www.ijbar.org
ISSN 2249-3352 (P) 2278-0505 (E)
Cosmos Impact Factor-5.86

Identity Management in the Internet of Things In Medical Applications

Rejina P V
Assistant Professor in Computer Science,
Co-operative Arts And Science College, Madayi , Payangadi, Kannur- 670358, Kerala.

Abstract The Internet of Things (IoT) in healthcare and medical applications promises to solve many problems which are currently challenging the sector, ranging from remotely caring for our aging population to medical discoveries on incurable diseases. However, the challenges and risks of having 50 billion Things and users connected together are complex and may be detrimental to control. Concerns have been raised in relation to the IoT Identification Management (IDM) issues, in which each Thing (user and device) will be required to have a unique identity, and the IDM to be able to distinguish between a device and user, as well as ensuring identity and information context safety. This paper examines the underlying issues behind IDM and proposes a framework which aims to achieve the identification of Things and their safe management. The IDM framework is embedded in Mobile Ad Hoc Networks (MANETs) and assumes that most healthcare devices will be linked wirelessly and in mobile environments. The paper aims to open a research debate which will help to solve the future IoT IDM issues in healthcare applications.

Keywords Internet of Things (IoT), MANET, Identity Management (IDM)

1. Introduction

The purpose of this paper is to describe a joint research project that seeks to address the important issue of identity management in the Internet of Things (IoT) as specifically applied to healthcare and medical applications. The paper contends that the IoT is of particular importance and has great potential in healthcare and medical applications and environments due to the prevalence of objects and devices including mobile devices. Despite the fact that technology is having an increasing role in many fields of medicine, future healthcare and medical technologies face many challenges [1]. This includes the inability to offer a unified network environment which can provide innovative services applying to the underlying infrastructure of the future IoT. In addition, the healthcare field is becoming increasingly knowledge intensive, requiring the separate identification and management of numerous objects, about which knowledge (or at least information) must be stored. Furthermore, the prevalence of mobile applications, including the use of 'bring your own device' (BYOD) systems imposes the problem of healthcare applications that must function without rigid IT infrastructures. The problems that the identification of objects and management of knowledge presents in such environments are likely to restrict the development of the IoT in healthcare applications. This paper considers the introduction of new Identity Management (IDM) systems for use in *ad hoc* mobile networks (MANETs) to be the key to these problems.

This paper aims to introduce a new Mobile Ad-hoc Network (MANET) framework that will support the IDM of the future IoT. It is organised as follows: the remainder of Section 1 'sets the scene' and explains some of the technological issues involved in the IoT. Following on from this Section 2 discusses the ideas behind IDM; Section 3 examines MANETs and their role in IDM, and introduces a new MANET framework which will support IDM for the future IoT. Section 4 concludes the paper and makes recommendations for future research and the implementation of such a framework in practice.

1.1. The Problem of Complexity

The problem of managing complex knowledge in healthcare is hardly new. Francois-Marie Arouete Voltaire writing about 250 years ago opined that, '*Doctors prescribe medicine of which they know little, to cure disease of which they know less, in human beings of which they know nothing*' [1]. Since those days the diversity of medical knowledge and the complexity of healthcare environments have multiplied rapidly, a trend that shows little sign of ceasing. The 21st century has changed healthcare and medical sciences through the evolution of a number of significant healthcare and medical technologies that are used for epidemiology and

www.ijbar.org
ISSN 2249-3352 (P) 2278-0505 (E)
Cosmos Impact Factor-5.86

diagnosis. For example, six billion bases of the human genome were sequenced in the Human Genome Project and this led to the discovery of the underpinning characteristics of over one hundred common diseases such as most cancers, autoimmune disorders, and neurological conditions [1].

As a result, it may be said that there has never been a better time to develop the Internet than now, when the healthcare and medicine disciplines need it most. Due to advancements in medicine, people are now living longer but with increasing co-morbidities. Demography shows that between the years 2006 and 2036 the number of people over 85 in England will rise by approximately 180%, an increase from 1.055 to 2.959 million [2]. In addition, the pressure to cut down hospital costs, increasing staff shortages and insufficient intensive care and hospital bed volumes has forced the healthcare system to undergo a rapid evolution in its medical technologies which are intended to help in facing these challenges.

