Privacy in the Age of Internet of Things: Challenges and Prospects

Amira Ayadi
Laboratory VPNC, Faculty of Law, Economics and Management of Jendouba,
Avenue U.M.A, 8189 Jendouba, Tunisia
amiraayadi124@gmail.com

Salma Sassi
Laboratory VPNC, Faculty of Law, Economics and Management of Jendouba,
Avenue U.M.A, 8189 Jendouba, Tunisia
Salma.sassi@fsjegj.rnu.tn

Abstract— Technologies change our life. Out of many emerging technologies, Internet of Things (IoT), also known as machine to-machine (M2M) (where smart devices that collect data, relay information to one another. While current information technology enables people to carry out their business virtually at any time in any place. The fact that the personal information can be collected, stored and used without any consent or awareness creates fear for privacy violation for many people. Personal data should be handled under control of individuals to restore the necessary confidence. This paper attempts to put forward architecture to M2M called plug M2M which would address these new threats.

Keywords- M2M, privacy,Plug M2M,SPD.

Introduction

The M2M environment consisted of machine, server, and gateway .It is important to keep an eye on M2M connections especially when most machine exists in the end point that has mobility [1]. It can offer convenience to the user, but someone can have collected information from the machine. Machine must be used only by owner, but someone can search or have access to information that he or she does not have possession of in the M2M environment [2]. This can provoke big privacy problems. Owner can trace the path of a machine movement that can make very serious trouble in the M2M environment,because existent M2M environment does not slacken authentication about a machine [3]. Suppose that a person who has a bad purpose does a machine's position tracing. Then, this person is going to collect position information will damagethe owner.In this paper we will study M2M security problem and our solution in front of this problem.

I. M2M CONTEXT AND ARCHITECTURE

M2M uses a device (sensor, meter, etc.) to capture an 'event' (temperature, inventory level, etc.), which is relayed through a network (wireless, wired or hybrid) to an application (software program), that translates the captured event into meaningful information. (e.g., items need to be restocked) [4] . High-level architecture of the emerging M2M communications consists of threeinterlinked domains: the M2M, network, and application domains [5].

A. M2M domain

In the M2M domain, an M2M area network is potentially formed by a large number of M2M nodes N0, N1,.. and an M2M gateway (GW). Each M2M node Ni is a very flexible and smart device equipped with some specific sensing technology (i.e., body sensors in an e-healthcare system or other types of sensors in environmental surveillance) for realtime monitoring. Once monitoring data are sensed, M2M nodes will make intelligent decision and transmit the sensory data packets to the GW in single-hop or multihop patterns. The M2M gateway GW is an integrated device *[6]*.

B. Network domain

Network Domain is composed of the following elements: Access Network, Core Network, M2M Service Capabilities and M2M applications [7]. In the network domain, the great success of wired networks and the ubiquity of wireless networks provide cost-effective and reliable channels for transmitting the sensory data packets from the M2Mdomain to the application domain.

C. application domain

In the application domain [8], the BS is the key componentfor the whole M2M communications paradigm, which not only forms the data integration point for storing all sensorydata from the M2M domain, but also provides these real-time data to a variety of M2M applications for remote monitoringmanagement.(figure1)

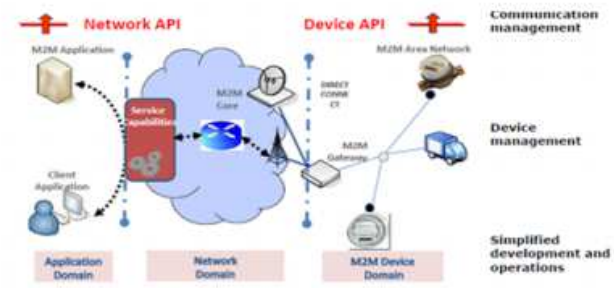

Figure 1:M2M architecture [7]

II. EXISTING SOLUTIONS

978-1-5090-2659-3/17 $31.00 © 2017 IEEE
DOI 10.1109/GSCIT.2016.22

Existing solutions for sharing and processing of data (medical, social, administrative, commercial, professional,
etc.) are typically based on a server approach ensuring consistency and availability of information. These solutions, however, suffer from two deficiencies. The first is the inability to access the data without a reliable connection, secure, permanent and fast server, a set of conditions difficult to meet in all environments. The second is the distrust of users to centrally manage their personal data. This distrust can be explained as much by the lack of security guarantees once the data leaves the secure area of the server by the user to lose control of how their data is shared and used by different actors. So a decentralize server can solve those problem.(table 1).

