International Research Journal of Human Resources and Social Sciences
Vol. 4, Issue 1, January 2017 Impact Factor- 5.414
ISSN(O): (2349-4085) ISSN(P): (2394-4218)

Website: www.aarf.asia Email : editor@aarf.asia , editoraarf@gmail.com

SIGNIFICANT THREATS TO RETAIN SECURITY IN ELEGANT MODELS ON E-COMMERCE

DR. K. N. SHEWALE
HOD, DEPT. OF COMMERCE
SHRI SHIVAJI COLLEGE, CHIKHLI

Abstract

E-Commerce plays very critical role in everyone' s life. Smart models and models have become popular as technological solution that offers a better experience for children. However, the technology employed greatly increases the risks to children' s privacy, which does not seem to have become a real concern for toy makers. We investigated this issue through a study driven by two major research questions: which are the major smart models-related children' s privacy risks and which are the major mitigation so to such risks. To answer these questions, we conducted a scoping review. The most mentioned technical risk is data disclosure, while from a domain-specific perspective there is much concern on the children' s physical and psychological safety. From a mitigation standpoint, many recommendations and solutions have been proposed, but without a more common type of contribution. This paper focuses on the significant risk or threat to maintain security in the elegant models on E-commerce.

Keywords: *E-commerce, Models on internet, Data privacy, IoModels, scoping review*

INTRODUCTION

Both toy and game companies have started to integrate hardware and software computing into smart models Smart models became able to collect and process data in real time favored by miniaturization and lower costs of processing circuits. The industry also refers to them as connected models given their connectivity to other models or gadgets such as smart phones, tablets and game consoles. They can often connect to mobile and cloud services consequently permeating the domains of the Internet of Things (IoT), which in this context is sometimes called the Internet of Models. IoModels uses short- or long-range wireless communications protocols such as Wi-Fi, Bluetooth or Near Field Communication (NFC) for the acquisition, computing and transfer of child user' s personal and non-personal information. The National Institute of Science and Technology (NIST) define Personally Identifiable Information (PII) as " any information about an individual maintained by an organization that can be used to distinguish or trace an individual' s identity, including any information linkable to an identifiable individual" (NIST, 2010). The International Organization for Standardization (ISO) defines PII as " any information that (a) can be used to establish a link between the information and the natural person to whom such information relates, or (b) is or can be directly or indirectly linked to a

natural person" . In addition to PII, there are other types of user-sensitive data that may reveal personal information about them, such as context data. Context data is data observed and collected through sensors that gather signals on the user and its environment Context data can be used to characterize some situation, as location or time, for example. Interaction data can also be sensitive, i.e., data derived from children' s interactions with the toy, such as video and voice recordings. Smart models use user-sensitive data for a variety of reasons. For example, pervasive location-based applications, such as Niantic' s Pokémon Go, collect Global Positioning System (GPS) data to allow outdoor playing. Smart models such as Mattel' s Hello Barbie, including companion robots such as Asus' Zenbo aim to promote social communication between the user and the social toy or robotic agent. Conversation functions use speech recognition and Artificial Intelligence (AI) to establish and maintain a reasoning-based dialogue with the child. Thus, collecting, sharing, and storing PII, context data or interaction data, such as geo-location and child voice recordings, are common practices for these social agents in order to offer an experience resembling human communication.

BACKGROUND

Privacy can be considered a very vague concept and can be defined in different forms depending on the purpose. A generic way of defining privacy aligned to the purpose of this paper is the right that someone has to keep their personal life or personal information secret or known only to a small group of people. We refer to children' s privacy when the data for which privacy is desired is that of a child. IoT-related products, including IoModels, offer clear risks to the user' s privacy since they can collect, store and manage PII, including sharing users' PII with third parties. Governmental entities are worldwide taking efforts to regulate data privacy protection rules to be employed in companies and organizations. For example, the General Data Protection Regulation is a generic regulation on data protection and privacy for all individuals within the European Union and the European Economic Area, which also addresses the export of personal data outside this region. GDPR defines Personal Data (PD) as anything containing directly or indirectly compromising information that can expose user privacy and allow the singling out of individual behavior.

IoT-related products, including IoModels, offer clear risks to the user' s privacy since they can collect, store and manage PII, including sharing users' PII with third parties. Governmental entities are worldwide taking efforts to regulate data privacy protection rules to be employed in companies and organizations. For example, the General Data Protection Regulation (GDPR) is a generic regulation on data protection and privacy for all individuals within the European Union and the European Economic Area, which also addresses the export of personal data outside this region. GDPR defines Personal Data (PD) as anything containing directly or indirectly compromising information that can expose user privacy and allow the singling out of individual behavior. Models are products intended for leisure, learning, socialization and physical play that can address various benefits to child development. Smart models appeared as a response to the sales decrease of traditional models, which happened because of the increasing popularity of the internet- and console-based video gaming products. The term smart toy covers a range of play products that can present different levels of network, processing and reasoning capabilities. Smart models appear in various shapes, including anthropomorphic and humanoid, such as a plush toy, a doll, a companion robot or a wearable gadget. Technological solutions used by these smart models vary since Augmented Reality (AR) resources to advanced functions

such as wireless connectivity features and AI-based conversation functions. A new wave of smart models appeared more recently with the models that listen.

