Traceability versus Privacy: A Flow Model Perspective

Abdulrahman R. Alazmi

Abstract—Traceability of objects or persons is the ability to track a certain target, its movements, its actions, and be able to locate it during the surveillance period. By definition, traceability contradicts that of Privacy. Privacy of objects or persons insures the confidentiality and discreetness of the targets' whereabouts, their actions, and current locations. With the inception of Ubiquitous Computing UC technologies, such as Location Based Services LBSs, tracking and monitoring in Mobile Ad hoc Networks MANETs and Vehicle Ad hoc Networks VANETs, and/or Biometric Identification, both *traceability* and *privacy* could be either *maintained* or *violated*, because objects and persons can be tracked and or protected using UC applications. As the objectives of both terms Traceability and Privacy collide in UC applications, a rise in the need of providing a model to verify that each term's goals do not contradict one another by drawing lines and/or providing channels or solutions to insure equilibrium on both sides of the equation.

Index Terms— Ad hoc networks, flow-thing model, mobility, privacy, system modelling, traceability, ubiquitous computing.

1 Introduction

Smart technology has made its way into almost every electronic device in the present time. It is almost natural to see everyday electronics making the jump. By Smart we mean that a device can process, store, and collect data. Mobile phones have been transformed from communication devices into full-fledged smart devices. They can locate their user, collect data from the internet, Geographical Positioning System GPS, send and receive, and detect signals. Advancements in nano technology have enabled very small processors that require, very small space, power, and have low battery usage, and heat emissions, have made the tiniest sensors to be very accurate, capable, and resilient. These sensors can track the movement of persons, or objects with special tags (Electromagnetic EM bars, or Radio Frequency Identification Devices RFIDs). And so a simple form of a traceability system is a group of sensors in a given area. Existing traceability systems strive for linking actions to a source, monitoring targets, or locating and authenticating objects or persons using their personal identifiers, such as their fingerprint, retina, serial number, or face recognition. These systems' objective is to be able to trace their targets. UC technologies have paved the way for monitoring, tracking, as well as tracing systems to be elaborate, distributed, and be available almost in any time (e.g. cameras, low power devices, and small sensors, RFIDs, wireless communication networks, GPSs). UC usage can be seen in material management, supply chain management, health care sectors, and identification of individuals [1], and continually making the internet an Internet of Things.

While the purpose, and usage of such systems is meant to be benign, and to help users complete more tasks, and insure quality of work and proof of existence in work environments. This advancement however, might be unwelcomed in the privacy, security, and anonymity world. Because such systems can store sensitive data about individuals (e.g. their names, current location, current actions), or objects (e.g. the owner might not be aware that his/her object is being tracked, which may lead to the tracking of the owner as well). And with questionable security measures, this contradicts directly with the use of privacy measures or systems (users are not tracked, sensitive information regarding people, objects is handled with care, all use of private information is seen and known to participating parties.)

According to [2], some of the privacy concerns in UC are inappropriate usage of the collected data, and the UC system dissemination of the users' data to other users, without the knowledge or consent of the users themselves. An example is an employee in a UC environment who is being monitored, his/her actions, and movement are all being tracked by a UC system [3]. Another is the tracing of an object such as a book in a library, its circulation, and current location can be known using the tracking system. In the first example, privacy is clearly being violated, as an employee might not want to be tracked during the working hours. The latter example might also violate the borrower's privacy, if it can track the book in a specific environment, the campus for the library for example, but to a lesser degree.

The answer to this problem might lie in the foundation of a privacy-aware tracking system, in which both goals of traceability and privacy concerns are met. How can such a system be made? By providing a modeling method, as well as the utilization of privacy protection techniques, such as Separation of Duties SoD, privacy aware environments, and/or encryption protocols, into these systems we can have a privacy-aware tracking system. In this paper, the proposed method will utilize the Flow-thing Model FM, proposed by S. Al-Fedaghi in [4], in order to verify the usage of data and its flow among tracking systems to allow us to find or point out privacy concerns.

This paper is organized as follows: in Section II, review of the works on traceability and privacy systems, and how to

• *A. Alazmi is working in the field of RFID and items inventory, security and managament at Kuwait University. E-mail: abdulrahmanr.alazmi@ku.edu.kw*

provide both in the infrastructures of UC systems will be given. Section III sheds light on the FM model and how to use it to display data usage and dissemination. Then, in Section IV, a case study is given to highlight the privacy issues in tracking systems, and in Section V, the proposed model which is the modified system discussed in the case study (with FM) will be used to pinpoint the privacy problems, and extract solutions. Finally, Section VI gives the concluding remarks found throughout the research done in this paper.