At the moment, predictable pathways of information in the healthcare sector are constantly changing: the physical world is becoming a type of information system in itself as objects and the information they contain increasingly coincide. In the IoT, sensors and actuators are often embedded in physical objects which are linked through wired and wireless networks, often using the same Internet Protocol (IP) that establishes connections on the Internet. The healthcare sector is already promoting e-health and personal health-oriented objects (or devices) which will be referred to in this paper as 'Things'.

1.2. The Scale of the Problem

In 2008, the number of Things connected to the Internet exceeded the number of people on earth, and it is predicted that 50 billion Things will be interconnected by the year 2020. A technological evolution of medicine has taken place in which healthcare professionals are now able to monitor patient heartbeat, blood pressure, the rate and depth of breathing, body temperature etc. remotely and continuously. In addition, the technology supports personalisation, in which patients with chronic conditions are able to live independently in a community of their choice using technology to support their lifestyles. For example, current technologies which have been providing support includes those used by the clinicians to monitor patients in their homes, with the patients checking their own HBP, temperature etc. Such devices include Lifeline Home Units, Personal Pendants, Wandering Client Alarms, PIR Movement Detectors, Fall Detectors, Flood Detectors, Bed Occupancy Sensors, Bogus Caller Buttons, Smoke, Natural Gas and Carbon Monoxide Detectors, Temperature Extremes Sensors, Automatic Medicine/Pill Reminders and Dispensers, Talking Colour Detectors for Blind People and Assisted GPS/GSM technologies which recognise when the user goes outside the safe zone. The number of such devices and their applications is increasing daily [3].

IoT enables the interconnections between people and Things and, through intelligent applications, Things and Things using a variety of access technologies. The world of Things includes physical devices, (see above), virtual Things and, as occurrences can be Things in themselves, even the events that are connected to Things [3]. The IoT is therefore considered in this paper to be an expansion of the Internet, and which will be able to detect and monitor changes in the physical status of connected Things. However, as there will eventually be billions of interconnected Things and humans communicating with them, it will require especially sophisticated technologies to manage and operate the IoT if consistency and integrity is to be maintained. This involves assigning each Thing in the network a unique identity (ID). Similarly, the IP, data and other technologies which are related to the ID can be included in the combinatorial complexity. As a result, the performance of the IoT depends on an effective and efficient means of identifying Things (i.e. an IDM framework).

Automatic identification technologies such as Radio Frequency Identification (RFID) are fundamental to the realisation of the IoT because they enable Things to be constantly linked with their virtual identity on the Internet. RFID tags attached to objects involve unique ID numbers that can be read wirelessly by interrogating devices and the result can be used to obtain information related to individual instances of objects that are managed by networked "back-end" systems. Miniaturised sensors now provide the ability to monitor the condition of objects (i.e. Things) and consequently make it possible to act dynamically upon changes in the status of Things such as those that are derived from their temperature, humidity, and chemical composition. Furthermore historical records, including both ID and sensor data, can be used off-line to trace the evolution of the Things' location and status throughout their life. Low-power radio communication technologies and the availability of increasingly powerful low-cost embedded processing power increase the autonomy of Things by providing them with networking capabilities and local intelligence. The distributed information infrastructures using Internet protocols for communication serve as connection hubs for all the Things, together with other resources such as databases, data mining tools, and computer networks [4]. However, the sheer number of devices which will be interconnected in future through the IoT and the expected limitations in user interface requires the redesigning of current Identity Management (IDM) systems. It is therefore necessary to discuss the issue of Identity Management and the technical challenges that this entails, which have resulted the development of a number of IDM architectures.

2. Identity Management (IDM)

The future IoT architecture in healthcare applications (based on the integration of the existing networks and services and the addition of many new healthcare devices such as remote–health monitoring devices, sensors, etc.)

www.ijbar.org
ISSN 2249-3352 (P) 2278-0505 (E)
Cosmos Impact Factor-5.86

faces a series of important technical challenges, one of them being the management of diverse user and object identities [5]. 'The separation of identity and locator is one such innovative trend, although the architectural problem of supporting the real people behind the physical device while at the same time protecting information about the user and its context has no solution yet' [6].

Various architectures have been proposed in relation to IDM including those which are concerned with naming, addressing, routing and security issues such as MILSA and Enhanced MILSA [7, 8]. These are based on identities rather than addresses to organise networks using distributed hash tables [9, 10]. Some are concerned with separating the ID and the locator [11]. The EU projects Daidalos [12] and SWIFT [13] are currently addressing the problem of IDM with a focus on the network and service infrastructures. The Virtual Identity concept [14] was proposed in this context, although it did not address the problem of how the wide range of entities can be organised in establishing a particular handshake session. Other schemes include: Microsoft Passport [15] Microsoft Cardspace [16], OpenID [17]. However, these schemes address general Web 2.0 types of approach without addressing explicitly how the IDM will cope with the sheer number of devices which will emerge when implementing the IoT [18].

