From Gadget to Gadget-Free Hyperconnected World: Conceptual Analysis of User Privacy Challenges

Tanesh Kumar[1], Madhusanka Liyanage[1], An Braeken[2], Ijaz Ahmad[1], Mika Ylianttila[1]
[1] Centre for Wireless Communications (CWC), University of Oulu, Finland
[2] Industrial Engineering INDI, Vrije Universiteit Brussel VUB, Nijverheidskaai 170, 1070 Brussel
Email: [1][tanesh.kumar, madhusanka.liyanage, ijaz.ahmad, mika.ylianttila]@oulu.fi, [2]an.braeken@vub.ac.be

***Abstract*—Currently, gadgets are the most common and frequent ways of acquiring digital services. However, due to recent advancements in smart sensing and communication technologies, it seems that, this trend might get change in coming days. Future is hinting us towards a gadget-free hyperconnected society, where each object can sense, gather and process the information and can be able to take context based decisions. The vision behind this novel concept is to provide users, digital services anywhere and anytime, without using explicit gadgets or even wearables. Smart surrounding will be able to provide digital services to users according to their requirements. Also with the addition of 5G technology, this vision will get more strengthen and thus novel services will come into action. This will generate massive amount of critical data and eventually dealing with privacy in such ambient and gadget-free environment will be one of the major concerns for users. Therefore, this paper presents privacy challenges from user's perspectives, that can potentially arise in such gadget-free environment. An initial and tentative conceptual privacy framework is also discussed in the light of the user's privacy issues. Furthermore, we provide an overview of transformation requirements needed in transition from the gadget to gadget-free world.**

***Index Terms*—Gadget, Gadget-Free, Privacy, Identity, Hyperconnected World, Digital Services, Ambient Environment**

I. Introduction

Nowadays, gadgets such as smartphones, tablets, Personal Digital Assistants (PDAs) are mainly used to get digital services in everyday life. They have been successfully used in many critical applications such as banking, healthcare and transportation among others. Along with gadgets, acquiring services through wearables are another quite popular trend nowadays. However, concepts like ubiquitous and persuasive computing are opening new doors for research community to look a step ahead of gadgets and wearables. This leads us to the vision, where the user can be able to get similar services (as previously from gadgets/wearables), but without carrying any hand held gadgets. We termed this novel concept as the Gadget-Free Hyperconnected World or the Naked World [1,2] as shown in Figure 1. Digital services will be available anywhere and anytime in a ubiquitously manner, but without any direct involvement of gadgets from the user side. Intelligent environment will play key role, as the services would be embedded in the environment. 5G and Internet of Things (IoT) are considered backbone for this gadget-free hyperconnected world.

User privacy concerns are constantly increasing with respect to the advancement in the technology. Every individual in this digital era wants the autonomy and control over their personal data, however this is not completely achievable in the real world. Several companies/service providers are using consumer's personal and location information from their gadgets, to draft critical decisions without concerning them and that can eventually effect on their reputation. However, for gadgets, there are already some privacy regulations and polices are formulated in order to protect the privacy of the user. In the case of gadget-free environment, the privacy concerns are high, because the user is constantly monitored by the surrounding and huge amount of data is generated.

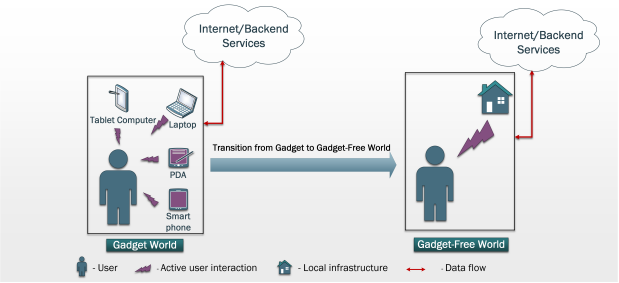

Fig. 1: Transition from Gadget to Gadget-Free World

Therefore, in this paper, we highlight the privacy challenges that the user will potentially face in the gadget-free hyperconnected world. Based on the user's privacy concerns, we have discussed the conceptual privacy framework for such ambient and gadget-free surrounding. The rest of paper is organized as follows: Section II and III explains the background and user's privacy challenges respectively. Section IV elaborates the conceptual privacy framework for gadget-free world and section V highlights transformation requirements. Finally, we conclude the paper in section VI.