Tableau 1:COMPARATIVE TABLE CENTRALISE AND DECENTRALISE SERVER

	Centralize server		Decentralize server	
DB Stockage	Centralize	Decentralize	Centralize	Decentralize
	*			*
Authentification	yes	no	yes	no
	*		*	
Acces control	yes	no	yes	no
	*		*	
administration	administrator	custmer	administrator	custmer
	*			*
creator	IBM	Other	IBM	Other
	*		*	
computing power	Big	Small	Big	Small
		*	*	
perfermance	Hight	law	Hightt	law
		*	*	
Servers Number	One	Many	One	Many
	*			*
Cost	Expensive	Sheep	Expensive	Sheep
	*			*
DB	Hippocratic	Embedded	Hippocratic	Embedded
	*			*

A. Centralise server

Centralise server is a mechanism that stores all the data on a server for all elements of the computer network. The location of a single server or a central data server involves the daily absence of the individual; it can neither administer his data. Individual data has no authority over its data personnel. A central server is managed by a system administrator. System Administrator refers to the person responsible for the servers in an organization (company, association, administration).
This administrator manages the authentication gives access authorization to resources and data. And it also manages access control, which is to verify whether an entity (a person, a computer ...) requesting access to a resource has the rights to do so. It has a large storage capacity and computing power over at least preferment .the cost of a central server is very expensive about 10 times the cost of a decentralized server .to manage the sql queries the central server is implemented by Hippocratic DBMS that provides a set of founding principlesand mechanisms to protect the private data of individuals ina database. Users connected to the central server an entity by a computer terminal. This convenient structure for the organization, however, poses network security problems if the central server fails the entire network no longer works. But still, for pirates, there is only one target, and finally saturation of the central server if there are too many simultaneous connections. The location of a single server or a central data server involves the daily absence of the individual; it can neither administer his data. Individual data has no authority over its data personnel.

B. Decentralise server

Trusted devices is emerging and radically changing the way personal data management. Decentralized server (secure device) consists of a smart card, a secure key, and USB), secure chips combine hardware security chip, memory storage capacity in a flash Nand and communicate by a USB protocol. [9] Personal data can be managed under the owner's control (customers). Customers manage authentication and access control. To manage its sql queries the personal data server has an embedded DBMS as a software component that consists of a software library linked with the software. Decentralized erver has a low cost and hight level of data security. Such server first supplies of the main features of a database engine (data structure, access control, interrogation facilities and transactions) and are interoperable with existing data sources and with other users. Also it allow the user to control the sharing of their data (which data, with whom, for how long, for what purposes) .Finally it guarantee the principles of respect for privacy (consent, collection and retention minimum, audit) for its own data and those belonging to others, and guarantee the a high level of security and offer a disconnected access to data that might get with a typical server.

III. PLUG M2M OBJECTIVE

The objective of the plug implementing a SPD into M2M architecture is design and testing technologies for ubiquitous and secure management of personal data. The existing architecture of M2M system sharing and processing of data (medical, social, administrative, commercial, professional, etc.) are typically based on a server approach ensuring consistency and availability of information. Unlike traditional smart card, the storage memory of an SPD is not protected against physical attacks threatening the privacy and integrity of the embedded data. We must therefore develop cryptographic protocols to resist these attacks while remaining compatible with efficient embedded databases treatments. The SPD has microcontroller meanwhile the same safety characteristics as that of a smart card. One can imagine using it as secure coprocessor to protect the data from the SPD and hosted on a vulnerable device or to establish a secure exchange scheme in a circle of trust where each member has a SPD.