In addition, Lampropoulos *et al.* [19] state that most proposed solutions are considered to implement ID frameworks which are applicable within well-defined administrative boundaries, as a result creating the "identity management island with interoperability issues". Such solutions are shifting the problem from the isolation of domains to the isolation of federations and certainly away from network convergence (which is a key aspect of the IoT) [20]. The healthcare sector is sensitive and also very broad as it is interconnected with many other sectors including monitoring and control, 'assisted living', security, mobility and many more. As a result, new technologies to support reliable IDM systems are essential.

3. MANETs and the IoT

Mobile users may make use of partial identities. Identity is usually defined as something that can be used to identify a particular person, device or entity. For a fuller discussion if the broader concept of identity see Abdelal *et al.* [21]. Mobile devices are used to demonstrate the research that informs this paper as it is assumed that most future healthcare devices will be connected by wireless links for ease of use and flexibility in a healthcare environment. Mobile devices have fixed identifiers (i.e. their number or address), which essentially provide unique mobile identities. Such identities take into account locations and user identities that enable users to enforce security and privacy.

Partial identities on the other hand are defined as the set of personal attributes of a user, where the user can have several partial identities, e.g. his/her work address, home telephone number, etc. [22]. For healthcare applications, we consider MANETs to be able to support issues related to IDM with several personal attributes and mobility. This will apply to devices (i.e. Things) as well as humans. Each device (or Thing) in a MANET is capable of independent movement in any direction, and should be capable of rearranging its links to the other devices in the network frequently and seamlessly.

A MANET at first glance may not seem to be directly related to the issue of IDM as IDM normally gives the impression of a traditional client/server structure, where users can establish a handshake with a server for authentication and other purposes. Although these have some security implications which involve packet forwarding and routing, as a part of network management, they are also the functions which are carried out by all available nodes within the network. Clearly IDM has considerable implications where MANETs are being used to connect the IoT, and the potential for IDM frameworks to operate in this area is capable of extension. A new IDM framework that will operate over MANETs is therefore proposed in this research and this is described in the next section of the paper.

4. The proposed IDM framework

The new MANET-based flexible and efficient IDM framework is expected to meet the current and future needs of IDM within the domain of IoT and ubiquitous computing environments in general. Figure 1 shows the proposed framework, which is modular and user-centred. Each module is designed to work either on its own or in conjunction with.

