Human Factors in Smart Home Technologies using Internet of Things

B. Swathi[1], K. Ravi Chythanya[2], D. Mahesh[3], Seena Naik Korra[4] ,A.Harshavardhan[5]
Department of CSE, S R Engineering College, Warangal[1,2,3,4,5]
jrswathi.hi@gmail.com

Abstract:

The term "smart" is widely recognized as intelligence in different areas.One of the representative technologies of the IoT era, smart home technology has turned as the home equipment into intelli gent, more remote controllable and interconnected. In past years the use of the Internet of Things (IoT) has made smart homes increasingly popular.Rapid diffusion in sensor technology has also made advances in smart homes inevitable. The advancement of these technologies in smart homes has provided the smart home users with many convenient products and services. Contrary to the term convenience, areas remain to be improved in order to achieve effective and simple smart home environment. In this paper, we have discussed on the purpose, benefit and technology of smart home definition. In addition to, the emphasis is given to the challenges of making a smart home is to an ideal and simple environment to live.There is also proposed solution for some of its challenges.

Index Terms
Smart home, Internet of Things, Usability, Smart Homes, Human Factors, Energy Consumption, Control Systems.

1. Introduction

Smart Home is the organic combination of different home-based subsystems by state-of - the-art in advanced technologies such as fiber optic composite cable home. It can share resources and communicate within the home and we may exchange information through the smart home gateway with home external network. The main objective is to ensure the convergence of framework, service, and management in an efficient comfortable, safe, convenient and environment- friendly living environment for people [1].

In order to meet the automation requirements of an entire system is to provide more efficient control and management, a Smart home incorporates computer technology, control technology, wireless transmission technology, and communications technology through various networks. The traditional smart home implementation generally controls and communicates building facilities through the wiring of wired lines, it is difficult to get rid of the restraints of various cables, the installation cost is high, and the scalability of the system is also poor. The smart home system based on wireless sensor network technology can not only get rid of the shackles of cables, reduce the installation cost, but also greatly improve the scalability of the system. There are some main features for smart home as follows:

(1) The smart home can realize the interaction between the user and the power grid enterprise, obtain the information of electricity consumption and electricity price, set the electricity consumption plan and so on, guide the scientific and rational electricity use and advocate the family's consciousness of energy saving and environmental protection.

(2) Smart home can enhance the comfort, safety, convenience and interactivity of home life, and optimize people's life style.

(3) Smart home can support remote payment.

(4) Smart home can monitor and interact with the home through telephone, mobile phone and remote network, discover the abnormal and timely processing.

(5) The smart home realizes the real-time meter reading and security service of water meter, electric energy meter and gas meter, which provide more convenient conditions for the high-quality service.

(6) Support the smart business of "triple Networks" and perfect intelligent service.

2. Related Background

Related work on smart home privacy has noted the technical and design-demanding challenges and explored potential attacks to identify users and behaviors from records collected from smart environments. In contrast, several papers have suggested layout and evaluation frameworks and proposed structures for data management and visualization in smart environments. The range of proposed solutions for IoT privacy includes design, network, and social technological efforts; But, as Jacobson et al. [20] The term is important in an effort to create a privacy mechanism recognizable to customers. This inspires primarily sociological research for specialization in addition to consumer interplay with IoT devices.

Survey studies have also examined user opinions about IoT privacy. In 2017, Consumers International published the results of international surveys examining consumer opinion about the increasing proliferation of Internet-connected devices across industries. More than 60% of respondents worldwide reported security concerns about the connected items. The survey by Choi et al. And McCreery et al. [29] have indicated that American users are particularly concerned about Internet-connected devices recording and sharing private in-home activities. Martin and Nisenbaum surveyed 569 individuals and found that the use of the data collected was more relevant to users' privacy opinions than the sensitivity of the data. This supports our finding that users weigh privacy risks against perceived benefits. Other large-scale studies of IoT privacy preferences exist. Lee and Kobasa [19] surveyed 200 individuals to classify IoT information collection reference criteria based on respondent responses. Similarly, Emami-Naeni et al. 1,007 participants were surveyed across IoT device cases and scenarios to measure their privacy expectations. Finally, Epthorpe et al. [10] Survey of the perceived acceptability of 1,313 persons of information flow including IoT device, information type, data receiver and collection status. Each of these survey studies has demonstrated that "privacy preferences are diverse and context-dependent", supporting the importance of interview studies to uncover nuanced user opinions and clarify the reasons why survey participants IoT in particular respond to privacy issues.