2 Previous Work

In Ref. [3], the authors face the problem of traceability and privacy. The paper defines the goals of privacy and traceability in the light of Ubiquitous Computing. The goals of both traceability and privacy are contradictory still. UC can be viewed as the infrastructure for computing devices that are ubiquitous and are there, almost everywhere. These computing elements are also invisible, and can sense their environments and collect data and save it, and hence their potential benefits and threatens for both traceability and privacy, respectively. The paper defines an architecture that would strike a balance in between both the traceability and privacy goals of Ubiquitous Computing environments. The architecture is made out of several elements, which are a Sensor Manager, Context Server; Access Control; Identity Management; Virtual Environment, and a Transparency Management. The first, the Sensor Manager, is responsible for gathering and managing every sensor unit, it collect the sum of information and interoperates them with the Context Server. The second element, Context Server, is responsible for creating the data about the objects and individuals; it can store and process this data. The third, the Access Control, this component is situated on top of the Context Server and it governs the access to the data in it. It can be tuned to allow sets of data to be accessed selectively, such as sensitive and non-sensitive data can be filtered. The fourth component, which is the Identity Management, is responsible for managing the users for these environments. Through the Identity Manager allows the users to configure their setting for traceability and privacy. The fifth component, which is the Virtual Environment, which provides a layer for the system to and an outside body, using this layer allows for system data to be secured before it is transported to a different outside body, such as a third party organization. Sensitive data can be selected as not to be transported. The sixth and final element, the Transparency Manager audits the access to private data. This component is essential to ensure privacy for individuals from the users of the system, such as companies and governments. While the paper provides robust system architecture, it does not provide a model to capture the weaknesses in current UC systems, nor does it provide an information flow for its novel system architecture. In this paper, these shortcomings will be overcome, while adapting some components of this architecture. The paper also discussed several architectures that provide privacy in tracing and UC systems, such as Mix Zones, Spatial and Temporal Cloaking, and Virtual Walls [3].

Methods have been proposed in order to preserve a level of privacy in environments where traceability is a perquisite, environments such as MANETs and VANETs [5] [6]. For VANETs, in [7], a protocol that provides privacy in the authentication process is proposed. In VANETs, vehicles are authenticated, and monitored by the infrastructure through Road Side Units RSAs, which are scattered across the road. These provide the sensors for the VANETs. Vehicles are equipped with computing devices that allow for communication with RSAs, such as communicating when entering and leaving the VANET. The privacy issue comes into play when we consider the nature of the RSAs. Since vehicles enter and exit the VANET very quickly, the RSAs job of authentication, especially given the amount of traffic and the very little allotted time for a RSA. Given their high number, their low cost is required, which entails their simplicity in structure. This enables for easy tampering of their data, or even compromising them with fake RSAs. The proposed method suggests the use of public key encryption in VANETs. Utilizing hierarchy of Trusted Authorities TAs, a TA, then a State TA STA, and finally a City TA CTA, this will elevate the demeaning computational overhead from the RSAs and unto more capable units. Privacy is insured since public key cryptography is highly used in almost every type of communication technology protocol.

Another proposed method for VANETs is given in [8], where a privacy preserving authentication protocol is proposed for VANETs. The proposed protocol uses a mutual-authentication protocol that allows for a privacy-preserving VANET, through anonymous communication. The method utilizes a Trusted Center TC in the VANET, where only this entity knows the identity of the participating vehicles in its domain. Therefore any other communication between vehicle to vehicle, or vehicle to any road side unit would be anonymous communication. Public key is also in use in this method. The problem faced in the proposed method is the additional delay made by the introduction of levels in which certification go through.

In Ref. [9], the paper vision of the UC future might as well parallel that of Ohm's nightmare scenario [10]. In which an adversary, or an authority body, given enough information found on the internet, databases, or any other source (most probably the data banks of a UC system), this foe or controlling body can use this information through re-identification methods (de-anonymization) [11] [12], to harass individuals, blackmail them, or geographically identify them and may physically bring harm to them. The paper proposes Privacy Awareness System pawS, which relies on democratic basis of rules, where people are expected to respect the others safety, freedom, and privacy. This is done by utilization of law enforcement, social etiquette, and legal laws. Similar to, as the author claims, traffic laws and monetary laws, social and lawful laws and norms facilitate them. pawS is a set of tools and collections, used by such UC systems, while utilizing pawS, the data subjects need to be notified about their the data collected about them. This holds the UC system's implementing pawS to be accountable against the law if a privacy breach is done to an individual or a group of individuals. pawS also

