy laws. The concealed data is stored at the cloud based service in order to enhance the recommendation model and future requests. Moreover, this health data by default is protected by the retention policies of data protection laws.
- **Initiation:** The proposed solution attains a user-based recommendation. End-users are the entities that initiate the recommendation process. Each user in the network is aware that a healthcare recommendation service is running and he/she can decide whether or not to join it. The incentive for participants when joining a recommendation request includes receiving daily referrals regarding personalized life-styles that could potentially improve their health conditions in a private manner.
- **Anonymity:** The proposed solution attains anonymity, which aids in preventing frauds and Sybil attacks. The anonymity is realized within the holistic privacy framework using the following procedures:
  a. Dividing IoHT devices into a VPN coalition with their fog node: each VPN coalition to be treated as one entity by aggregating its IoHT devices' concealed health data in one aggregated profile at the fog node. This fog node will then handle the interaction with the cloud based healthcare service. IoHT devices within the VPN coalition interact with each other in a P2P fashion and form a virtual topology to aggregate their data.
  b. Using anonymous channels like Tor: each IoHT device might benefit from these anonymous channels while contacting the cloud based healthcare service or other cloud based services.
  c. Utilizing pseudonym for IoHT device: each IoHT device within the system is identified by a

pseudonym in order to reduce the probability of linking its collected health data with a real user's identity.

- **Local Profiles:** Our solution attains a local storage to users' health profiles. Users' health profiles are stored locally on their own devices (Personal gateway, Smart phone, Laptop...) in an encrypted form. This can guarantee that these profiles are attainable only to their owners. Furthermore, in doing so these profiles will be inaccessible to viruses or malwares that may affect the user's machine to gather his/her personal data. As a result, each user will possess two profiles; one is a local profile in a plain form that is stored locally in his/her fog node and is updated frequently. The other is a public profile in a concealed form that is stored remotely at the cloud based service provider and is updated periodically within each recommendation process where this user participated.
- **Clustering Techniques for Data Privacy:** The proposed concealment process relies on a set of cluster analysis based stochastic techniques. These techniques are to be carried out in two consecutive steps within a two-stage concealment process. The proposed concealment process destroys the structure of data in the user's health profile but, at the same time, maintains some properties in it, which is required in the planned recommendation algorithm. The implementation of such applications also confirmed that it is feasible to make use of, and at the same time, to protect the personal sensitive health data of individuals, and do so in an accurate way.

D. PRIVACY MANAGEMENT APPROACH USING THE HOLISTIC PRIVACY FRAMEWORK

The core hypothesis of our holistic privacy approach is that personal health profiles are stored locally at the users' side of their fog node. Two related questions may arise in the mind; how can we ensure that the end-users will participate in such a solution and what are the incentives for cloud based healthcare service providers to adopt this solution. We are aware that our holistic privacy approach represents an extreme case for privacy management and enforcement. However, our holistic privacy approach serves as a proof of the concept that fair information practices can be deployed, implemented, and enforced in a more efficient way when it is being utilized in service oriented architecture like cloud based healthcare service rather than adopting the current approaches. In particular, within our framework, personal health profiles can be handled in a privacy respecting manner that is complying with the OECD privacy principles. The recent emergence and spread of user centric applications, makes it feasible to fully embrace a framework such as our holistic privacy framework. Nevertheless, the growing privacy invasions within the current approaches have contributed in facilitating the misuse of personal information, which is considered one of the most common problems when taking advantage of digital services.

Due to the previously mentioned reasons, we believe there are some shortfalls in separating technological and legislative solutions, which open the doors for us to further investigate into a new holistic solution that combines both technological and legislative efforts together in a unified framework. The new solution meets the crucial requirements of OECD privacy principles and amends the user's control over his/her personal health information that is released to external parties. In this regard, we developed and evaluated our holistic privacy framework in different scenarios. Obviously, that much work has to be done in order to demonstrate the possibility of applying a solution like *EMCP* in the various business models while complying with varied privacy guidelines. However, our previous research work confirms that our holistic privacy framework is feasible for different applied contexts.

V. MOTIVATIONS AND RESTRICTIONS OF THE VARIOUS PROSPECTIVE PARTIES IN OUR HOLISTIC PRIVACY APPROACH

There are numerous motivations and restrictions for the various parties involved within our holistic privacy framework, this does not make it only valuable to the user but also to cloud based healthcare service providers. Our proposed middleware which is employed in the implementation of this framework permits the end-users to control the privacy of their released health data while interacting with cloud based healthcare services. This kind of approach is quite flexible and can easily be adopted in a conventional business model of the current cloud oriented based services, like cloud based healthcare recommender service, because it is executed at the user side and it takes advantage of the topological structure that is offered by the IOT network without the need for significant modifications at the healthcare service provider side. Healthcare service providers can also attain many benefits from adopting the proposed framework, such as, promoting a privacy friendly environment for their offered healthcare services, simplifying the data management process at their side and finally reducing their liability to secure their clients' personal health information.

A. MOTIVATIONS AND RESTRICTIONS FOR END-USERS

1) END-USERS' MOTIVATIONS

- Attaining ultimate control over their personal health information: The End-users can determine for each recommendation process, what purposes their health data will be released for, and what data from their health profiles gets collected at each concealment level. They are also aware of how long this data will be retained by the cloud-based healthcare service providers.
- Utilizing up-to-date health data for recommendations purposes: Storing the health data locally at the user side facilitates the creation of accurate health profiles and simplifies the update of these profiles with the most recent measurements for different vital signs. As a result, each time a recommendation process occurs,

the end-users will release an updated version from their current health profile instead of using an outdated health data stored at the cloud based healthcare service, which will allow the generation of accurate referrals that match their changing measurements and physical activities.