www.ijbar.org
ISSN 2249-3352 (P) 2278-0505 (E)
Cosmos Impact Factor-5.86

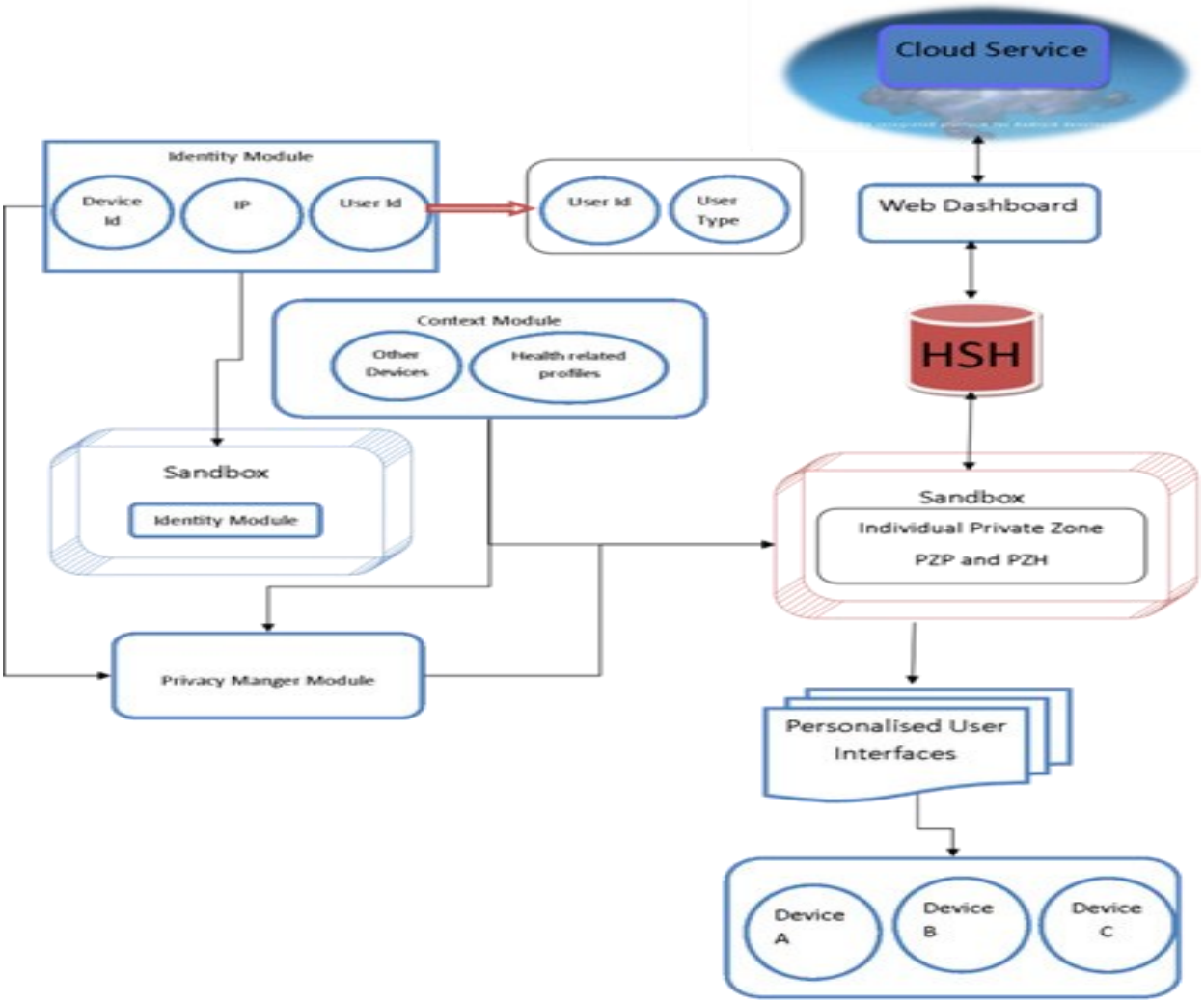

Figure 1. The IDM –MANET framework.

The *identity module* consists of Device ID, IP, and Use ID. The User ID is further divided to consist of Device ID and user type. It is of paramount importance to point out that in the IoT, there is a possibility of sharing a device with other e-Health or general IoT applications, it is also important to allow the usage of existing devices to be incorporated within the IoT domain. Therefore, a MANET provides a suitable platform and provides the means for seamless interaction of such Things. However, due to the nature of the sensitive information used with e-Health applications in the IoT, it is vital to create a separation of individual data within the shared device. This functionality is provided by 'sandbox' modules. These create a virtual 'wall' between the individual users of a shared device and provide a mechanism that segments the device and users' information cannot be shared or accessed by other users. This also provides an extra mechanism to help protect against ID theft and information misuse. One of the key elements that the framework will provide is offering new approaches to adding data security functions for Things. This is done by isolating individual personal content by creating a virtual lock-box (using sandboxing techniques) on Things. This can provide the necessary safeguards of individual content on shared devices within home environments and will separate content as well as applications of individual users who are sharing the same device(s). This will enable both individual users and corporate users to establish policies that meet the needs for managing personal content.

The *context module* will play a crucial role in the IoT. It helps to provide a personalised service to Things that will facilitate the functionality of the framework. This is done by providing a means of tracking the identity of Things and users in a more dynamic way and will help in restricting the usability of Things based on the context in which it is intended to be used.