utilizes anonymity and encryption as well by the compatible system. Using Platform for Privacy Preferences Project (P3P) privacy policies the user can decide to what level he/she wants to be tracked, these services are integrated in pawS. These privacy policies are also stored along with the user data, in order to allow accountability for each set of data collected from the same user. This, however, is not enough, because the systems main infrastructure is still in danger of hackers' attacks, which can still compromise our privacy, but at least not from within the system itself. While pawS provide a sufficient infrastructure, problem arise from the fact that extra pawS hardware must be used (e.g.: pawDB), and pawS allow for privacy enabling method, but cannot guarantee the architecture to be protected against hackers. The idea behind pawS is to merge private data into metadata, such as with Digital Right Management DRM.

Legal and privacy issues of UC can be found in [1]. The German Federal Constitutional Court has pointed out some point in order to that would adhere to the privacy issue in UC. These points do come in conflict with the definition of UC, and they can be summarized as follows:

- Limiting the data collection conflict the UC goal to be invisible, ready, and loaded with information to help users
- Users' need of viewing data collected about them conflicts with the data amount and processing procedures
- Since UC systems are spread over a myriad of systems, locations, devices, and even people. It is difficult to find a single body accountable for legal issues

The paper also lists the potentials and future problems that might arise if there were no policies to govern and solve privacy issues in UC systems. The potentials are: large companies would integrate UC system (which includes traceability systems by default) into their architectures, these large bodies would then provide these services to smaller companies, and so UC will see huge market penetration, and with it privacy is at risk. The problems include: the increased complexity of UC systems makes it difficult for users and systems to insure private handling of the data. The paper claims that a modeling schema that enables formal specifications for the balancing of both traceability and privacy are met, and privacy is insured and intact in these systems.

Preventive measure for UC systems include Observation and monitoring [13], authentication, and privacy aware protocols [14], Securing existing UC systems such as RFID systems [15], Anonymization and encryption [1], and utilizing privacy policies [9] [16], where users select the level of privacy they want and are legally accountable of. The key in providing and meeting requirements lies in a system model that will enable for information flow elements, and in doing so, enables modelers to identify privacy risks in traceability systems such as UC systems.

3 Model Analysis

In order to provide a model to verify or evaluate the privacy awareness, or potential privacy concerns, in traceability systems and UC applications, the proposed model will use the FM [4]. Proposed by Al-Fedaghi, FM has seen a wide area of usage, such as in database access control, software engineering, web applications, and information security [17] [18] [19] [20]. It is inspired by the flow that naturally exist among many entities whether concrete or abstract, such as those in supply chain management, or in computer science in the Shannon-Weaver's communication model. FM is a diagrammatic model, in which flow-things, which can be the system's components, signals, or maybe information itself, trigger events or exchange data among one another. An FM model, shown in Fig. 1, is a collection of one or more than one flowsystem. A Flowsystem can include up to 6 stages or states, plus an extra 7th one. These are:

- Arrive: a flow-thing has arrived at the flowsystem
- Accepted: it is allowed to enter the flowsystem
- Processed: a flow-thing is changed or transformed from its original state
- Released: a flow-thing is ready to leave the flowsystem
- Created: a new flow-thing is made inside the flowsystem
- Transferred: a flow-thing is leaving the flowsystem
- These states can be added by one which is Storage; this can represent a flow-thing which is being stored in a state inside the flowsystem.

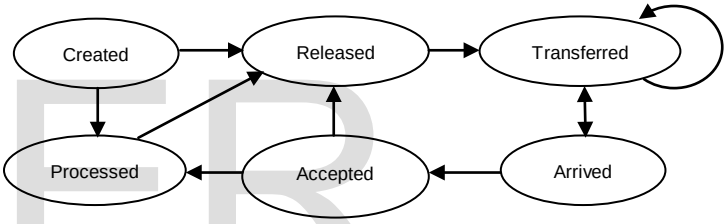

Fig. 1. The FM model

Fig. 1 shows the general FM model. Of course, the FM model can be customized by removing states, adding states, or changing the way these state communicate. For example, a flowsystem might not process data, and simply collects it, verifies it, and then pass it to another flowsystem; in this case, we would have Arrived, Accepted, and Released. This high level of flexibility allows the modeler to convey the system flow of information with clarity, and the triggering of events, indicated by the dashed arrows (not shown in Fig. 1), allow showing that data flow affects events in the system as well. In addition, a single entity can include more than one flowsystem.