IV. THE SCHORTCOMING OF THE M2M ARCHITECTURE

To address these shortcomings, the new M2M architecture is built around a new hardware component called here SPD. SPD combines the intrinsic security of a smart card with the storage capacity of a USB key (several gigabytes futures) and universality USB (playback from any device connected to a port USB: workstation, laptop, cell phone, etc.). The innovative character of the project lies in the marriage of sophisticated techniques embedded data and cryptographic protocols to database management on an SPD media type. The goal is not to replace a server approach but to supplement it with new techniques meeting the two identified deficiencies. In particular, an SPD can host a replica of all or part of a personal data file managed by a server to allow for offline processing. Moreover, the SPD security capabilities can be leveraged to implement new data-sharing schemes, highly secure and controlled directly by the user.

V. PLUG M2M DESCRIPTION

We illustrate below how the SPD technology can respond to the problem. The principle is the following. We assume that each user U has a personal data record SPD managed by a media server. The SPD contains the U certificate to strong authentication to the server when accessing his file in connected mode. The SPD also contains a replica of the U's personnel file and embedded software components (including Web server and DBMS) giving access to the file offline, from any device with a USB port and a web browser.(figure2)

Figure 2:actors of system

A. UserU

person who want to establish an access control policy to his data For U can exchange data with P partners, they must also be equipped with a customized SPD. The SPD of a partner P is similar to that of U software and hardware point of view, but its role in interactions with the U-file is special. P undergoes set by U access control policy.

B. Partner P

person authorized to have access to the User data U.

VI. USER AND PARTNER AUTHORIZATION

If P decides to replicate on his terminal, for example to access in offline mode without the presence of U, this data will be encrypted with a key known only SPD P. When P questioned these data, the embedded DBMS in its SPD accesses and decrypts the response to the query. The difference between U to drop data unencrypted or encrypted format on the supporting servers is as follows. In the first,case data sharing is controlled by the access to which U control policy agreed.(figure3)

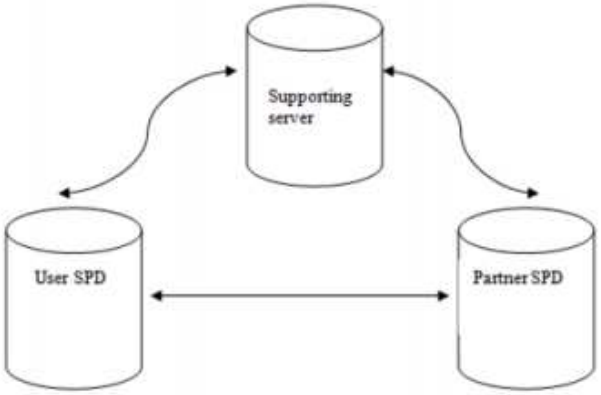

Figure 3:Supporting server in relation with SPD

In the second case, the access control policy is coupled with a physical sharing obligation of encryption keys, sharing that can be organized by name and that under the total control of U.To organize sharing, U user can choose different status for its data.(figure4)

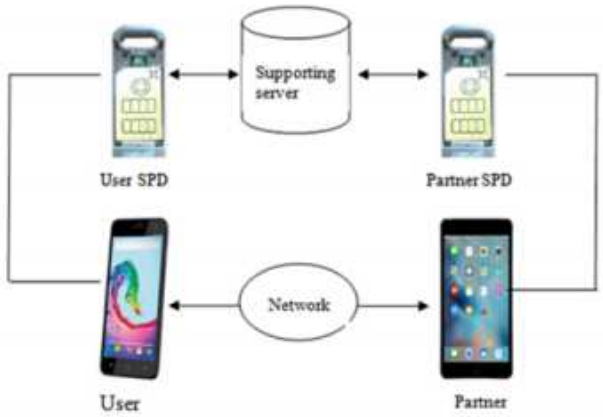

Figure 4: communication between user and partner

VII. DATA CLASSIFICATION IN PLUG M2M

User can classify this data into four types of data: data regular data, secret data, Sustainable secret data and limited data[?].

A. Regular data

Regular say data is replicated to the support server and embedded server, protected by the same access control policy. The motivation to replicate regular data in the embedded file

is to ensure availability offline. Its data are explained in the contract by standard items.

B. Secret data

The so-called secret data is only stored on the SPD U. Just as for a paper record, U guard the freedom of access to its SPD, so the secret data, the partner he physically P in front of him. It is guaranteed that nobody can access the data without its knowledge. Sustainability remains secret data by against the U. load its data is explained in the contract by time items.