www.ijbar.org
ISSN 2249-3352 (P) 2278-0505 (E)
Cosmos Impact Factor-5.86

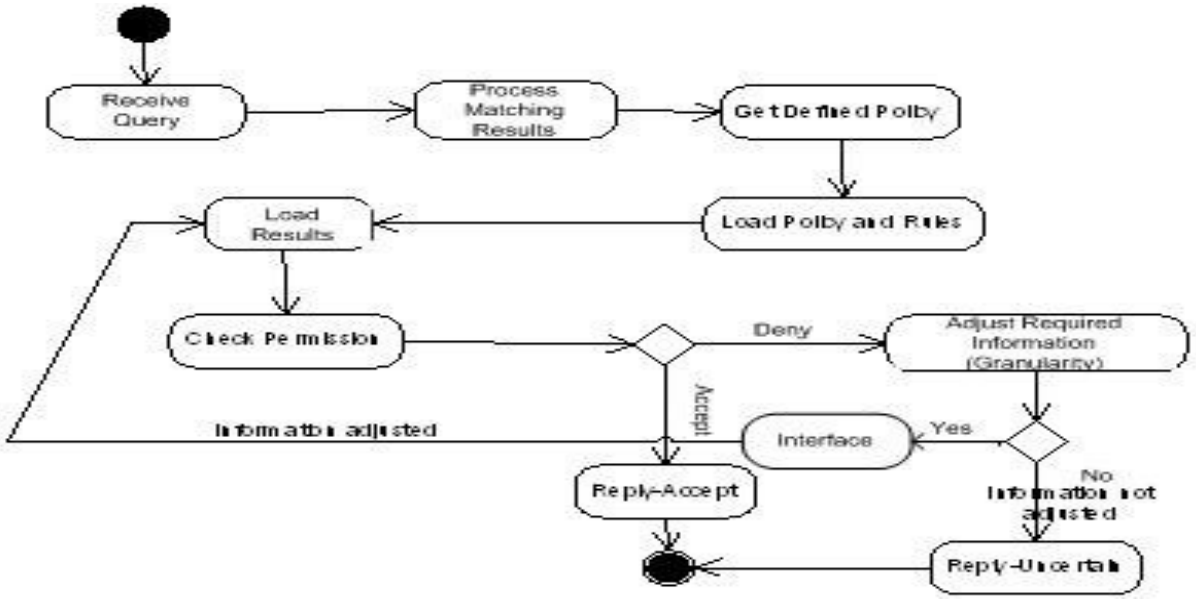

Figure 2. Information Granularity

The *privacy management module* provides an extra means of creating dynamic privacy policies that will enhance IDM security. The functionality of the contextual modules, the privacy module and the sandbox of the identity module is used to provide a personalised user interface to help in accessing and managing Ids in the IDM of the IoT. Personalised user interface and information access rights will be generated in the framework for individual users who are identified within the framework; in this case mainly doctors, nurses and home users. It is important to emphasise that the information communicated between Things should be restricted to the minimum if possible. This is for many reasons such as limiting the needed bandwidth during transmission, particularly when the devices involved are small, which reduces the amount of information that users may access, and preventing users from building a whole profile of a user. Hence, the proposed framework makes use of the information granularity module [24] that will provide a means of releasing only information that is needed based on the required functionality. For these reasons, to reduce the amount of information sent and received within the network, we are proposing an algorithm for the flow of events depicted in Figure 2 to be implemented in the privacy manager module for adjusting the granularity of information before sending.

The process is initiated after receiving a query where a relevant policy will be checked. If the request is successful then this is passed on to the algorithm used to reduce the amount of information before sending. The 'Adjust Required Information (Granularity)' process is triggered to allow users to be able to reduce the level of information that is to be sent to the node involved. The user will be given the option and an interface showing the current information available to other nodes. The user will then decide if he or she wants to reduce such information by indicating the appropriate boxes that represent user's information.

Figure 3 further expands the attributes in Figure 1 as structured identity attributes organised into tables with relationships between them. Each of the tables defines a structure in a way that information/attributes disclosure will be kept to minimal and not propagated to the world. Each identity or partial identity can be mapped to multiple profiles; each profile table has a 'one to many' relationship with the ProfileMapper table, while each identity table consists of several email tables. The ProfileMapper table can have and can manage more than one profile type.

This also allows each user identity in the Identity table to appear in more than one Profile table, i.e. social profile, home profile, work profile etc. The line(s) between the boxes that represent each of the individual schemas represents the inheritance that passes between the items in the tables.

In Figure 4 both XML schemas OfficeProfile and HealthProfile inherit from the RootContext schema, ProfileContext schema and Status schema respectively. We adopted the notion of defining the schemas as shown to reduce the level of duplication in terms of defining the users' profiles. For example, to define a new profile 'SocialProfile', we can inherit the elements from RootContext and just add new properties for the new profile type. This not only eliminates repetition but also saves storage space, level of user interaction etc., making the system more portable and more efficient.