Privacy breaches that are made in systems that collect sensitive data can be detected if we can find components that might store, process, or transfer these data sets on non-trusted links. If a modeler uses FM to illustrate such data exchange, with good knowledge of how the system communicates, security and privacy risks can be detected. From Ref. [3], the proposed model will borrow architectural elements, such as the Identity Manager, Context Manager, Virtual Environments, and the Transparency Manager. The proposed model will try to overcome privacy threats, and identify them.

4 Case Study

The UC system given in [21] will be used as the case study. In this paper, the details of implementation of the system will not

be discussed, but will only use the actual hardware and software architecture in order to show the possible privacy threats by using FM modeling. Moreover, in the next section, section V Results, the FM will be used in applying the proposed model presented in [3], in order to overcome the privacy threats in the system. The objective is to illustrate FM prowess in modeling privacy threats in UC systems.

Health care sector is one of the best candidates for UC systems, and one with privacy perils as well [1] [22]. The proposed UC system, in [21], is a health monitoring system. Its environment imply its critical and private functions, it is composed of a group of health monitoring sensors that are able to connect to the Wireless Area Network WAN in the hospital. All the sensors' collected data are sent to a medical server. The sensors use Zigbee and Bluetooth as well to transfer their data. The medical server keeps the records of the patients, processes and monitors the uploaded data, and allows users to access the data. It is also responsible for authenticating users, and monitors health thresholds in order to give warnings and alarms. The system architecture is given in Fig. 2.

Fig. 2 shows the Health Monitoring System. It can be segmented into 4 sections. Part (1) is the Hospital area, where sensors collect data and PDAs can access the collected data. Part (2) is the Wireless WAN, where all gathered data is being transferred to the network. Part (3) is the Internet, where the data is uploaded to the Medical Server to be processed, and be available for the Health Care Providers. Part (4) is the final section and where data is available for the end users, such as patients, medical staff, and outside users. In Fig. 3, we apply the FM to the system in [21], shown in Fig. 2. Since the model is too detailed, the model shall use the sectioning parts to show Fig. 2 in parts using FM. In each part, a flowsystem is used, and for simplicity, the model shall consider one flowsystem for each section.

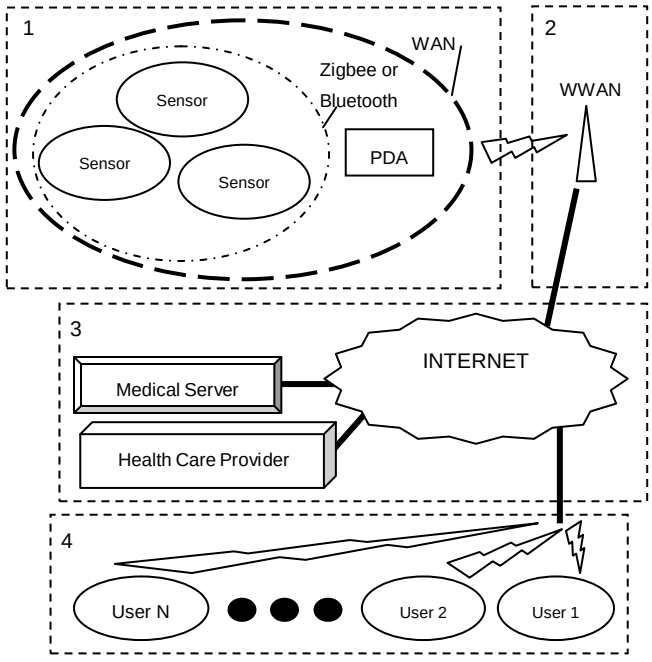

Fig. 2. Health Monitoring System, from [21]

In Fig. 3, for the first part (1), we can see that the sensors can collect data (Create), and then either sending it to part (2) or to other points of sensors and finally sending it out to (2) (Released and Transferred). For part (2); the WWAN can only receive the data and then transfer and release it. For part (3); the Internet and Medical Server, they accept the data, validate it, and process it as well. Finally they can transfer it or release it to the users in part (4). Finally in part (4); the end users can accept the data, release and transfer it. From a privacy point of view, we can see from FM that there are several points that may lead to privacy breaches in the system. For part (1); the state of Transfer suggests that the data is circulated between the sensors. Given how poor the security is in MANETs [5] [6], this could pose a huge privacy risk. Part (2), has also the Transfer state, but since this is done using hardware more complicated than simple sensors, such as gates, switches, and wireless antennas, so standard network measures against intruders should be used to reduce privacy risks. In part (3); the Internet and the Server level, because data is Processed here, this poses threats on the data privacy. For example, threats can be from the Medical Server users themselves, or from third party Health Care Providers. And for part (4); users can view, release and transfer the data sets. If users are limited to a set of anonymized or small public data sets, this will not be a privacy threat. However, if users can access private data, regardless of the standard authentication procedures, this could pose privacy threats as well, if further levels of security are not used. Table 1, has the possible privacy threats that are in the Health Monitoring System of [21]. Using FM in Fig. 3, potential threats can be identified (e.g.: part 1 Transfer and Release datum to part 2 using WAN, and collects data, Create and Accept, using Zigbee and Bluetooth).