- Specifying their privacy preferences: End-users can express their privacy preferences using APPEL as a set of rules which are then decoded into a set of elements that are stored in a privacy preferences database. These rules will enable *EMCP* to make self-acting decisions on data elements that are encountered during the data collection process regarding different P3P policies.
- Reducing the impact of privacy breaches: In case the occurrence of privacy invasion happens at the cloud based healthcare service, the leaked users' health data will be worthless with a diminished informative value, because it is already concealed with a two-stage concealment process and cannot be linked directly to a specific user. The leaked users' health data is also concealed in a way to be only useful for recommendations purposes and it would be difficult to perform different kinds of analytical processes on such data.
- A third option for privacy aware users: Privacy aware users will no longer have to choose between two options, either releasing their whole health data to a cloud based healthcare service which they have to trust or not using the service at all. Our holistic privacy framework provides an alternative to the current models of practice.

2) END-USERS' RESTRICTIONS

- The end-users have to formalize their privacy preference, which is a critical task, as the end-users need to realize various privacy concerns. They also need to deduce future recommendation requests that might raise privacy concerns for their collected health data.
- The holistic privacy framework does not fully protect end-users from malicious Internet service providers. The malicious Internet service provider can uncover the user's anonymity during the release of his/her health data to a specific recommendation request. This problem has been mitigated by utilizing anonymity networks while sending the health data from fog nodes to cloud based healthcare services and employing reputation mechanisms in order to select proper relay nodes with a stable success rate within the anonymity network. Moreover, the user's health data is not in a raw form and its privacy is already protected with a two-stage concealment process before leaving the user's device.
- Within the proposed holistic privacy framework, the user's health profile is stored at his/her fog node in a raw form, which makes it vulnerable to a malware/spyware that might infect this machine. In order to mitigate this problem, the user's health profile is encrypted with a secret key encryption algorithm when the end-user is not using the system. Special considerations also need to be added to the operating system of the fog node in order to ensure strong safety and trustworthy guarantees in the middleware while running in the fog node's memory even with the presence of a malicious software (sandboxing, instruction detection.. etc.).

B. MOTIVATIONS AND RESTRICTIONS FOR CLOUD-BASED HEALTHCARE SERVICES

1) CLOUD-BASED HEALTHCARE SERVICES' MOTIVATIONS

- Providing accurate referrals: The referrals list is extracted from up-to-date health data, which is collected prior to the start of the recommendation process. This has a number of beneficial advantages on the offered service, such as, reducing the users' frustration, increasing the number of potential end-users for the service, and raising the revenue of the service providers.
- Using the current recommendation techniques: adopting the holistic privacy framework does not require the design of new recommendation techniques, the current off-the-shelf recommendation algorithms can be used directly on the concealed health data without the need to return it back into a raw form.
- Readiness to be used in the conventional business model of the current cloud oriented based services: Most of the existing service providers find difficulties in integrating privacy enhancing frameworks within their services, as the addition of privacy and cryptography components requires a significant change on their services' back-end infrastructure. The holistic privacy framework utilizes the fog nodes at the end-users side to act as an infrastructure for the implementation of our framework. The holistic privacy framework is quite flexible and can easily be adopted in the current business model of cloud-based healthcare services because it is executed at the user side and takes advantage of the personal gateways that already exist as intermediate fog nodes between IoHT devices and cloud-based healthcare services without the need for significant modifications at the service provider side.
- Simplifying the data management process at the cloud-based healthcare service provider side: Within the holistic privacy framework, the users' health profiles is stored on their side on their own fog nodes. However, in order to enable the cloud-based healthcare service providers to use the users' health data in more sophisticated business processes, a concealed version of users' health profiles is stored on their side to serve the enterprise business initiatives of these services.
- Promoting a privacy friendly environment for the offered referrals: Privacy aware users will be encouraged to participate on such cloud-based healthcare service, since their health data will be stored locally on their own side and they can decide what data to be released for every recommendation request. In addition, the released health data will not leave their devices until it is properly concealed.

- Reducing the liability of cloud-based healthcare service providers in securing their clients' health information: The responsibility of the cloud-based healthcare service providers for protecting their clients' health data is alleviated, as the clear and accurate version of users' health profiles are stored on the users' devices. Privacy invasion on these concealed health profiles will not be as harmful as much as it is when compared with the ones that occur in the current conventional approaches of privacy.
- Increasing the revenues of the cloud-based healthcare service providers: The extracted referrals list can be used to enhance the revenues of the cloud-based healthcare service providers from different perspectives, such as maximizing the precision of target marketing by advertising various medical services, healthcare related devices and local business based on the predicated recommendations.

2) CLOUD-BASED HEALTHCARE SERVICES RESTRICTIONS

- Losing the control over users' health profiles: Indeed, the users' health profiles are stored remotely at their side. However, the service providers are also holding and storing concealed health profiles from previous recommendation processes for a certain period of time. Although, the concealed profiles are an outdated snapshot of the users' health data in a concealed form, they are sufficient enough for training, building, and maintaining the recommendation models of the cloud-based healthcare service.
- Potential abuse for the cloud based service by malicious users: The anonymity attained by our holistic privacy approach can induce malicious users to perform attacks on the cloud based service or other users while exploiting the advantage of hiding their identity, thus they can escape from legal prosecution. We have introduced the usage of security authority centre (SAC), which is a trusted third party responsible for assessing the reputation of each entity involved in the referrals generation process. Moreover, SAC is in charge of issuing anonymous credentials for each user in the system. Future research should investigate how to attain the functionality of SAC in P2P fashion and without relying on a centralized entity.

C. PRIVACY ENFORCEMENT

Utilizing topological formation for data collection with a two-stage concealment process within our framework allows the end-user to control what data to be collected from their health profiles at each concealment level. Specifically, the group profile that is exposed to the cloud-based healthcare services contains a set of recorded vital measurements from the users' health profiles that are released to a specific recommendation request. These measurements usually represent a small proportion of recorded vital sign measurements in relative relation to the total number of recorded vital sign measurements in the users' health profiles. Moreover, the anonymity and concealment techniques used during the data collection process ensure attaining an appropriate privacy level for system end-users. Those are very important aspects in our framework that depicts its ability to diminish the impact of the privacy breaches, limit the misuse of health information, and to enforce and verify the attained privacy for its end-users. Using P3P policies also enable the end-user to present evidence that his/her health data were released for a specific recommendation process, at a specific time, and for a specific cloud-based healthcare service.