II. Background

With the introduction of smart phones, the consumer way of living is changed dramatically. Now the user enjoys certain

useful services on mobile devices such as communication, entertainment, healthcare and banking among others. People use them to store highly sensitive personal information including email, passwords, financial accounts, and medical records. Privacy issues in such context become critically important because vendors/service providers may access a large volume of the user's personal information. The applications (apps) in smartphones which deliver various services to the subscriber, are also major cause of the information leakage. The work in [3,4], examines such kind of privacy risks raised by the various apps. In [5], authors also explained location privacy breaches, which arise due to using Location Based Services (LBS) on mobile devices.

Next, concepts like ubiquitous and persuasive computing enabled the vision of services anywhere and anytime[6,7]. Weisser [8], introduced the concept of Ubiquitous Computing, which became the major breakthrough for the services everywhere vision. The ambient intelligence play vital role in smart and ambient environment and research in [9,10] discusses such privacy threats and corresponding conceptual frameworks for ambient surroundings. The privacy risks explained in [11], are for smart home environment from the context of data oriented privacy and context oriented privacy. According to the authors, data privacy can be caused by internal and external adversaries whereas context oriented privacy is protecting contextual information such as location and timing of transmitted data traffic. In [12], authors presented a detail survey about identification of various privacy requirements for pervasive based applications and also mentioned potential approaches to preserve it and finally discuss other crucial aspects that includes technical, user experience, legal and economic challenges. The work in [13], addresses privacy issues for coming digital future and recommends few technically innovative solutions to reduce the risk of privacy.

Furthermore, recent developments in technology and in addition with some existing concepts leading us to the next major transition in the coming future. We call this phase as gadget-free hyperconnected world, because it assumes that all computing technologies and user interfaces (UIs) are embedded in the nearby surroundings. This vision is strongly based on the user centric approach and thus environment will provide services according to the user's need. There will be no explicit gadgets used for acquiring digital services. With the current available technology, it may not be practical or realistic to our comprehension at this moment. However, in more limited spaces the benefits and value of some of its ideas and solutions have been demonstrated already by ambient intelligence and smart environments. Also with the evolution of technology, the gadget-free vision will get constant improvements in terms of its practical use in daily life

III. User's Privacy in Gadget-Free World

The world is facing a rapid evolution in information technology, which is creating several new opportunities from social and economic perspectives, but at the same time imposing great challenges to the individual's privacy. Data is generated in massive volumes and the user has limited control over it. To discuss the user privacy in further detail, we divided it into three major categories i.e. data, location and identity.

A. Data Privacy

Data privacy concerns refer to the threats caused to the user when personal information is leaked. In the case of gadget based services, users personal data can be collected through various applications running on gadgets such as banking, healthcare, education, entertainment, social networking websites and online shops. These applications are either provided by service providers or application developers. The major concern here for users is that companies/service providers do not provide the clear explanation that how the personal information of individual is gathered and for what purpose it is going to be used. Another concern is whether the data storage is secure or not. There are certain sensitive applications for instance, healthcare, which requires serious data protection and therefore access of patient's critical data should be limited to the specified people such as doctor or family members. Moreover, user's privacy is not only violated by the collection of personal information by the companies but also by the aggregation and centralization of the personal information.

Next, for the gadget-free scenario, smart environments themselves are responsible for delivering digital services to users. Unlike gadgets, users in this case do not have any proper screen or display to interact with. Privacy risks can cause, for example, if multiple users are available in the same smart space and one individual wants to see his/her personal information. Numerous amounts of sensors, actuators and other chips are embedded in the surrounding that are able to sense, gather and process huge amount of personal data. This will also impose similar data privacy concerns, as we have discussed in the case of gadgets such as usage of personal data by service providers without consumer's consent. Storage and protection of personal information are other major issues to consider during the design and implementation of such environment.