5 Results

Continuing the example in the last section, in this section the proposed architecture given in [3], will be used to remedy the privacy holes discovered in section IV, in Fig. 2 and Fig. 3. FM will also make a presence after the application of the privacy aware architecture. Since the architecture of [3] is elaborate and consists of six main components, the proposed model shall not use all these components, and instead use only what is needed. Assumptions can also be made, in order to minimize the complexity and lessen the amount of added components. This addition will help in solving the privacy problems found in the UC and traceability system of the Health Care System in [21], because the architecture has been proposed to solve common UC systems' privacy problems that are sometimes overlooked. After the addition, FM will also be applied to highlight the solved privacy issues

The proposed privacy-aware architecture of [3], which is also discussed and explained in Section II, consists of 6 components; they are the Sensor Manager; Context Manager; Access Control; Identity Manager; Virtual Environment; and Transparency Manager. The first, which is the Sensor Manager, is responsible for managing the sensors. The proposed model assumes that the Health Care UC system has already integrated Sensor Manager with integrated security measures. For the

second component, the Context Manager, which creates and process data, it is already there in the system in part (3) of Fig. 2 (the Network and Medical Server). Component 3, the Access Control and component 4, the Identity Manager, are responsible for granting permissions and authenticating the users, these will be added and separated. Virtual Environment, which is component 5, will also be added, because it is responsible for securing third party access to the system data, through secure and controlled channels. The sixth and final component, the Transparency Manager, which audits and logs every data access and modification, will also be added to the Health Monitoring system. Fig. 4 shows the proposed model which is the modified system of [21], with privacy-aware architecture from [3], and the added assumptions.

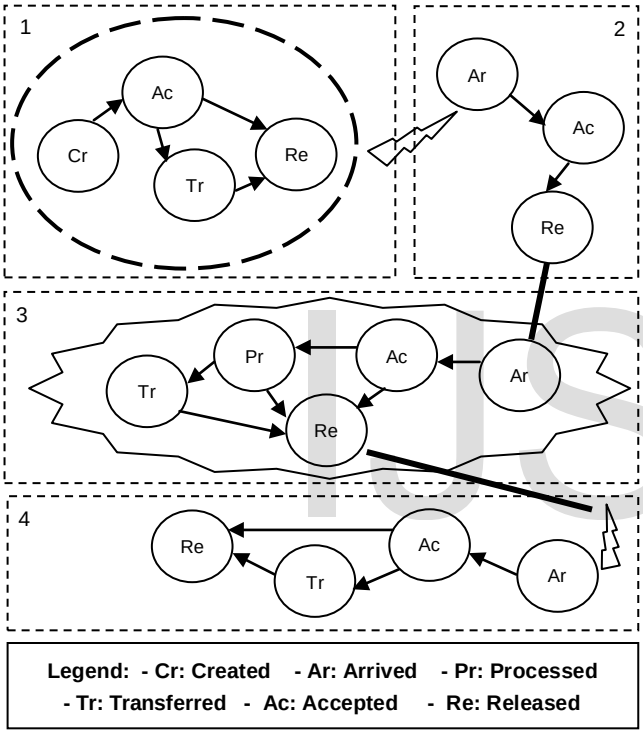

Fig. 3. FM for the Health Care Monitoring System

Fig. 4 shows all the additional components that were added, and these are in part (3) and (4) from the original model. Context Manager has been added to part (3), in order to add the processing prowess for the system, after that the Identity Manager was added in the same section, part (3). The Identity Manager will work on authenticating the users; it can be even by a physical device such as an electronic card. It can also provide privacy policies, in which users can decide the level of privacy they would expect or want by committing to a privacy policy. Also in part (3), and (4), two more components were, and they are the Virtual Environment and the Transparency Manager. The first is used for making interaction with third parties (e.g. Health Care Providers) more secure and safe. Via using, secure channels, such as HTTPS, along with precautions, such as limiting their view of the data the Medical Server processes. This would help keep malware a step behind the raw data in the Medical Server. The Transparency Manager will provide the auditing and logging needed in case of a privacy threat occurred on the behalf of the end users. For example, if a user reports that his/her data has been published, abused, or misused in any form. The logs can easily track the perpetrator, and help in preventing further privacy breaches. The last two components work at both sections (3) and (4), so both the privileged users at part (3) and the end users at part (4), will benefit from the additional components.