VI. PROSPECTIVE SCENARIOS FOR THE HOLISTIC PRIVACY FRAMEWORK

The proposed framework was utilized in diverse scenarios to create privacy aware versions for three beneficial applications of the cloud-based services, which are a recommender service for IPTV content providers [14], [20]–[22], [26], data mash-up service for IPTV recommender services [19], and community discovery & recommendation service [23], [24], [27]. Privacy aware versions of location based recommendation service and mobile jukebox content recommender service [16] were also introduced in order to show the applicability of our approach. The implementation and evaluation of such applications of the collaborative privacy framework confirmed that it is possible to employ the concealed profiles of end-users to extract accurate recommendations. In the next subsection, we will present the preliminary result of a case study for healthcare recommender service based on IoHT devices and how our holistic privacy framework can be used as a privacy-preserving infrastructure to control the privacy for users within the recommendation process.

A. CASE STUDY: HEALTHCARE RECOMMENDER SERVICE

We consider the scenario where a healthcare recommender service (CHS) is implemented as an external cloud based service and end-users give information about their health data to that service in order to receive personalized health insights. The user's health data is stored in his/her profile in the form of measurements for different vital signs; such measurements are implicitly recorded by the various IoHT devices. The normal ranges for these measurements depending on gender, age, weight, and overall health status of the patient. The fog node at the end-user side will explicitly extract the recorded measurements from the various IoHT devices to reconstruct a detailed health profile, which will be used by a cloud-based healthcare recommender service. The healthcare recommender service collects and stores different users' health profiles in order to generate useful health insights.

In this scenario there are two possible ways for the user's discloser through his/her personal measurements included in his/her health profile [53] or through the user's network address (IP). *EMCP* employs two principles to eliminate these two disclosure channels, respectively. The two stage concealment process was used to conceal user's health data for different measurements in his/her profile and an

anonymous data collection protocol is used to hide the user's network identity by routing the communication with other participants through relaying nodes in Tor's anonymous network [13]. We did not assume the external cloud based healthcare recommender service to be completely malicious. This is a realistic assumption because the service provider needs to accomplish some business goals and increase its revenues. In this scenario, we will use the fog node storage to store the end-user health profile. However, the healthcare recommender service maintains a centralized database for storing the group profiles that is used in building and training the recommendations' models. Additionally, we alleviate the user's identity problems stated above by using anonymous pseudonyms identities for end-users. The recommendation process based on the two-stage concealment process in our framework can be summarized as follows:

1. In the setup phase, EMCP is deployed in the user's fog node, which in turn will be responsible for the concealment of any data that is collected by the healthcare recommender service. Subsequently, the manager agent within EMCP creates an IoHT network by preparing a virtual private network (VPN) to provide a secure transmission channel for any communication between the fog node and various IoHT devices. Additionally, this step separates IoHT network from the local area network. Thereafter, the end-user needs to redirect the network connection of each IoHT device to this node. Once the connection is established and verified, EMCP dispatches a local concealment agent to each IoHT device in the patient's environment. The local concealment agent will be residing on devices' memory, and will be responsible for executing the first-stage of the two-stage concealment process on any data to be released from this device.
2. The learning agent within the EMCP periodically collects the health data from different IoHT devices in order to construct locally a user's health profile. The local profile is stored in three databases, the first one is the vital sign measurements database that contains (DeviceID, time_date, measurement_type, measurement_value) and the second one is the metadata database that contains the feature vector for data related to the measurement of the vital sign (id, feature1, feature2, feature3). The feature vector can include: normal range, average readings, atmospheric pressure, moisture, humidity, temperature, location and so on. Finally, the last one is the realized activities database that contains (type of activity, path length, time interval, average speed, location).
3. Based on user's appeal, the manager agent within the EMCP broadcasts a message to various IoHT devices placed on the patient's surrounding environment to request recommendations for a personalized life-style that could potentially improve the health condition of its owner. The IoHT device with a sufficient amount of health data performs a local concealment process to conceal its log-file. The log-file is a lightweight embedded database which is hosted on each IoHT device that is responsible for storing vital sign readings, which were locally collected by this device. Finally, The IoHT devices submit their locally concealed health data to the manager agent using a predefined secure WI-FI or Bluetooth connection.
4. After the manager agent receives all the devices' data, it constructs an aggregated profile (group profile), then, executes a global concealment process to conceal this group profile. Then after, it can interact with the cloud based healthcare recommender service by acting as an intermediary node that has the group profile as its own health profile. The manager agent submits the group profile through an anonymized network to the healthcare recommender service in order to obtain recommendations, while ensuring the anonymity of the user's network address.
5. The healthcare recommender service performs its filtering techniques on the group profile that return a list of personalized life-styles that are correlated with such a profile. Then, this list is encrypted with the private key provided by the manager agent. The healthcare recommender service sends back the encrypted list on the reverse path to the requester fog node. The manager agent within the user's fog node in turn gets this final list decrypted and published to the mobile phone of its end-user.

1) LOCAL CONCEALMENT PROCESS USING CLUSTERING TRANSFORMATION ALGORITHM (CTA)

In this research, a novel algorithm for the local concealment process has been proposed in order to conceal the locally recorded data (log-file) hosted on various IoHT devices before sharing it with external parties and/or the fog nodes. *CTA* is especially designed for the sparse data problem we have here. *CTA* partitions the log-file into smaller clusters and then pre-processes each cluster such that the distances inside the same cluster will be maintained in its concealed version. We use local learning analysis (*LLA*) clustering method proposed in [25] to partition the log-files. After the completion of the partitioning, we embed each cluster into a random dimension space (based on parameter *d-dim*) so the sensitive readings will be protected. Then, the resulting clusters will be rotated randomly. In such a way, *CTA* conceals the data inside log-file while preserving the distances between the data points to provide highly accurate results when performing recommendations. More details about the algorithm can be found in [16].