C. Sustainable secret data

These secret data replicated to the central server in a format encrypted by encryption keys known only to the SPD U. The server ensures durability as well as for regular but keeps the data U guarantee that no one can access that data without holding the SPD U. only the sustainability of encryption keys remains the responsibility of U.ses data are explained in the contract by exceptional items.

D. Limited data

This is data that U wants to share exclusively with a small circle of trusted partners P, with the guarantee that no one else can access this data. To do this, U deposited on the central server via the SPT, the figures whose keys are known exclusively by TPS confiance.ses circle data is explained in the contract by standard items. At any time, U retains the possibility to change the status of its data. If it is possible to lower the security level of a given for easy sharing, the reverse process is more uncertain. For example, given that the regular secret we would have already passed through a shared state, and therefore have been accessed, copied, etc. Beyond the implementation of a more controlled consent by the user, these statutes also control the data retention period, at least until they have been placed in the state of regular data.

VIII. ARCHITECTURE DESCRIPTION

This architecture focuses on the integration of portable equipment in a global infrastructure. The principle of secure portable record may indeed be conceived in isolation.(figure5) The contents of a portable file intended to be integrated into a comprehensive information system that feeds or be powered by it. In addition, any portable equipment has an intrinsic vulnerability to risk of loss, theft or destruction, requiring replication of data on a server to ensure sustainability and availability. This raises the problem of integration of mobile equipment and its contents in a global infrastructure, the latter must be done transparently and without compromising data security.

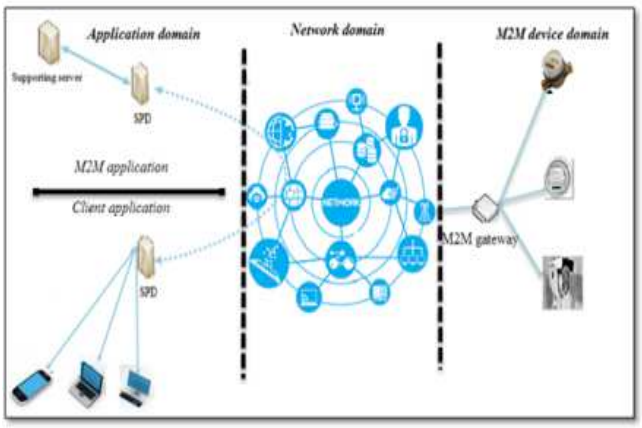

Figure 5:proposal architecture

A. contract structure

The Device and Gateway Domain are composed of the following elements: M2M Device, M2M Area Network and M2M Gateway.

B. Network domain

The Network Domain is composed of the following elements: Access Network, Core Network, M2M Service Capabilities and M2M applications.

C. Application domain

The back up server will be changed by a supporting server in coordination with personal server data.

IX. PLUG M2M THE PRINCIPLES

The user of plug M2M will draw up a contract to describe the set of access permissions and access constraints to the SPD by partner.

A. Contract structure

The contract is an agreement which creates obligations and permissions, which means a voluntary agreement between the owner of SPD and partner want to access to owner data. This contract contains three types of articles .First standards articles, second Exceptional articles and finally temporal articles.(figure6)

1. Standards articles

The Standards articles of the contract are set by one of the parties User and the other party partner that has little or no ability to negotiate more favorable terms. So Standards articles are shared by all people. In standards articles we differentiates between standard obligation and standard permission.

2. Exceptionals articles

User formatted an exception access to partner. Those articles do not apply to all partners.

3. Temporal articles

The access of partner is relating to the sequence of time, to a particular time or to a period of time.