TABLE 1
POSSIBLE PRIVACY THREATS IN THE HEALTH MONITORING SYSTEM

System	Privacy Threat	Threat Status
Health Monitoring System of Ref. [21]	**Part 1**: Zigbee and Bluetooth have weak security features, they also Transfer and Release data	High
	Part 2: the WWAN Release data, wireless communication must be encrypted	High
	Part 3: the Internet Transfer and Release data to the Server and the Health Care Provider. These connection need to be secure	Medium
	Part 4: the end-users Transfer and Release data as well. The users must not be allowed all these privileges unless using role-based privileges	Medium

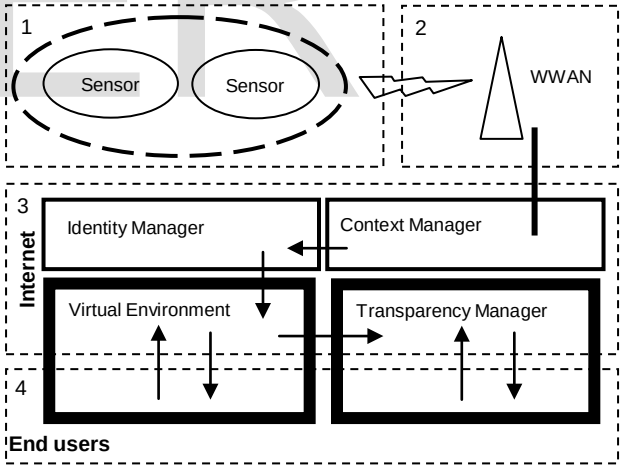

Fig. 4. Privacy-Aware additional components for the Health Care Monitoring System

In Fig. 5, FM has been applied to the proposed model architecture, yet again, for the modified Health Monitoring UC system of [21] shown in Fig. (4). It can be seen how FM gives insight on how the added components differed the way data handling was in the system.

For part (1), since no new component was added it remains the same, save for the assumption that was made, that a Sensor Manager is already there to monitor and secure the data handling. In part (2), nothing was added as well, and it remains the same. In part (3), the Context Manager handles Arrived data, and then Processes these data, or Creates and Processes data. It is then Accepted at the Identity Manager, where

it is verified and ready to be used only by privileged users. Then, it is Transferred to the Virtual Environment, this component spans both part (3) and (4). Moreover, it is Processes data and either Release or Transfer and Release data to the Transparency Manager. The latter also spans both part (3) and (4), and is responsible for Creating logs and audit sessions for the Released data. Final data is Released at the Virtual Environment, while the Transparency Manager Releases logs and audits.

The additional privacy-aware components have done well in order to lessen the privacy holes in the system. However, for the first two sections, assumptions were made of safety and privacy, and so added no new component. The Identity Manager can also extend for part (4) as well, we only showed that it allows and validates users at part (3), but end users are authenticated as well. The Virtual Environment can be used for providing secure channels, which can imply authenticating users, if not at a less complex level, since users are all less privileged in general. In Table 2, the issues that were in Table 1, are solved. Details of how the proposed model handles the privacy issues, while maintaining all the UC, and traceability functions of the original system, are given in Table 2.

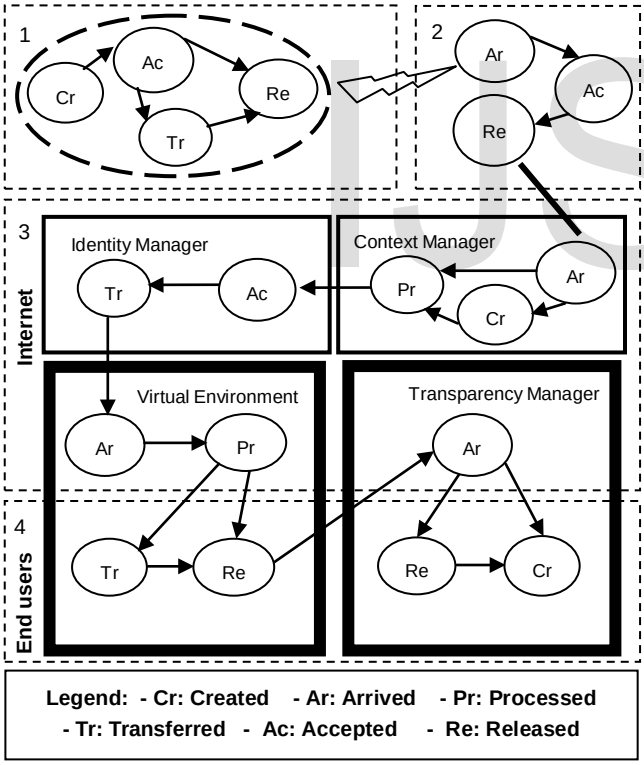

Fig. 5. FM Privacy-Aware additional components for the Health Care Monitoring System