2) GLOBAL CONCEALMENT PROCESS USING THE ENHANCED VALUE-SUBSTITUTION (EVS) ALGORITHM.

After executing the local concealment process, the global concealment process starts on the aggregated profile. The key idea for *EVS* is based on the work in [31] that uses the Hilbert curve to maintain the association between

different dimensions. In this subsection, we extend this idea as following: we also used the Hilbert curve to map *m-dimensional* profile to *1-dimensional* profile then *EVS* discovers the distribution of that *1-dimensional* profile. Finally, we perform perturbation based on that distribution in such a way to preserve the range of aggregated profile. More details about the algorithm can be found in [16].

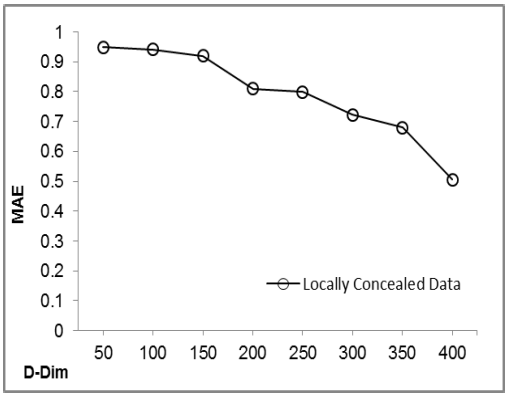

FIGURE 5. Accuracy of recommendations for the locally concealed log-file.

3) EXPERIENTIAL RESULTS

To evaluate the accuracy of *CTA* algorithm with respect to a different number of dimensions in the log-file, we controlled the *d-dim* parameters of *CTA* to vary the number of dimensions during the local concealment process. Figure 5 shows the performance of recommendations of a locally concealed log-file in terms of mean absolute error (*MAE*), as shown in the accuracy of recommendations based on the locally concealed data is a little bit low when *d-dim* is low. But at a certain number of dimensions (250), the accuracy of recommendations on the locally concealed data is nearly equal to the accuracy obtained using the original data. In the second experiment performed on the *CTA* algorithm, we examined the effect of the *d-dim* on the attained privacy level in terms of the variation of information (VI) metric. As shown in Figure 6, privacy levels decrease with respect to the increase

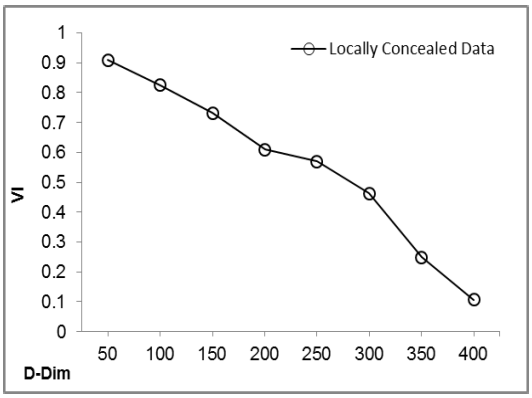

FIGURE 6. Privacy levels for the locally concealed log-file using CTA.

in *d-dim* values in the log-file. The *d-dim* is the key element for controlling the privacy level where smaller *d-dim* values, the higher privacy level was attained. However, clearly the highest privacy is at *d-dim*=50. There is a noticeable drop of attained privacy when we changed *d-dim* from 200 to 350. The *d-dim* value 200 is considered as a critical point for the privacy. Note that rotation transformation adds an extra privacy layer to the data and in the same time maintains the distance between data points to enable the healthcare recommender service to build accurate recommendation models.

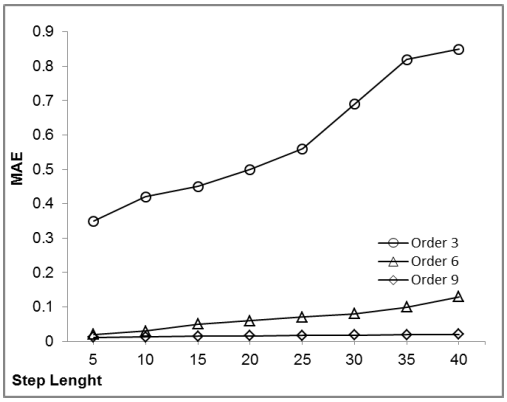

FIGURE 7. Accuracy level for different step length and orders of EVS.

In the third experiment, which was performed on the *EVS* algorithm, we measured the relation between different Hilbert curve parameters (order and step length) on the attained accuracy and privacy levels. We mapped the concealed aggregated profile to Hilbert values using order 3, 6, and 9. We gradually increased the step length from 5 to 40. Figure 7 shows the accuracy of recommendations based on different changes in step length and curve order parameters. As seen, increasing the value of the order parameter in the *EVS* algorithm, the concealed version of the aggregated profile offers more accurate recommendations according to MAE metric. When a bigger value is given to the curve order parameter, the granularity of the Hilbert curve becomes finer. So, the mapped values can preserve the distribution of the data within the aggregated profile. Additionally, selecting a larger value for the step length parameter increases the attained accuracy as bigger partitions are formed with a larger range to generate random values from, which will be used later to substitute the real data values in the aggregated profile. Finally, as shown in Figure 8 when increasing the value of the order parameter, a smaller range is calculated within each partition, which introduces less substituted values compared with lower orders that introduce larger ranges that realize a higher variation of information (VI) values. The reason for this behavior is the larger order divides the *m-dimensional* aggregated profile into more grids, which makes Hilbert curve better at reflecting the distribution of the data within the aggregated profile. Moreover, as seen for the same order parameter, the VI values are generally the same for different step length parameters