B. Location Privacy

Every modern smartphone or tablet has Global Positioning System (GPS) capabilities that work just as well as that of a dedicated device. In fact, in some cases they may get a faster fix on your location since smartphones are able to use cell tower triangulation to augment the GPS technology. GPS technology is also currently integrated into several wearables. If not, by the communication of wearables to the smartphone, the position can still be revealed. Based on this information of the user, new doors to location aware computing and services have been explored for the research. For instance, there are many location based applications available for users that are providing numerous services such as the nearest hospital in case of the emergency or the nearest cinema or restaurant for the purpose of entertainment. The other potential example is famous social networking websites like Facebook, where location can be seen with the updated status or even the user

can share his/her current location with an option check in to the airport or shopping malls.

Besides all these useful benefits, there are also a number of risks associated while using these services because, the location information may allow adversaries to track users and try to steal sensitive information. In addition, location information can be misused by an attacker to check whether their home is empty or to know their exact location at a particular time or to predict what could be their possible activities in a particular day. Stalkers by tracking location information can harm mobile users economically, physically and legally [14]. Consequently, the major privacy challenge is the leakage of undesired users location information to location based service (LBS) operators or external adversaries [15].

However, the privacy situation is comparatively more risky in the case of the gadget-free surrounding because smart sensors present in the environment would continuously monitor/track user's movements and actions. Therefore, attacker, instead of attacking a particular device of the user to track its position at any time, an attack of the fixed devices in the environment would leak the location information at a particular time of a whole bunch of people, leading to a much larger impact.

C. Identity Privacy

While discussing identity privacy, distinction needs to be made between real identity visible in the public space such as name, address, telephone number, etc and users' credentials like password, biometrics, etc. required to get access to the digital services.

1) Public identity: The trend of stealing online identities is getting very popular nowadays because of the online applications such as shopping and online banking. For example, when the user is buying something online and when he/she pays the amount online through the credit card, his/her real identity may lead to some privacy risks. There are some situations, where users do not want to show their real identities publicly and thus they use fake or temporary identities during communication or while getting the services. In [16], an efficient security mechanism using a registration center and smart card have been described to offer such kind of anonymity to the user.

In the case of the gadget-free environment, the type of identity related information for the user depends upon the power of the system. In the first place, this might happen through biometrics characteristics, for instance, face recognition and Iris [17]. However, as the systems are getting smarter, it is just a matter of time to link faces to real names. The only possibility for the user to prohibit its collaboration is to hide his/her face.

2) Users credentials: The credentials of a user, typically called the knowledge factors and the inherence factors, correspond with things the user knows like passwords, pass phrase, Personal Identification Numbers (PINs), challenge responses, security questions and things the user uniquely possesses like fingerprint, retinal pattern, DNA sequences, face, voice, unique bio-electric signals. It is clear that this information should be private at any time, because the leakage of this information would lead to access all confidential and personal data of the user and can cause to lost of digital identity.

Independent of the type of environment and the behaviour of the user, leakage of this sensitive information can be possible on the side of the service provider or application developer, that might get hacked. For instance, at the end of August 2016, it came into the news that the popular cloud storage firm Dropbox had been hacked, with over 68 millions of user's email addresses and passwords leaking on to the internet. The same happened with LinkedIn for more than 117 million LinkedIn accounts that were being traded on the dark web.

In gadgets, there exist a user-centric trust and privacy model, where the user's credentials are stored in secure tamper-resistant hardware on the device and never leave the device. Recently, Mobile Biometric Authentication Systems (MBAS) are installed on the smartphones besides the classical PIN based password. The two biggest MBAS deployments to-date have been powered by embedded fingerprint sensors, with Apple's Touch ID and Samsung's swipe fingerprint.

In the gadget-free environment, the captured information to uniquely identify a person is in the form of physiological characteristics such as fingerprints, DNA, face recognition, hand geometry, voice waves, retina and iris patterns. In this phase, the identification mode that the system performs, is a one-to-many comparison against a biometric database in an attempt to establish the identity of an unknown individual. The system will succeed in identifying the individual if the comparison of the biometric sample to a template in the database falls within a previously set threshold. Lost of this biometrics information is permanent as it cannot be changed by password in the case of knowledge factors. Therefore, usage and storage should be very carefully managed.

IV. Privacy Framework For Gadget-Free Hyperconnected World

We examine some of the most important privacy factors needed to consider during the transition from gadget to gadget-free world. We have formulated an initial and tentative conceptual privacy framework for the user as shown in Fig 2.