Figure 4 presents the defined XML schema for contextual information [25]. We first start by creating a general schema that contains the base elements of all schemas, and then from there other schemas are created inheriting from the general schema as well as other schemas.

www.ijbar.org
ISSN 2249-3352 (P) 2278-0505 (E)
Cosmos Impact Factor-5.86

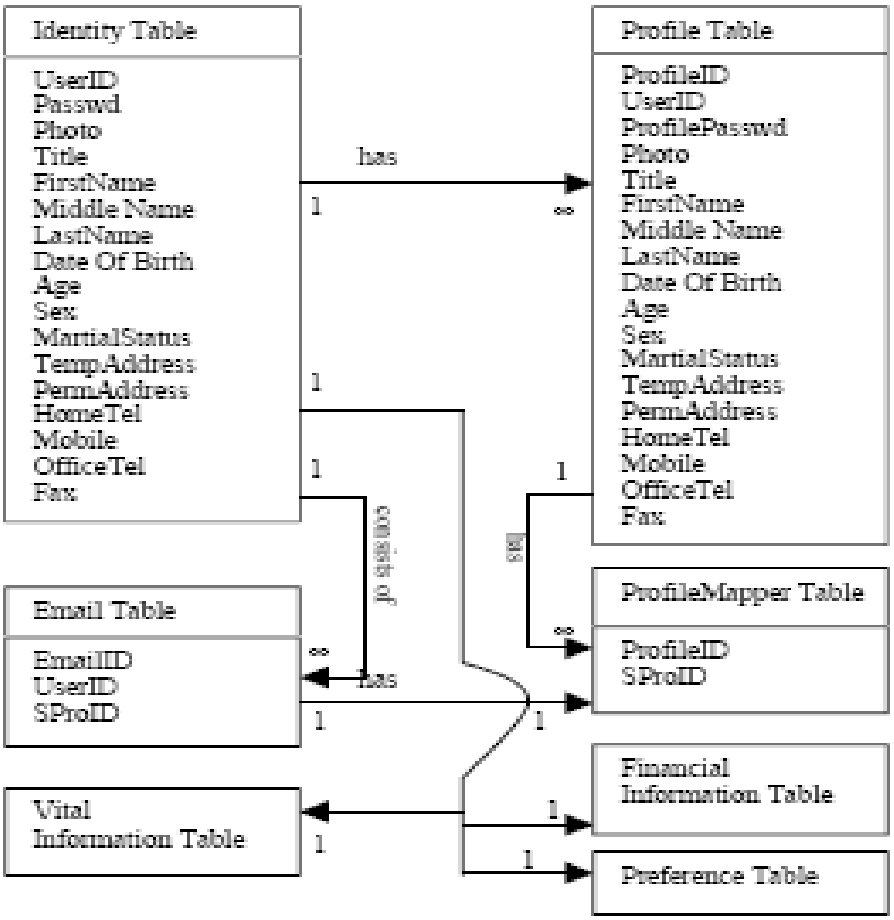

Figure 3. Identity Attributes

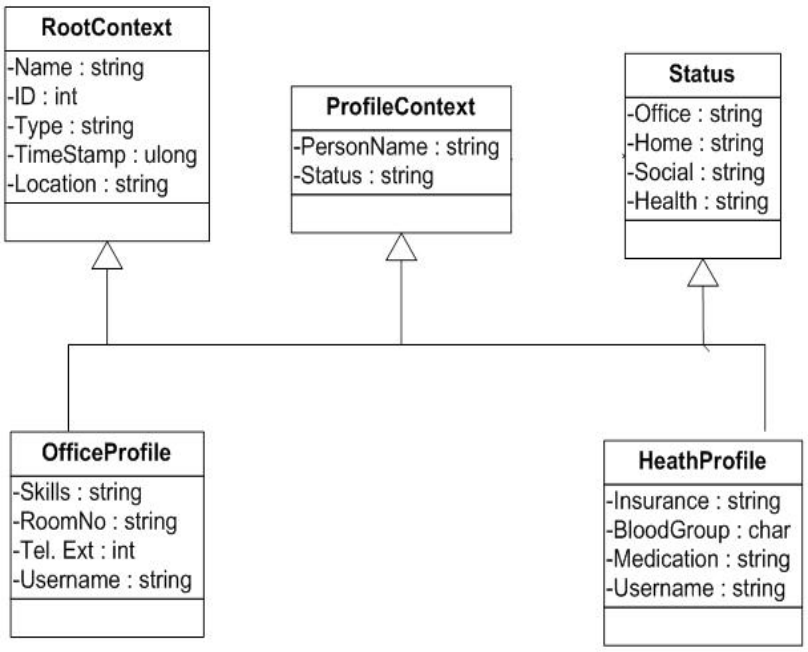

Figure 4. XML Schema

www.ijbar.org
ISSN 2249-3352 (P) 2278-0505 (E)
Cosmos Impact Factor-5.86

5. Proposed Implementation

The proposed IDM framework is intended for general use with IoT applications that use MANETs in a healthcare setting. As such, a degree of abstraction is necessary and the implementation details must not be dedicated to a particular technology to account for different network infrastructures and BYOD applications. Generally, therefore, the recommendations for the implementation of the IDM framework in healthcare are based on 'best practice' in the area of IDM in general. These include the organisational case, the project plan and the technology case.

5.1 The Organisational Case

The implementation team should take steps to measure or estimate the benefits of linking Things in a healthcare environment (e.g. nurses and doctors, devices and equipment) efficiently in a seamless manner. This will include the following steps:

- The likely improvements in productivity and communication and the reduction in delays through better workflows should be agreed with users and factored into the organisational case;
- The case should identify new and unique efficiency opportunities through improved communications and that would not be possible without using the MANET and IoT;
- The implications of IDM for the organisation for improved security and better data administration (e.g. through a 'single version' of Things) should not be neglected.

The BPM modelling convention [26] would be suitable for modelling these cases.

5.2 The Project Management Case

The implementation of the IDM framework in a typical healthcare application (e.g. an acute hospital) can be regarded as a major project and should be planned as such. The following steps are recommended by the authors:

- Define a standard naming convention and agree the rules around unique identifiers These should be simple but consistent (e.g. doctors = dxxxxxx, nurses = nxxxxx);
- Define a consistent convention for naming organisational roles so that profiles may be defined in advance. This will allow approvals and access priorities to be established and maintained;
- Meta-information should be established for individual roles to allow users to define the roles they need and parameters defined for devices and equipment to allow new devices to be added as needed;