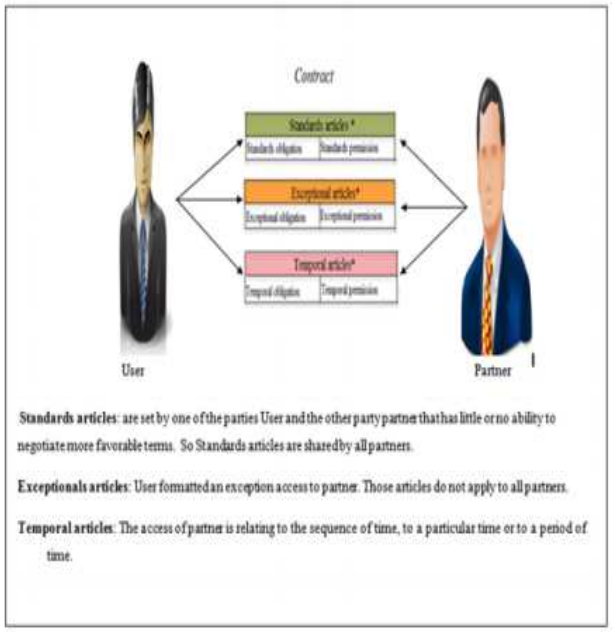

Figure 6: contract between owner of SPD and Partner

X. EXPERIMENTATION

We will implement this architecture on a medical scenario.

Actors of this architecture are:
Patient has medical examinations, treatment by a doctor or other health professionals to deal with an illness or injury.

Doctor coordinates all the care data received by the patient.

Doctor directs patient if necessary to a specialist doctor. A health professional s or injury.Doctor is person exercises its powers to the treatment or care of individuals injured and sick. A health professional can be a nurse, specialist doctor, biologist, gynecologist, etc.

Specialist doctor is a doctor that performs a special function and he understands better patient illness. The biologist in specializing in medical analyzes of biological fluids then he interprets the results. The gynecologist medical and surgical specialty, deals with the physiology and diseases of the female reproductive system.

XI. SCENARIO

A. Recording doctor in Plug M2M

First doctor must be part of the system. To perform the registration task doctor must fill the form that contains his training and his experience (figure7). Once the form is completed the doctor becomes a member of the system and he will obtain an SPD.

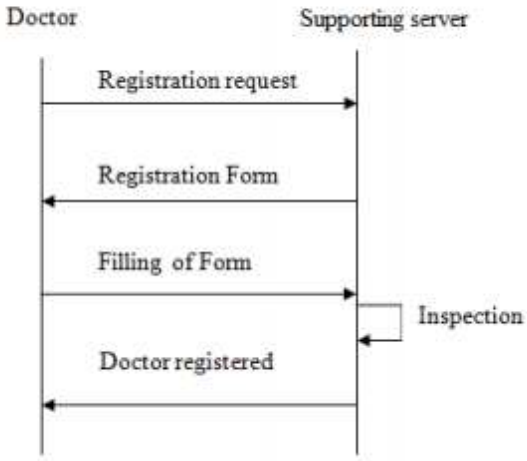

Figure 7 :Doctor recording

B. Recording patient in Plug M2M

The patient also must be part of the system. To perform the registration task patient must fill the form that contains information and data about his disease. Once the form is completed patient become a member of the system and he will obtain an SPD(figure8).

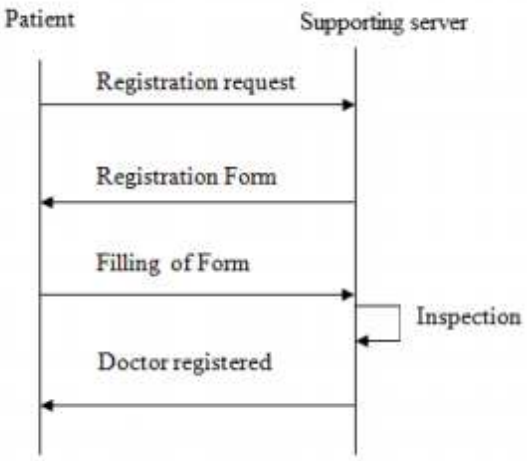

Figure 8:Patient recording

C. Drafting of the contract

The first owners of a SPD, the patient and the doctor, will draw up a contract to describe the set of access permissions and access constraints to the SPD by other health professionals. The doctor has a big role in the management of SPD, this role is given by patient. The contract require to doctor and patient, to give, to do or not to do something, to health professional. This contract contains three types of articles .First standards articles, second Exceptional articles and finally temporal articles.