- **Access Control:**

Access control mechanisms ensure that users must have access over their personal data when they give it to companies through gadgets. Using gadgets (smartphones, tablets), access control mechanisms can be implemented relatively in more secure ways because there already exist some rules for the subscriber and service provider. In contrast, for gadget-free services, it requires stronger and secure level of access control mechanisms because in this case, environment would have more access over data, as digital services are delivered by surrounding itself.

- **Anonymity:**

Many of our everyday activities are more or less anonymous, e.g. different kinds of phone or public enquiries can be anonymous, and also on social networking sites and online

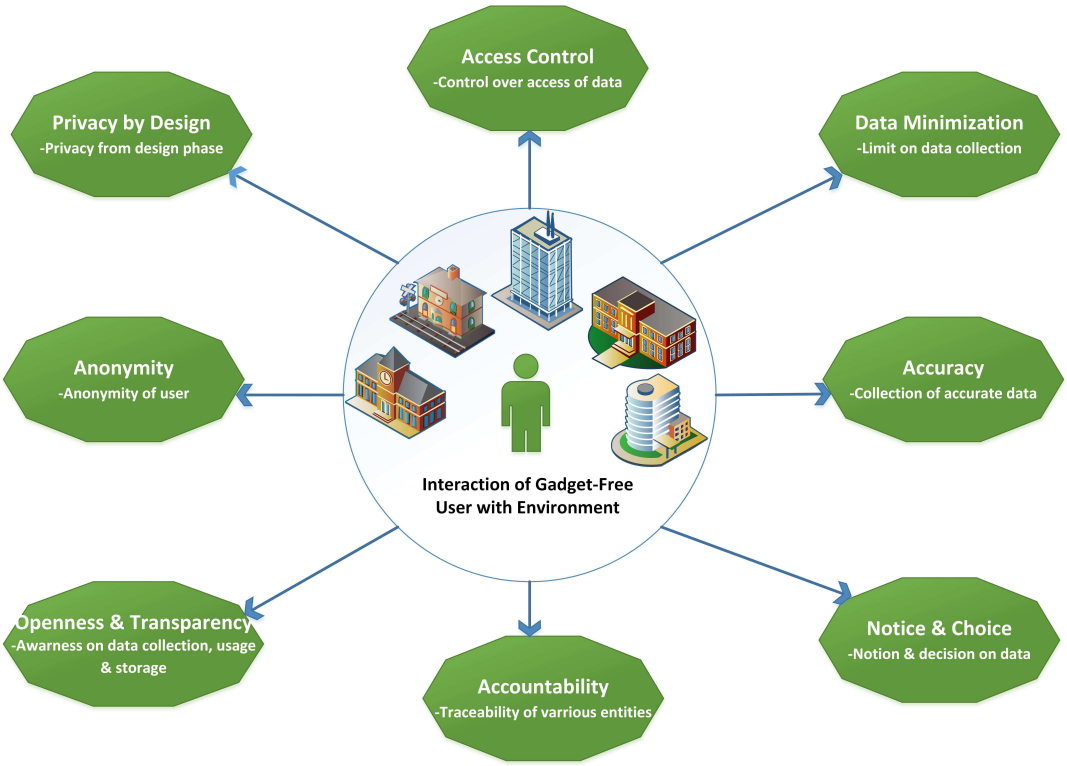

Fig. 2: Conceptual and Tentative Privacy Framework for the User

cash transactions. Using gadgets, there are various efficient mechanisms available where the user can securely achieve anonymity to acquire these digital services (e.g. smart card based remote anonymous user authentication using mobile devices in [18]). The situation for gadget-free environment is different as the authentication of the user utilizes biometrics information, which cannot be anonymized. The biometrics data is unambiguously linked to the identity of the user, compared with the usage of pseudonyms applied in gadgets.

- **Notice and Choice:**

Notice is about the notion a user has on the collection of its data and its use. Choice defines the decision, a user can make on allowing its data to be collected and used in a predefined way. On mobile devices, it is in theory possible to read a privacy policy or the terms of a service document. However, given the constrained physical size and display area, it is in practice almost never consulted. In the case of gadget-free surroundings, where the user will be dependent on the intelligent environment for desired digital services without any use of explicit gadgets, it is even more challenging to establish notice and choice features from the users side.