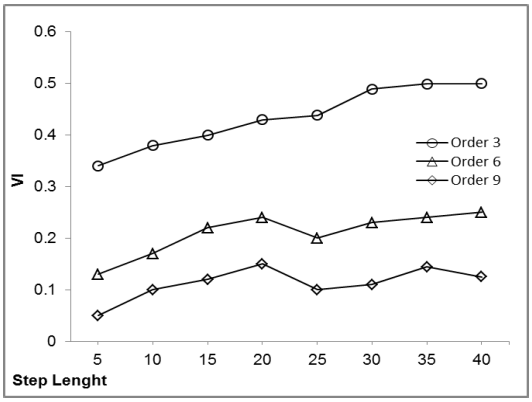

FIGURE 8. Privacy level for different step length and orders of EVS.

except for order 3, in which VI values have a sharp increase when the step length grows from 25 to 30. The effect of increasing step length parameter on VI values is more sensible in lower curve orders as fewer grids are formed and any increase of the step length parameter leads to covering of more portions of these grids. Eventually, this introduces a larger range to generate random values from. Considering the previous results, the manager agent should select *EVS* parameters in such a way to achieve a trade-off between privacy and accuracy levels.

VII. THE HOLISTIC PRIVACY FRAMEWORK PROTOTYPE

We have implemented the holistic privacy framework prototype with an aim to demonstrate the applicability of our approach in real life scenarios. However, we need to perform more design work in order to enhance its usability and make it friendlier to comply with the changing privacy practices and guidelines. The technologies used to develop our holistic privacy framework are:

1. The proposed two-stage concealment process is implemented in C++. The various local concealment algorithms were implemented using octave libraries. Moreover, the MPICH implementation of the MPI communication standard for distributed memory implementation of the global concealment algorithms to mimic a distributed reliable network of peers. To implement Paillier encryption scheme, the Number Theory Library (NTL) was used. One practical issue that must be dealt with when using the Paillier cryptosystem is the fact that it cannot naturally encrypt floating-point numbers. Floating-point numbers must be converted to a fixed-point representation. This is done by multiplying them by a large constant and then truncating the result to an integer.
2. The Aglets library was used to build different agents within the proposed *EMCP* middleware, which are running inside the user's fog nodes.
3. P3P policies and APPEL preferences rules standards were used to encode data collection, usage practices, and their actions.
4. MySQL database was used as data storage for storing users' health profiles, policies, and privacy preferences that were acquired by the *EMCP* middleware.
5. Tor network was used to attain anonymity when sending data between different parties within the system, either between the IoHT devices and fog nodes or between the fog nodes and the cloud based healthcare recommender service.
6. The experiments were conducted using a dataset pulled from the SportyPal network[10] that was linked to another dataset containing health parameters (blood pressure, heart rate, electrocardiogram, blood glucose, and respiratory rate) of 6000 students in one of the universities in North America in the period of 2010 to 2012.

In order to set-up the proposed holistic privacy framework, the end-users have to install the *EMCP* middleware on their personal gateways (Setup box or mobile phone). Then after, they relocate their stored health profiles into vital sign measurements, meta-data and realized activities databases within the learning agent. Finally, they formalize their privacy preferences and actions for the various policies. The healthcare recommender services are only required to offer P3P-compliant service by encoding their data collection and data usage practices in the form of P3P policies.

VIII. CONCLUSIONS AND FUTURE WORK

In this paper, we presented an attempt to develop an innovative approach for handling privacy in the current service oriented model. The holistic privacy framework that was developed in complying with the OECD privacy principle has been depicted in detail. The proposed framework was implemented as a middleware that we have entitled *EMCP* ''enhanced middleware for collaborative privacy''. We gave a brief overview of *EMCP* architecture, components, and interaction sequence. We presented a novel two-stage concealment process, which provides complete privacy control to patients over their vital measurements. The concealment process utilizes a topological formation for data collection, where IoHT devices and personal gateway are organized into some form of structure for creating an aggregated profile. Fog nodes and Healthcare recommender services use a platform for privacy preferences (P3P) policies for specifying their data usage practices. While end-users describe their privacy constraints for the data extracted from their health profiles in a dynamically updateable fashion using P3P policies exchange language (APPEL). The proposed framework allows a fine-grained enforcement of privacy policies by allowing end-users to ensure the extracted preferences for specific recommendation requests do not violate their privacy by automatically checking whether there is an APPEL preference corresponding to the given P3P policy. Fog nodes aggregate the vital measurements obtained from the underlying IoHT devices, encapsulate them in a group profile,

[10]http://www.sportypal.com/

and then send it to the healthcare recommender service. We have tested the performance of the proposed framework on a case study for healthcare recommender service using a real dataset. We evaluated how the overall accuracy of the recommendation varies based on various parameters of the two-stage concealment process. The experimental and analysis results show that privacy increases under the proposed framework without hampering the accuracy of the recommendation. Thus, adding the proposed framework does not severely affect the accuracy of the recommendation based on the off-the-shelf recommendations techniques.

Upon the end of this research work, we realized that there would be many challenges in building a holistic privacy framework for cloud based healthcare services. As a result, we focused on a middleware approach in our holistic privacy solution. A future research agenda will include utilizing game theory to better formulate groups of IoHT devices, sequential vital measurements release and its impact on the privacy of the whole health profile. Furthermore, it is included to strengthen our holistic privacy framework against shilling attacks, extending our scheme to be directed towards multi-dimensional trust propagation and distributed collaborative filtering techniques in a P2P environment. We also need to perform extensive experiments on other real datasets from the UCI repository and compare our performance with other techniques proposed in the literature. Finally, we need to consider different data partitioning techniques as well as identify potential threats and add some protocols to ensure the privacy of the data against those threats.

REFERENCES

[1] B. Alghamdi and H. Fouchal, "A mobile wireless body area network platform," *J. Comput. Sci.*, vol. 5, no. 4, pp. 664–674, Jul. 2014.