TERMINOLOGY

We found a significant number of works addressing privacy and security concerns regarding smart models. However, there is not yet a systematic study of the literature that analyzes the papers published in this context. We found some literature reviews that only partially cover our topic of interest. That means we could find some secondary studies on privacy and security in contexts other than smart models as well as some secondary studies on smart models with concerns other than privacy and security. Although smart models are considered a sub-area of IoT or BYOD, these more general reviews fail to address smart models as this is a very specific subject within IoT and BYOD and they refer to more general aspects. Loukil et al. addresses six specific application domains: smart cities, smart homes, smart grids, health care, location sharing and smart spaces; none directly related to smart models. Big data is high relevant to smart models as one of the primary sources of risk of privacy violation when using smart models is the large amount of data collected by the toy companies from their child-users.

However, also in this case, as it is a very specific subject within the big data area, smart models is not one of the topics covered in this review. The other three reviews address smart models without covering privacy concerns. Two of them address smart models applied for clinical treatment. Nunes et al. present two complementary reviews on applying smart models in the medical field, which include works to explain medical procedures for hospitalized children or to assist in rehabilitation therapies for children with disabilities such as children with autism. The length of time each review covered varies greatly (3– 19 years), which depends on the specific context and purpose of each case. One may desire to increase or decrease the number of studies to be analyzed; or a specific topic may be so recent that it would not make sense to look for papers in a distant past. Another factor potentially influencing the number of studies to be selected and analyzed in the review refers to which data sources were chosen to search for papers. Most reviews used multiple databases. Two reviews also looked for papers in specific conference proceedings. In the end, the number of papers (primary studies) ranged from 5 to 118, which resulted from both the search protocol decisions and mainly the review topic and context themselves.

CONCLUSION

This study aimed to review the scope of published work related to privacy issues in smart models, focusing on the risks solutions. Two research questions were addressed. For the first research question - which risks to children' s privacy when using smart models have been addressed?, the most commonly mentioned technical risk is data disclosure, while from a domain-specific perspective, there is much concern on the children' s physical and psychological safety. As for the second research question - which mitigation solutions to children' s privacy risks have been proposed?, while several recommendations and solutions have been proposed, we did not identify a more frequent contribution type. We observed that many issues could certainly be mitigated most of the time with existing, and even simple, solutions from the broader IoT context.

REFERENCES

1) Gerpott, T., and Kornmeier, K. (2009) 'Determinants of customer acceptance of mobile payment systems', International Journal of Electronic Finance, Vol. 3, No. 1, pp.1- 30.
2) J.R., Kohno, T., 2009. A spotlight on security and privacy risks with future household robots: attacks and lessons. In: Proceedings of the 11th International Conference on Ubiquitous Computing (UbiComp). ACM, New York, NY, USA, pp. 105– 114. https://doi.org/10.1145/ 1620545.1620564.
3) Gilaninia, S., Chirani, E., Banikhedmat, S. and Mousavian, S. (2011). 'Affecting factors on bank customers' intention to use of mobile payment services', Trends in Advanced Science and Engineering, Vol. 1, No. 2, pp. 40-48.
4) Gunasekaran, A. and McGaughey, R. (2009). 'Mobile commerce: issues and obstacles', Int. J. of Business Information Systems, Vol. 4, No. 2, pp. 245-261.
5) Hackbarth, G., Grover, V. and Yi, M. (2003). 'Computer playfulness and anxiety: positive and negative mediators of the system experience effect on perceived ease of use', Information & Management, Vol. 40, No. 3, pp. 221-232.
6) Hair, J., Babin, B., Money, A. and Samouel, P. (2003). 'Essentials of Business Research Methods', New York: John Wiley & Sons Inc.
7) Heneman, H. and Judge, T. (2003). 'Staffing Organization', 4th edn. McGraw-Hill. New York. Hsiu-Fen Lin (2011). 'An empirical investigation of mobile banking adoption: The effect of innovation attributes and knowledge-based trust', international journal of information management, Vol. 31, No. 3, pp. 252-260.
8) Hwang, R.-J., Shiau, S.-H., and Jan, D.-F. (2007). 'A new mobile payment scheme for roaming services', Electronic Commerce Research and Applications, Vol. 6, No. 2, pp. 184-191.
9) Jaradat, M-I. and Twaissi, N. (2010). 'Assessing the Introduction of Mobile Banking in Jordan Using Technology Acceptance Model', International Journal of Interactive Mobile Technologies, Vol. 4, No. 1, pp. 14-21.
10) Kamoun, F. and Halaweh, H. (2012). 'A fuzzy classification approach to assess ecommerce security perception', Int. J. Business Information Systems, Vol. 9, No. 1,pp.108-126.
11) Karahanna, E., Straub, D. W. and Chervany, N. L. (1999). 'Information technology adoption across time: A cross-sectional omparison of pre-adoption and post adoption beliefs', MIS Quarterly, Vol. 23, No.2, pp. 183-213.
12) Khalifa, M. and Ning, K. (2008). 'Explaining the adoption of transactional B2C mobile commerce, Journal of Enterprise Information Management, Vol. 21, No. 2, pp. 110- 124.
13) Khan, W. (2012). ' Mobile payments strategy', Journal of Payments Strategy & Systems, Vol. 6, No. 3, pp. pp. 210-218.
14) Khraim, H., AL Shoubaki, Y., and Khraim, A. (2011). 'Factors Affecting Jordanian Consumers' Adoption of Mobile Banking Services', International Journal of Business and Social Science, Vol. 2, No. 20, pp. 96-105.