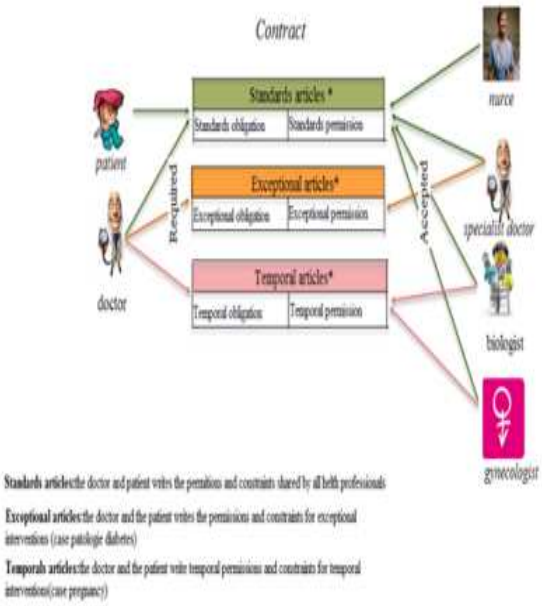

Figure 9:contract structure

D. Standards articles

In standards articles we differentiates between standard obligation and standard permission.

•Standard obligation

something that health professionals must do because of rule and constraint putted by patient and doctor. Patient and the doctor set the following obligations:

*Health professional must respect life and dignity of the patient.

*Health professional must respect principles of morality and probity.

*Health professional must respect professional secrecy.

*Health professional prohibit advertising patient secret.

*Health professional has the primary duty to protect and promote the health and well-being of patient.

Standard permission

The right or ability to do something that is given by patient and doctor who has the power to decide if it will be allowed or permitted to access to patient data or information. Patient and the doctor set the following

• Standards permission

*Health professional participate in medical consultation, prescription drugs or treatments, radiotherapy, practice accouchement, making a diagnosis, treatment of disease.

*Health professional determines the reason that causes the patient to consult.

*Health professional establishes a treatment plan that includes the patient.

*Health professional refers to anther health professional or working with them as needed.

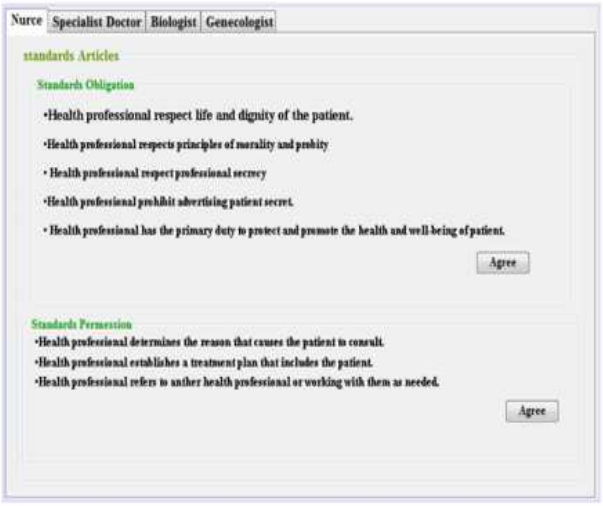

Figure 10:standards articles

E. Exceptional articles

Patient and doctor formatted an exception access to health professionals.

Those articles do not apply to all health professionals, but rather the specialist doctor.

• Exceptional obligation

*Specialist doctor makes rigorous monitoring.

*Specialist doctor plan the flow of his treatment plan in a care path.

• Exceptional permissions

*Specialist doctor established a diagnostic.

*Specialist doctor implements appropriate treatment.

*Specialist doctor improve the quality of care.

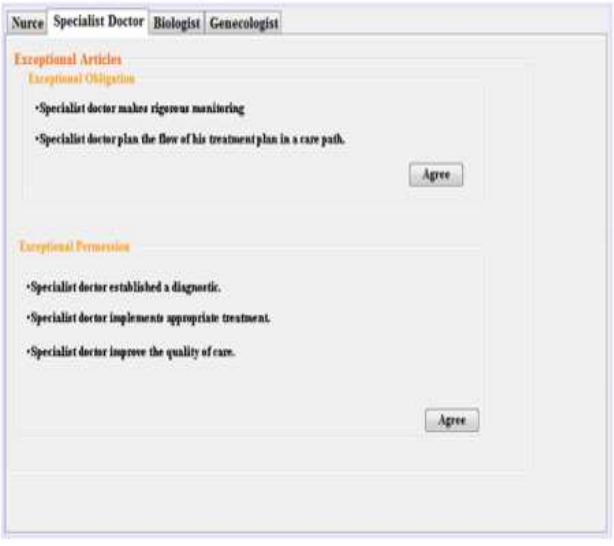

Figure 11:Exceptional articles

F. Temporal articles

The access of health professional is relating to the sequence
of time, to a particular time or to a period of time Those articles apply to the biologist and the gynecologist at time.