[2] J. Blum and E. Magill, "M-psychiatry: Sensor networks for psychiatric health monitoring," in *Proc. 9th Annu. Postgraduate Symp. Converg. Telecommun., Netw. Broadcast.*, Jun. 2008, pp. 33–37.

[3] J. M. Blum and E. H. Magill, "The design and evaluation of personalised ambient mental health monitors," presented at the 7th IEEE Conf. Consum. Commun. Netw. Conf., Las Vegas, NV, USA, 2010, pp. 1–5.

[4] G. Blumrosen, N. Avisdris, R. Kupfer, and B. Rubinsky, "C-SMART: Efficient seamless cellular phone based patient monitoring system," presented at the IEEE Int. Symp. World Wireless, Mobile Multimedia Netw., Jun. 2011, pp. 1–6.

[5] F. Bonomi, R. Milito, J. Zhu, and S. Addepalli, "Fog computing and its role in the Internet of Things," presented at the 1st edition MCC Workshop Mobile Cloud Comput., Helsinki, Finland, Aug. 2012, pp. 13–16.

[6] J. Canny, "Collaborative filtering with privacy," presented at the IEEE Symp. Secur. Privacy, May 2002, pp. 45–57.

[7] J. Canny, "Collaborative filtering with privacy via factor analysis," presented at the 25th Annu. Int. ACM SIGIR Conf. Res. Develop. Inf. Retr., Tampere, Finland, May 2002, pp. 45–57.

[8] S. Cockcroft and P. Clutterbuck, "Attitudes towards information privacy," in *Proc. ACIS*, 2001, p. 20.

[9] L. Columbus, "83% of healthcare organizations are using cloud-based apps today," Forbes, New York, NY, USA, Tech. Rep., 2014.

[10] E. Commission, "Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector," *Off. J. L*, vol. 201, no. 31, p. 7, 2002.

[11] L. F. Cranor, "'I didn't buy it for myself' privacy and ecommerce personalization," presented at the ACM Workshop Privacy Electron. Soc., Washington, DC, USA, 2003, pp. 111–117.

[12] B. Dagnall. (2016). *Leveraging The Internet Of Healthcare Things (IoHT). Digitalist Magazine From*. [Online]. Available: http://www.digitalistmag.com/customer-experience/2016/02/29/leveraging-internet-of-healthcare-things-04043784

[13] R. Dingledine, N. Mathewson, and P. Syverson, "Tor: The second-generation onion router," presented at the 13th Conf. USENIX Secur. Symp., vol. 13. San Diego, CA, USA, 2004.

[14] Directive, E., "95/46/EC of the European Parliament and of the Council of 24 Oct. 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data," *Off. J. EC*, vol. 23, no. 6, 1995.

[15] K. Dvorak. (2015). *IoT in Healthcare Could Have Economic Impact of up to 1.7T. From*. [Online]. Available: http://www.fiercehealthcare.com/it/report-iot-healthcare-could-have-economic-impact-up-to-1-7t

[16] A. Elmisery and D. Botvich, "Privacy aware obfuscation middleware for mobile jukebox recommender services," presented at the 11th IFIP Conf. e-Business, e-Service, e-Society, Kaunas, Lithuania, 2011, pp. 73–89, doi: 10.1007/978-3-642-27260-8_6.

[17] A. Elmisery and D. Botvich, "Privacy aware recommender service using multi-agent middleware- an IPTV network scenario," *Informatica*, vol. 36, no. 1, 2012.

[18] A. M. Elmisery, "Private personalized social recommendations in an IPTV system," *New Rev. Hypermedia Multimedia*, vol. 20, no. 2, pp. 145–167, 2014, doi: 10.1080/13614568.2014.889222.

[19] A. M. Elmisery and D. Botvich, "Agent based middleware for private data mashup in IPTV recommender services," presented at the IEEE 16th Int. Workshop Comput. Aided Modeling Design Commun. Links Netw. (CAMAD), 2011, pp. 10–11 Jun. 2011, doi: 10.1109/CAMAD.2011.5941096.

[20] A. M. Elmisery and D. Botvich, "Privacy aware recommender service for IPTV networks," presented at the Multimedia Ubiquitous Eng. (MUE), 5th FTRA Int. Conf., Jun. 2011, pp. 28–30, doi: 10.1109/MUE.2011.70.

[21] A. M. Elmisery and D. Botvich, "Agent based middleware for maintaining user privacy in IPTV recommender services," in *Proc. 3rd Int. ICST Conf. Secur. Privacy Mobile Inf. Commun. Syst. MobiSec*, Aalborg, Denmark, May 2011, pp. 64–75, doi: 10.1007/978-3-642-30244-2_6.

[22] A. M. Elmisery and D. Botvich, "Multi-agent based middleware for protecting privacy in IPTV content recommender services," *Multimedia Tools Appl.*, vol. 64, no. 2, pp. 249–275, 2013, doi: 10.1007/s11042-012-1067-3.

[23] A. M. Elmisery, K. Doolin, and D. Botvich, *Privacy Aware Community Based Recommender Service for Conferences Attendees*, vol. 243. Amsterdam, The Netherlands: IOS Press, 2012, doi: 10.3233/978-1-61499-105-2-519.

[24] A. M. Elmisery, K. Doolin, I. Roussaki, and D. Botvich, *Enhanced Middleware for Collaborative Privacy in Community Based Recommendations Services* (Computer Science and its Applications), vol. 203, S.-S. Yeo, Y. Pan, S. Y. Lee, and B. H. Chang, Eds. Dordrecht, The Netherlands: Springer, 2012, pp. 313–328, doi: 10.1007/978-94-007-5699-1_32.

[25] A. M. Elmisery and H. Fu, "Privacy preserving distributed learning clustering of healthcare data using cryptography protocols," presented at the IEEE 34th Annu. Comput. Softw. Appl. Conf. Workshops (COMPSACW), Jul. 2010, pp. 19–23, doi: 10.1109/COMPSACW.2010.33.