- **Data Minimization:**

Data minimization refers to the concept that companies/service providers/third party should collect the data in lawful ways, limit the data they collect for that particular service and dispose it once they do no need it longer. With the technologies such as IoT, companies are able to access more and more personal data in easy and reliable ways. In the gadget-free hyperconnected environment, the data generation would even be higher than gadgets based services because the environment constantly monitors the behavior and actions of the user and responds according to that. It needs to store a lot of user related information for analyzing, in order to speed-up the identification process of the user and then provide respective services.

- **Accountability:**

Accountability refers to traceability of the operations performed on the system by specific entities (such as user, process, and device). It ensures to monitor and identify the actions carried out by various entities. The work in [19], shows one mechanism for privacy preserving accountability for personal devices (i.e. mobile phones) explaining the accountability of employees in corporate network using mobile devices. The traditional privacy practices for accountability might not be completely adaptable in the gadget-free world. Thus accountability requirements for such ambient environment need deeper consideration because it is challenging to trace the actions of users in a situation, when they are not carrying any hand held gadgets.

- **Accuracy:**

Personal data which is taken by companies/third parties should be accurate, complete, and kept up-to-date. The data should also be used for the limited purposes which is already defined by companies and users with their mutual consent. Inaccurate data may lead to various consequences because, the inaccurate data cannot be properly used for desired purposes

by companies/service providers. In gadgets, it is relatively more convenient to manage and update data accuracy along with preserving the privacy because of the higher computational and storage capabilities. Gadgets also have proper display screen for interaction with the user. In the gadget-free scenario, the requirements of accuracy should be high as the environment will be the only medium to interact and communicate. There might be some possibilities for inaccuracy such as, successfully identification of invalid user through biometrics. Also the computational and storage capabilities will be limited in this case.

- **Openness and Transparency:**

Openness and transparency are key pillars in developing the trust between the customer and companies/service providers. It guarantees that user must be aware while the personal information being collection by service provider. The user must also ensure the purpose of data collection and the place to store it. The gadget-free environment need more concrete steps towards this issues as compared with gadgets which relatively have already few secure mechanisms for it.

- **Privacy by Design:**

Privacy by Design (PbD) approaches are quite popular for providing privacy in gadgets based services. PbD considers the privacy requirements at organization level and right from the design phase. In the gadget-free hyperconnected environment, similar kind of methodologies should be adapted while designing such kind of ambient environment.

V. The Transformation Requirements

The transition from gadget to gadget-free hyperconnected world will require radical changes not only in the infrastructure/architecture, service provisioning and access, but in the user behavior as well. Since most of the user information will be embedded in the infrastructure, new user interaction models need to satisfy both user privacy and service provisioning requirements. The user information will already be embedded in the environment because the notion of gadget-free services requires the environment to ubiquitously interact with the user and eventually the user will need to access all of their information anywhere and anytime. This will require strict privacy enforcement mechanisms compared with what we already have in gadgets. There are two main dimensions of privacy enforcement that are consistent in the evolution from gadget to gadget-free environments i.e. functional and non-functional requirements.

A. Functional Requirements

The functional requirements include technological mechanisms that ensures the user privacy through various technologies. The main technological areas that could be used to ensure user privacy include identification mechanisms for authentication, access control and non-repudiation, and encryption technologies to ensure integrity and confidentiality of data in transit. In gadget-free environments, the inherence factor will be used to meet the identification requirements. The instant access of user's data and the offered services will require quick authentication and hence the fast exchange of identity information is needed. This will require high processing at the edge, backend devices and fast communication links between the user, the interactive environment and the backend servers. Moreover, the user will need to have trust relations already developed and require transparency mechanisms to ensure data integrity must be developed. One of the challenges faced by such systems will be privacy preservation in the wake of user mobility in interactive environments that will involve abrupt opening and closing of the user initiated sessions. This will require fast context exchange between different gadget-free environments under strict delay constraints.