- Define the workflows (see 5.1) in advance as a part of the workflow discussions and reach agreement on the workflow patterns (e.g. with doctors and nurses as well as administrators) in advance. The UML use-case technique [27] is suitable for use in this application.

Proponents of IDM in organisation-wide applications (e.g. ERP systems) recommend that good quality of data is a prerequisite of an IDM system implementation [28].

5.3 The Technology Case

A typical implementation of the IoT using MANETs in healthcare will involve achieving acceptable convergence between various heterogeneous architectures and technologies. The current wireless technologies that are likely to be used in a healthcare MANET are likely to include devices of varying sophistication using RFID, WiFi and 802.15.4 standards and therefore an IP-based solution may be the most feasible solution for implementation on the IoT. An IP-based scheme offers the potential for effective communication between heterogeneous systems (e.g. BYOD and RFID) by providing global unified addressing and routing [29]

The IPv6 standard has potential in applications such as is proposed in this paper, as it includes a scheme for connecting nay heterogeneous devices and uses the packet-switching communication system, which is important in the IoT for compatibility with many existing business applications and achieving compliance with the current Internet communication infrastructure [29]. It also overcomes the restrictions of limited address imposed by the IPv4 standard. Indeed, greater address capacity than is currently provided by IPv6 may be required for full IDM in the IoT, as although IPv6 headers can contain 32bytes of address data, an IoT packet may contain from 20 to 50 bytes. It may be possible to alleviate the problem by developing IPv6 header compression techniques without compromising IP routeing, but it is suggested that more research is needed in this area [29].

Clearly Quality of Service (QoS) is an important issue in using MANETs in the IoT and recent research is suggesting 'best practice' QoS models for use with the IoT that would be compatible with most conceivable MANETs operating in a real-time environment [30]. Communications between smart wireless devices in a healthcare application using the IoT may involve a local wireless sensor network (WSN), wide area 3G and/or 4G communications and an IP routing network. WSN is limited in terms of resource capacity as the network coding increases the complexity as the number of intermediate network nodes increases and in a MANET all the nodes are effectively intermediate nodes [29]. Also, many of the necessary IoT technologies (e.g. RFID and 802.15.4) and use the UHF and MSI frequency bands and are consequently crowded [29] which would be complicated by adding mobile and WLAN healthcare applications on the IoT [29].