[26] A. M. Elmisery, S. Rho, and D. Botvich, "Collaborative privacy framework for minimizing privacy risks in an IPTV social recommender service," *Multimedia Tools Appl.*, vol. 75, no. 22, pp. 14927–14957, Nov. 2016, doi: 10.1007/s11042-014-2271-0.

[27] A. M. Elmisery, S. Rho, and D. Botvich, "Privacy-enhanced middleware for location-based sub-community discovery in implicit social groups," *J. Supercomput.*, vol. 72, no. 1, pp. 247–274, Jan. 2016, doi: 10.1007/s11227-015-1574-x.

[28] A. Esma, "Experimental demonstration of a hybrid privacy-preserving recommender system," 2008.

[29] S. Fadilpašiá. (2016). *Most Enterprises Use Internet of Things Devices*. [Online]. Available: http://betanews.com/2016/06/30/internet-of-things-enterprise-adoption/

[30] R. K. Ganti, P. Jayachandran, T. F. Abdelzaher, and J. A. Stankovic, "SATIRE: A software architecture for smart AtTIRE," presented at the 4th Int. Conf. Mobile Syst., Appl. Services, Uppsala, Sweden, 2006.

[31] G. Ghinita, P. Kalnis, and S. Skiadopoulos, "PRIVE: Anonymous location-based queries in distributed mobile systems," presented at the 16th Int. Conf. World Wide Web, Banff, AB, Canada, 2007.

[32] J. Goecks, W. K. Edwards, and E. D. Mynatt, "Challenges in supporting end-user privacy and security management with social navigation," presented at the 5th Symp. Usable Privacy Secur., Mountain View, CA, USA, 2009.
[33] C. Huang, H. Lee, and D. H. Lee, "A privacy-strengthened scheme for E-healthcare monitoring system," *J. Med. Syst.*, vol. 36, no. 5, pp. 2959–2971, 2012, doi: 10.1007/s10916-011-9774-2.
[34] Z. Huang, W. Du, and B. Chen, "Deriving private information from randomized data," presented at the ACM SIGMOD Int. Conf. Manag. Data, Baltimore, MD, USA, 2005.
[35] IDC. (2015). *Explosive Internet of Things Spending to Reach $1.7 Trillion in 2020, According to IDC*. [Online]. Available: https://www.idc.com/getdoc.jsp?containerId=prUS25658015
[36] S. Jankowski. (2014). *The Sectors Where the Internet of Things Really Matters. Harvard Business Review*. [Online]. Available: https://hbr.org/2014/10/the-sectors-where-the-internet-of-things-really-matters
[37] H. Kargupta, S. Datta, Q. Wang, and K. Sivakumar, "On the privacy preserving properties of random data perturbation techniques," presented at the 3rd IEEE Int. Conf. Data Mining, 2003.
[38] M. Katagi and S. Moriai, "Lightweight cryptography for the Internet of Things," *Sony Corp.*, pp. 7–10, 2008.
[39] H. D. Kim, "Applying consistency-based trust definition to collaborative filtering," *KSII Trans. Internet Inf. Syst.*, vol. 3, no. 4, pp. 366–374, 2009.
[40] K. Lorincz, "Sensor networks for emergency response: Challenges and opportunities," *IEEE Pervasive Comput.*, vol. 3, no. 4, pp. 16–23, Apr. 2004, doi: 10.1109/mprv.18.
[41] K. Malasri and L. Wang, "Addressing security in medical sensor networks," presented at the 1st ACM SIGMOBILE Int. Workshop Syst. Netw. Support Healthcare Assisted living Environ., San Juan, PR, Territory, 2007.
[42] J. Manyika. (2015). *Unlocking the Potential of the Internet of Things*. [Online]. Available: http://www.mckinsey.com/business-functions/business-technology/our-insights/the-internet-of-things-the-value-of-digitizing-the-physical-world
[43] (2015). *IoT Deployments in Healthcare to Reach $117 Billion by 2020, Says New Mind Commerce Report*. [Online]. Available: http://www.prnewswire.com/news-releases/marketresearchcom-iot-deployments-in-healthcare-to-reach-117-billion-by-2020-says-new-mind-commerce-report-300070129.html and http://Market Research.com
[44] (2015). *IoT Healthcare Market by Components (Medical Device, System and Software, Service, and Connectivity Technology), Application (Telemedicine, Workflow Management, Connected Imaging, Medication Management), End-User-Global Forecast to 2020*. [Online]. Available: http://www.marketsandmarkets.com/Market-Reports/iot-healthcare-market-160082804.html and http://MarketsandMarkets.com
[45] I. Martinovic, M. Frank, D. Perito, T. Ros, and D. Song, "On the feasibility of side-channel attacks with brain-computer interfaces," presented at the 21st USENIX Conf. Secur. Symp., Bellevue, WA, USA, 2012.
[46] R. V. D. Meulen and J. Rivera. (2015). *Gartner Says By 2020, A Quarter Billion Connected Vehicles Will Enable New In-Vehicle Services and Automated Driving Capabilities*. [Online]. Available: https://www.gartner.com/newsroom/id/2970017
[47] B. N. Miller, J. A. Konstan, and J. Riedl, "PocketLens: Toward a personal recommender system," *ACM Trans. Inf. Syst.*, vol. 22, no. 3, pp. 437–476, 2004, doi:10.1145/1010614.1010618. [Online]. Available: http://doi.acm.org/
[48] C. Min, C. Yoo, Y. Lee, and J. Song, "Healthopia: Towards your well-being in everyday life," presented at the 4th Int. Symp. Appl. Sci. Biomed. Commun. Technol., Barcelona, Spain, 2011.
[49] Office, U. S. G. P. (1996). *Health Insurance Portability and Accountability Act of 1996 Public Law 104-191*. [Online]. Available: https://www.gpo.gov/fdsys/pkg/PLAW-104publ191/html/PLAW-104publ191.htm
[50] S. R. Oliveira and O. R. Zaïane, "Toward standardization in privacy-preserving data mining," presented at the ACM SIGKDD 3rd Workshop Data Mining Standards.
[51] J. S. Olson, J. Grudin, and E. Horvitz, "A study of preferences for sharing and privacy," presented at the CHI Extended Abstracts Human Factors Comput. Syst., Portland, OR, USA, 2005.
[52] D. Palmer, "The first big Internet of Things security breach is just around the corner," ZDNet, Tech Rep., 2016.
[53] R. Parameswaran and D. M. Blough, "Privacy preserving data obfuscation for inherently clustered data," *Int. J. Inf. Comput. Secur.*, vol. 2, no. 1, pp. 4–26, 2008, doi: 10.1504/ijics.016819.
[54] H. Polat and W. Du, "Privacy-preserving collaborative filtering using randomized perturbation techniques," presented at the 3rd IEEE Int. Conf. Data Mining, 2003.
[55] H. Polat and W. Du, "SVD-based collaborative filtering with privacy," presented at the ACM Symp. Appl. Comput., Santa Fe, NM, USA, 2005.
[56] N. Ramakrishnan, B. J. Keller, B. J. Mirza, A. Y. Grama, and G. Karypis, "Privacy risks in recommender systems," *IEEE Internet Comput.*, vol. 5, no. 6, pp. 54–63, Nov. 2001.
[57] M. Souil and A. Bouabdallah, "On QoS provisioning in context-aware wireless sensor networks for healthcare," presented at 20th Int. Conf. Comput. Commun. Netw. (ICCCN), Jul. 2011.
[58] D. Storm, "MEDJACK: Hackers hijacking medical devices to create backdoors in hospital networks," Computerworld, Tech. Rep., 2015.
[59] C. C. Tan, H. Wang, S. Zhong, and Q. Li, "IBE-lite: A lightweight identity-based cryptography for body sensor networks," *Trans. Inf. Technol. Biomed.*, vol. 13, no. 6, pp. 926–932, Jun. 2009, doi: 10.1109/titb.2033055.
[60] E. J. Topol. (2015). *The Future of Medicine is in Your Smartphone. The Wall Street Journal*. [Online]. Available: http://www.wsj.com/articles/the-future-of-medicine-is-in-your-smartphone-1420828632
[61] U. Varshney, "Pervasive healthcare and wireless health monitoring," *Mob. Netw. Appl.*, vol. 12, nos. 2–3, pp. 113–127, 2007, doi: 10.1007/s11036-007-0017-1.
[62] D. Malan, T. Fulford-Jones, M. Welsh, and S. Moulton, "Codeblue: An ad hoc sensor network infrastructure for emergency medical care," in *Proc. Int. Workshop Wearable Implantable Body Sensor Netw.*, vol. 5. 2004.