One of the results of this evolution process will be that, the user control over his data will be minimized due to the integration of identification mechanisms in the environment and high dependence on the interactive environment, identity storage, and authentication servers. This evolution process showing user control over his information, is presented in Figure 3. Along the process, gadgets that store user information will disappear gradually and hence the information and identity storing the process will go into the infrastructure. Since infrastructure will have more control over the user identity and information, strong security procedures will be needed to preserve user's privacy.

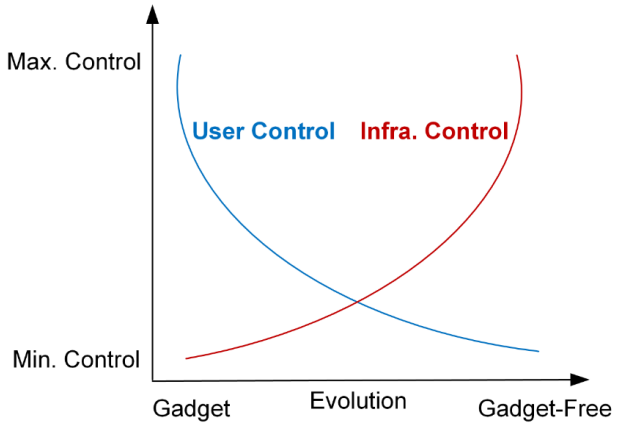

Fig. 3: Transformation from Gadget to Gadget-Free World

B. Non-Functional Requirements

Non-functional requirements include user's behaviour, ethical issues and legal frameworks for the gadget-free hyperconnected environment to maintain acceptable levels of privacy.

1) Behaviour aspects: Since users are not directly involved in the exchange process of identification (previously their gadgets used to), they need to get comfortable with the new identification mechanisms such as face scanning, retina scanning, fingerprinting or verbal identification techniques. Moreover, the users need to agree to fact that their information will be embedded in the infrastructure for fast and gadget-free identification.

2) Ethical aspects: Ethical issues are the kind of moral responsibilities for the consumer to preserve the privacy for others [20]. For example, the camera present on the google glasses which is taking pictures and monitoring the other people's movements without informing them. This is rising privacy threats to the people and therefore several casinos, bars and restaurants put ban on using google glasses in their premises. The same issues arise with the face recognition is done using google glasses without consent of the user. Consequently, ethical laws are needed in order to limit the functionality of gadgets and wearable devices at public places. The gadget-free hyperconnected environment needs additional ethical precautions because smart sensing technologies present in the environment continuously monitor/track the people (individual or in group). Also in this case, as explicit gadgets or wearables will not be in use, it would be challenging to realize that who actually is tracking the user.

3) Legal aspects: Data protection of the consumer is one of the core legal issue in gadgets. Everything related to the user is available online and can be easily accessed by the service provider and third party companies. Also, social media applications such as Facebook and Instagram reveal all your activities every day and store your personal pictures and information. Consequently, there should be a check and balance for consumer confidential data on their storage and usage. Many mobile apps in gadgets track the user's location information not only for adults but for children as well without their parents' consent. The Federal Trade Commission (FTC) has suggested some guidelines in [21] to protect the consumer privacy in this rapid digital era.

Legal and policy enforcement frameworks are necessary to ensure the user privacy in each of the environment. Regulation authorities can direct service providers to implement and use standard technologies that comply with legal regulations and maintain balance and check on the administration to enforce the suggested mechanisms. However, the privacy regulation is a hot debate and anonymity versus accountability laws are not very straight forward. The chance of privacy breaches increase in the gadget-free environments due to overwhelming dependence on the enabling technologies.

VI. Conclusion

The gadget-free hyperconnected world/Naked World provides all kinds of digital services without any involvement of personal gadgets. The transition from gadget to gadget-free environment is naturally bounded by evolution of technologies that are needed to implement it. This paper analyzes the possible privacy challenges from user's perspective during this transition. The user would have direct and seamless interaction with the environment for acquiring digital services. The privacy requirements need to be increased as we move from gadget to gadget-free world. Therefore, we have presented the initial and tentative privacy framework from the user point of view. Furthermore, the transition is also discussed from the perspective of function and non-functional requirements. Possible behavioral, ethical and legal implications for the gadget-free environment are also briefly mentioned in this work. As this gadget-free environment is not fully realized in practice yet, it is highly possible that new privacy threats might arise for this vision in coming future.