New open air interface '3G+' standards such as the Japanese Wideband Code Division Multiple Access (W-CDMA) and the Time Division Synchronous Code Division Multiple Access (TD-SCDMA) scheme recently

introduced in China may have potential for carrying the required communications volume, or 4G LTE (an evolution of the GSM/UMTS standards) may offer the true upgrade potential for the future [31] although it must be noted that current public networks were not designed for IoT real-time applications. In this context it may be worthwhile to revisit existing technologies such as intelligent or Cognitive Radio as a means of enabling the virtualisation of real-world objects and the cognitive management of their virtual counterparts [32]. Although further research and development is needed into these technologies and systems, there is the potential for them to support IDM on the IoT for healthcare applications.

6. Conclusions

This paper introduces an IDM framework which is embedded in a MANET with the assumption that most healthcare devices will be linked wirelessly. The framework will be able to distinguish between users and devices based on personal identifiers, and device profile details respectively. The framework considers the network limitations such as bandwidth etc. by making sure that minimum information is exchanged at one time. A sandboxing technique is employed to protect users' content when sharing a device. We envisage that the behaviour patterns of IDM users could be added to the model. This will allow the IDM system to use the information to compare and identify the user. The proposal in this paper is for an abstract and flexible framework that will be suitable for supporting healthcare applications on the IoT. The paper does not include concrete implementation details, although the main factors that would affect a proposed implementation are discussed and implementation factors such as the business case, project management and technological infrastructures are examined. It is concluded that more research and development will be needed if powerful and durable IoT applications are to run on heterogeneous MANETs in support of healthcare applications.

REFERENCES

[1] Topol, E. The Creative Destruction of Medicine: How the Digital Revolution Will Create Better Health Care. Perseus Books Group , NY, 3- 4. 2012.

[2] Office of National Statistics (ONS), 2006-based Principal Population Projections. 2007.

[3] McGee-Lennon, M.R. and Gray, P.D. Including Stakeholders in the Design of Home Care Systems: Identification and Categorization of Complex User Requirements, INCLUDE Conference, Royal College of Art, London, April. 2007.

[4] Silver, M,. Sakata, T., Hua-Ching S., Herman, C., Dolins, S.B. and O'Shea, M.J. Case study; How to Apply Data Mining Techniques in a Healthcare Data Warehouse. Journal of Healthcare Information Management Vol 15. No. 2. 155-164. 2001.

[5] El Maliki, T. Emerging Security Information, Systems, and Technologies. Proceedings of the International Conference on SecureWare. Valencia. 12-17. 2007.

[6] Gomez-Skarmeta, A.F., Martinez-Julia, P., Girao, J. and Sarma, A. Identity-based Architecture for Secure Communication in the Future Internet. DIM '10 Proceedings of the 6th ACM Workshop on Digital Identity Management. Chicago, 45-48. October 2010.

[7] Pan, J., Jain, R., Paul, S., Bowman, M., Xu, X., Chen, S., MILSA: a Mobility and Multi-homing supporting Identifier Locator Split Architecture for Naming in the Next Generation Internet. In: Proceedings of the Global Communications Conference, USA, IEEE, 2264-2269. Proceedings of the International Conference on Communications, IEEE, 14-18, USA. 2009.

[8] Pan, J., Jain, R. Paul, S., Bowman, M., Xu, X. Chen, S. Enhanced MILSA Architecture for Naming, Addressing, Routing and Security Generation on the Internet. In: Proceedings of the International Conference on Communications, IEEE, USA. 14-18. 2009.

[9] Stoica, I. R. Morris, R. Karger, D. Frans Kaashoek, M. Balakrishnan, H. Chord: A Scalable Peer-to-peer Lookup Service for Internet applications, Sigcomm. 2001.

[10] Cheng, L., Galis, A., Mathieu, B., Jean, K., Ocampo, R., Mamata. L. Self-organising Management Overlays for Future Internet Services. In Proceedings of the 3rd IEEE International Workshop on Modelling Autonomic Communications Environments, p. 74-89, Berlin, 74-89, 2008.

[11] Li T., Design Goals for Scalable Internet Routing. Internet-draft, Internet Research Task Force. 2007.

[12] Sarma, A., Matos, A., Girao, J., Aguiar R.L. Virtual Identity Framework for Telecom Infrastructures, Wireless Personal Communications, 45 (4), Springer. 2008.

[13] Sarma, A., Girao, J. Identities in Future Internet of Things, An International Journal Wireless Personal Communications: Volume 49 Issue 3, May. 2009.