AHMED M. ELMISERY is currently working as an assistant professor at the electronic engineering department of Federico Santa María Technical University (Chile). He is also a research fellow at Internet of Things and People Research Center, Malmö University (Sweden), and Adjunct Assistant Professor at Computer Science Department, Technical College (Egypt). He visited the Center for Advanced Technology in Telecommunications and Secure Systems at Monash University, Australia from May 2014 to June 2015. Before that, he was working as a Researcher in computer security at Telecommunications Software and Systems Group, Department of Computing, Mathematics and Physics, Waterford Institute of Technology, (Ireland). He received his B.S. degree in computer science from the Faculty of Computer Science, Mansoura University, Egypt (2001), M.S. degree in computer science from the Arab Academy for Science & Technology, Egypt (2007), and Ph.D. degree in computer science from Waterford Institute of Technology, Ireland (2014). He has published over 36 research papers in national and international conferences. His research interests include security, cryptography, and machine learning. He is conducting research on privacy and security for future telecommunication services. His work has been grounded to develop privacy enhanced algorithms for outsourced data in healthcare systems and recommender systems scenarios.

SEUNGMIN RHO received the M.S. and Ph.D. degrees in computer science from Ajou University, South Korea, in 2003 and 2008, respectively. He visited the Multimedia Systems and Networking Laboratory, University of Texas at Dallas, from 2003 to 2004. Before he joined the Computer Sciences Department, Ajou University, he spent two years in industry. From 2008 to 2009, he was a Post-Doctoral Research Fellow with the Computer Music Laboratory, School of Computer Science, Carnegie Mellon University. He was a Research Professor with the School of Electrical Engineering, Korea University, from 2009 to 2011. In 2012, he was an Assistant Professor with the Division of Information and Communication, Baekseok University. He is currently an Assistant Professor with the Department of Media Software, Sungkyul University. His current research interests include database, big data analysis, music retrieval, multimedia systems, machine learning, knowledge management, and computational intelligence. He has authored 100 papers in refereed journals and conference proceedings in these areas. He has received a few awards, including the Who's Who in America, the Who's Who in Science and Engineering, and the Who's Who in the World in 2007 and 2008. He has been involved in over 20 conferences and workshops as various chairs and over 30 conferences/workshops as a Program Committee Member. He has edited a number of international journal special issues as a Guest Editor, such as multimedia systems, information fusion, engineering applications of artificial intelligence, new review of hypermedia and multimedia, multimedia tools and applications, personal and ubiquitous computing, telecommunication systems, and ad hoc & sensor wireless networks.

DMITRI BOTVICH received the bachelor's and Ph.D. degrees in mathematics from the Faculty of Mechanics and Mathematics, Moscow State University, Russia, in 1980 and 1984, respectively. He led the PRTLI FutureComm project with the Telecommunication Software and Systems Group, Waterford Institute of Technology, Ireland, and has coordinated and worked in a number of EU and Science Foundation Ireland projects. He is currently a Chief Scientist with the Gaspard Monge Computer Science Laboratory, Université Paris-Est Marne-la-Vallée, France. He has authored over 100 papers in conferences and journals, and currently supervises seven Ph.D. students. His research interests include bio-inspired autonomic network management, security, trust management, wireless networking, queuing theory, optimization methods, and mathematical physics.