• Temporal obligation to biologist

*Biologist achieves and monitors the implementation of acts of medical biology.

*Biologist interprets the results valid to participate in medical
diagnosis and monitoring of patients.

• permission to biologist

*Biologist gives advice which is particularly valuable for people with long-term illnesses.

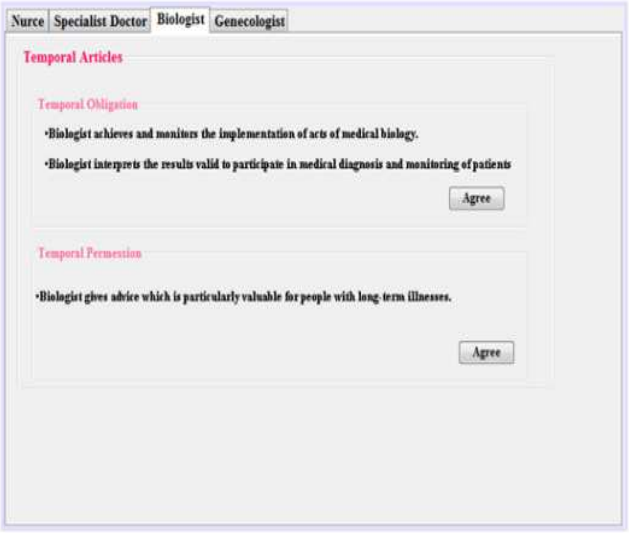

Figure 12:temporal articles

Conclusion

The present paper show the benefits of SPD in terms of
privacy protection and pervasiveness. The M2M architecture is composed of a set of SPD (one for each member of atrusted circle), a used as a terminal to interact with each SPD and a supporting server used for durability and availability purposes of durable and restricted data.

REFERENCES

[1] R. E. Balfour, "Building the internet of everything(ioe) for first responders," in Systems, Applications and Technology Conference (LISAT), 2015 IEEE Long Island. IEEE, 2015, pp. 1–6.

[2] J.-M. Kim, H.-Y. Jeong, and B.-H. Hong, "A study of privacy problem solving using device and user authentication for m2m environments," Security and Communication Networks, vol. 7, no. 10, pp. 1528–1535, 2014.

[3] J. R. Quinlan, C4. 5: programs for machine learning. Elsevier, 2014.

[4] D. Boneh, G. Di Crescenzo, R. Ostrovsky, and G. Persiano, "Public key
encryption with keyword search," in Advances in Cryptology-Eurocrypt
2004. Springer, 2004, pp. 506–522.

[5] M. Sneps-Sneppe and D. Namiot, "Micro-service architecture for emerging telecom applications," International Journal of Open Information
Technologies, vol. 2, no. 11, pp. 34–38, 2014.

[6] S. de Capitani di Vimercati, S. Foresti, G. Livraga, and P. Samarati, "Anonymization of statistical data," it-Information Technology Methoden
und innovative Anwendungen der Informatik und Informationstechnik, vol. 53, no. 1, pp. 18–25, 2011.

[7] R. Lu, X. Li, X. Liang, X. S. Shen, and X. Lin, "Grs: The green, reliability, and security of emerging machine to machine communications,"
Communications Magazine, IEEE, vol. 49, no. 4, pp. 28–35, 2011.

[8] D. Boswarthick, O. Elloumi, and O. Hersent, M2M communications: a
systems approach. John Wiley & Sons, 2012.

[9] L. Le Folgoc, "Personal data server engine design and performance
considerations," Ph.D. dissertation, universite de Versailles Saint-Quentin, ´2012.4, doi:10.1109/SCIS.2007.357670.