Acknowledgement

This work has been performed under the framework of "The Naked Approach" and "Towards Digital Paradise" projects which are funded by TEKES, Finland. Moreover, the authors would like to acknowledge the STSM Grant presented by the COST Action IC1303 AAPELE project.

References

[1] J. Aikio, V. Pentikinen, et.al., (2016), "On the Road to Digital Paradise". [Online], Available: http://nakedapproach.demoshelsinki.fi/wp-content/uploads/sites/3/2016/08/NA-concept-book.pdf

[2] "The Naked Approach, Nordic Perspective to Gadget-free Hyperconnected Environments", [Online], Available: http://nakedapproach.fi/

[3] Anne S.Y. Cheung, "Location privacy, The challenges of mobile service devices", Comp. Law and Security, Volume 30, Issue 1, February 2014, Pages 41-54.

[4] Wetherall, D., Choffnes, D., Greenstein, B., Han, S., Hornyack, P., Jung, J., Schechter, S., Wang, X.: "Privacy Revelations for Web and Mobile Apps". In: HotOS 2011.

[5] Kelley P, Consolvo S, Cranor L, Jung J, Sadeh N, Wetherall D. "A conundrum of permissions: installing applications on an android smartphone". In: Workshop on usable security (USEC- 2012); 2012.

[6] Michael Friedewald, Oliver Raabe, "Ubiquitous computing: An overview of technology impacts", Telematics and Informatics, Volume 28, Issue 2, May 2011, Pages 55-65.

[7] D. Saha and A. Mukherjee, Pervasive Computing: A Paradigm for the 21st Century, Computer, vol. 36, no. 3, 2003, pp. 25-31.

[8] Weisser, M. (1993) Some computer sciences isssues in ubiquitous computing, Communications of the ACM, 36(7), July, pp75-84.

[9] M. Lopez, J. et.al.,"Ambient intelligence: applications and privacy policies, in Highlights of Practical Applications of Heterogeneous Multi-Agent Systems". The PAAMS Collection. Springer, 2014, pp. 191201.

[10] P. Brey, "Freedom and privacy in ambient intelligence, Ethics and Information Technology", vol. 7, no. 3, pp. 157166, 2005.

[11] H. Drushti, "Security and privacy consideration for internet of things in smart home environments", International Journal of Engineering Research and Development, vol. 10(11), pp. 7383, 2014.

[12] C. Bettini and D. Riboni, "Privacy Protection in Pervasive Systems: State of the Art and Technical Challenges", Pervasive and Mobile Computing, vol. 17, pp. 159174, 2015.

[13] R. H. Weber, "The digital future, A challenge for privacy?" Computer Law and Security Review, vol. 31, no. 2, pp. 234242, 2015.

[14] M. Wernke, P. Skvortsov, F. D urr, and K. Rothermel, A classification of location privacy attacks and approaches, Personal and Ubiquitous Computing, vol. 18, no. 1, pp. 163175, 2014.

[15] R. Shokri, J. Freudiger, and J.-P. Hubaux, "A unified framework for location privacy", in In 3rd Hot Topics in Privacy Enhancing Technologies (HotPETs), 2010.

[16] Braeken A., "Efficient Anonym Smart Card Based Authentication Scheme for Multi-Server Architecture", International Journal of Smart Home, 9(9), 177-184 (2015).

[17] Tanesh Kumar, Madhusanka Liyanage, An Braeken, M. Ylianttila, Identity Privacy Preserving Biometric Based Authentication Scheme for Naked Healthcare Environment, ICC 2017, Paris.

[18] Shin SB, Yeh HJ, Kim KH, Kim KS (2012), "A remote user authentication scheme with anonymity for mobile devices". Int J Adv Robot Syst 9:17.

[19] Gheorghe G., Neuhaus S. "Poster: Preserving privacy and accountability for personal devices". 2013 ACM SIGSAC Conference on Computer and Communications Security (CCS 13), Berlin, Germany.

[20] Brey, P. (2012). Anticipating Ethical Issues in Emerging IT. Ethics and Information Technology 14: 305317.

[21] Protecting Consumer Privacy in an Era of Rapid Change", FTC Report [Online], Available: https://www.ftc.gov//