6 Conclusion

Mark Weiser of Xerox has foreseen (and coined the term) that Ubiquitous Computing technology holds great potential for modern devices and systems, while opening doors to new venues. These range from monitoring VANETs, MANETs, and the Educational and Health Care sectors as well, such as smart class rooms, and safer hospital rooms. Traceability is a key component in UC systems, among Invisibility, and the Collection and Access of data from any point in the system [1] [3] [9]. Therefore, in having these technologies that enable safe, quick, and invisible services, we have paid for them with our privacy. Indeed, UC systems provide great privacy risks to individuals or objects. Compromised or ill-used, such systems can allow perpetrators to trace our actions, monitor, or even locate our objects or ourselves. The key in solving the contrast in objectives is in providing the ubiquity of tracking systems and the safety and privacy of anonymity by using privacy-aware systems architecture. This architecture is provided by using a modeling schema that enables modeling systems with granular details of information flow. FM, which was used, allowed for such details to manifest, allowing the proposed model to discover privacy and tracing issues.

TABLE 2
THE PROPOSED MODEL THREAT TABLE

System	Privacy Threat (Solved)	Threat Status (Modified)
The proposed model (the modified Health Monitoring System of Ref. [21], with FM [4], and architecture elements of [3]	**Part 1**: Zigbee and Bluetooth have weak security features, they also Transfer and Release data **Solution**: assuming that the sensors have enough encryption capabilities	Medium
	Part 2: the WWAN Release data, wireless communication must be encrypted **Solution**: assuming that the WWAN connections are encrypted	Low
	Part 3: the Internet Transfer and Release data to the Server and the Health Care Provider. These connection need to be secure **Solution**: the Context Manager sorts data into groups –Arrive, Create, and Process- (e.g.: private data, public data), and then the Identity manager choses who views what data –Accept and Transfer-. The Virtual Environment allows for safe spaces to sort data-Arrive and Process-, while Transparency Manager takes data -Arrive-	Low
	Part 4: the end-users Transfer and Release data as well. The users must not be allowed all these privileges unless using role-based privileges **Solution:** the data is safely Transfer and Release to the Transparency manager that Release and Create logs and audits for sent data for security measures	Medium

FM was used to model a UC system in a health environment, and find privacy concerns. Since hospitals have private and sensitive data that includes the lives of the patients as well

as staff members, the exchange of data in the system has to be secure and safe [21] [22]. The FM showed many privacy risks such as how sensors transfer data from one point to another in MANETs, sensitive data being exposed to third parties, and allowing end-users to access data from the internet. The same UC system was augmented by additional components to remedy the privacy concerns [3]. After the additions, FM showed how the altered system handles data, through its flow-thing modeling. Added components allowed the system to filter, process, and monitor the data usage and end-users as well, not only allowing for a more safe system, but also made accountability and reliability for the actions users make. The results of the solved problems show how a modeling schema, especially if we had a very large system with many components, can reveal otherwise hidden privacy threats.

Other means of securing privacy in UC systems include the use of two-way authentication protocols, the use of pseudonyms, place-preserving, or policy-preserving methods such as mix zones and virtual walls respectively, and LBS services anonymization techniques, all of which can be modeled in FM, and can be further analyzed for privacy holes in their designs as well.

REFERENCES

[1] M. Friedewald, and O. Raabe, "Ubiquitous computing: An overview of technology impacts," *Telematics Inform*, vol. 28, no. 2, pp. 55–65, February 2011.

[2] S. Motahari, C. Manikopoulos, R. Hiltz, and Q. Jones, "Seven privacy worries in ubiquitous social computing," *ACM International Conference Proceeding Series; Proc. Of The 3rd Symp. On Usable Privacy and Security*, pp. 171-172, July 2007.

[3] S. Weber, A. Heinemann, and M. Mühlhäuser, "Towards an architecture for balancing privacy and traceability in ubiquitous computing environments," *International Workshop on Privacy and Assurance (WPA-2008) at 3rd International Conf. on Availability, Reliability and Security (ARES 2008), IEEE Computer Society*, pp. 958-964, March 2008.

[4] S. Al-Fedaghi, "Systems of things that flow," *52nd Annual Meeting of the International Society for Systems Sciences (ISSS 2008)*, University of Wisconsin, Madison, USA, July 13–18, 2008.

[5] S. Pathan, H. Lee, and C. Hong, "Security in wireless sensor networks: issues and challenges," *Proc. of the 8th Conf. on Advanced Communication Technology ICACT 2006*, pp. 1048-1054, 20-22 February 2006.

[6] Y. Ponomarchuk, and D. Seo, "Intrusion detection based on traffic analysis in wireless sensor network," *19th Annual Wireless and Optical Communication WOCC*, pp. 1-7, July 2010.

[7] B. Chaurasia, and S. Verma, "Infrastructure based authentication in VANETs," *International Journal of Multimedia and Ubiquitous Engineering*, vol. 6, no. 2, pp. 41-54, April 2011.

[8] Z. Tan, "A privacy-preserving mutual authentication protocol for vehicle ad hoc networks," *Journal of Convergence Information Technology*, vol. 5, no. 7, September 2010.

[9] M. Langheinrich, "A privacy awareness system for ubiquitous computing environments," *Proc. of the 4th International Conference On Ubiquitous Computing*, p.237-245, Göteborg, Sweden, September 29-October 01, 2002.

[10] P. Ohm, "Broken promises of privacy: responding to the surprising failure of anonymization," *UCLA Law Review*, vol. 57, August 2010. Available at: www.epic.org/privacy/reidentification/ohm_article.pdf . Apr. 2012.

[11] A. Narayanan, and V. Shmatikov, "Robust de-anonymization of large sparse datasets," *Proc. of the 2008 IEEE Symp. on Security and Privacy*, pp.111-125, May 18-21, 2008. Available at www.cs.utexas.edu/~shmat/abstracts.html. Apr. 2012.

[12] L. Sweeney, "Weaving technology and policy together to maintain confidentiality," *Journal of Law, Medicine, & Ethics*, vol. 25, no. 2, pp. 98-110, June 1997.

[13] B. Könings, F. Schaub, F. Kargl, and M. Weber, "Towards territorial privacy in smart environments," *Intelligent Information Privacy Management Symp. of the AAAI Spring Symposium Series*, Stanford University, USA, pp. 113-118, July 2010.

[14] E. Moschetta, R. Antunes, and M. Barcellos, "Flexible and secure service discovery in ubiquitous computing," *Journal of Network and Computer Applications*, vol. 33, no. 2, pp. 128-140, March 2010.

[15] T. Yeh, Y. Wang, T. Kuo, and S. Wang, "Securing RFID systems conforming to EPC class 1 generation 2 standard," *Expert System Applications*, vol. 37, no. 12, pp. 7678–7683, December 2010.

[16] N. Sadeh , J. Hong , L. Cranor , I. Fette , P. Kelley , M. Prabaker, and J. Rao, "Understanding and capturing people's privacy policies in a mobile social networking application," *Personal and Ubiquitous Computing*, vol. 13, no. 6, pp. 401-412, August 2009.

[17] S. Al-Fedaghi, "Software engineering interpretation of information processing regulations." *IEEE 32nd Annual Computer Software and Applications Conf.*, Turku, Finland, pp. 271- 274, July 28- August 1, 2008.

[18] S. Al-Fedaghi, "Conceptualizing software life cycle," *8th International Workshop on Conceptual Modelling Approaches for e-Business (eCOMO 2009)*, Sydney, Australia, pp. 438–457, April 2009.

[19] S. Al-Fedaghi, "Developing web applications," *International Journal of Software Engineering and Its Applications*, vol. 5, no. 2, pp. 57–68, April 2011.

[20] S. Al-Fedaghi, and F. Al-Azmi, "Evolution of data into an information hierarchy," *Journal of Convergence Information Technology (JCIT)*, vol. 6, no. 2, pp. 9–21, February 2011.

[21] C. Otto, A. Milenkovic, C. Sanders, and E. Jovanov, "System architecture of a wireless body area sensor network for ubiquitous health monitoring," *Journal of Mobile Multimedia*, vol. 1, no. 4: pp. 307-326, January 2006.

[22] R. Haux, J. Howe, M. Marschollek, M. Plischke, and K. Wolf, "Health-enabling technologies for pervasive health care: on services and ICT architecture paradigms," *Information on Health Social Care*, vol. 33, pp. 77–89, June 2008.