Apthorpe et al. [14,15] proposed a combinatorial method to obtain privacy norms in the smart home based on the contextual integrity privacy framework. Their methodology is very similar to Lee and Kobsa's and Naeini's [19], and ultimately most similar to our own survey's methodology (i.e., the survey we conducted to collect our training data), given its highly contextual approach to capturing privacy norms in the smart home. They conducted a study which revealed that people may be uncomfortable with entities other than the manufacturer accessing smart home data, and that consent and the ability to use the data for emergencies contribute the most toward increased comfort. On the other hand, targeted advertising and permanent storage contributed the most toward discomfort.

Yongping et al. [23] developed an embedded web server to control equipments employing the Zigbee protocol. For this purpose, they used a S3C2410 microprocessor, which was programmed with Linux 2.6 kernel. To provide online access, a small web server (only 60 KB) named Boa was installed. The authors have designed an interface to communicate with the Zigbee module (MC13192). This is a remote home automation project. The system does not possess any type of intelligence.

3. Architecture of smart home

Through the construction of indoor communication network in the family, we realize the home air conditioning and other smart appliances network by power fiber optic network interconnection. Through the intelligent interactive terminals, smart sockets, smart appliances, etc., we achieve household appliances automatically collect electricity information, analysis, management; and home appliances achieve economic operation and energy control [34]. Through the telephone, cell phone, Internet and other means, the system can remote control home and other services. Through intelligent interactive terminals, we also achieve smoke detection, gas leak detection, anti-theft, emergency assistance and other home security functions, and carry out automatic collection and information management of water meters, gas meters, and support and property management center cell master network, and also achieve home security information authorized one-way transmission and other services. Fig 1 shows the structure of a smart home. Through the service interactive website to achieve customizable information on household electricity information, equipment remote control, payment, newspaper, can service guide and other interactive service functions.

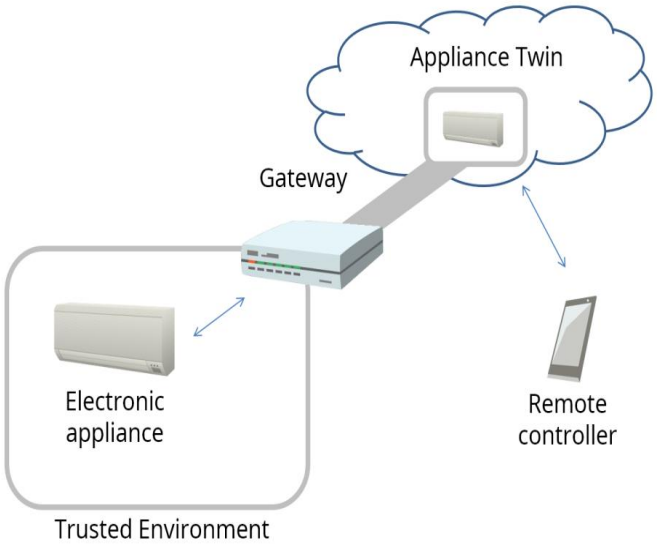


Fig 1. Smart Home Architecture

4. Algorithms and Methods used in Smart Homes

The purpose of the algorithm is to provide intelligence to create an interactive home environment. Location-detection algorithms are derived to gather information about user Location-based activities. Prediction, classification, and summarization algorithms have added functionalities of behavior tracking and activity recognition. Table I illustrates the lists many currently used methods and algorithms.

Artificial Neural Networks (ANNs) can predict the future state of a home environment by detecting usage patterns of home appliances. They can also be utilized to detect and recognize the ADL of the resident. Human behavior modeling is another possible application of neural networks. ANNs require high processing power and hugestorage space for data processing. Vast amounts of information should be used to train an ANN system, which requires a long time to obtain reasonable efficiency. Neural networks are still popular because they do not require any previous knowledge about the home environment or the residents, which is very effective in designing systems as complex as smart homes. The C4.5 algorithm is used to construct the spatiotemporal context of the home user. C4.5 [11] is a popular machine learning algorithm used to classify data according to various data characteristics to predict future behaviors. Smart home researchers have applied C4.5 to match the current behavior pattern of residents of a class of previous patterns to identify states of activity. A major disadvantage of C4.5 is that it requires longer CPU time and additional memory for rule sets.

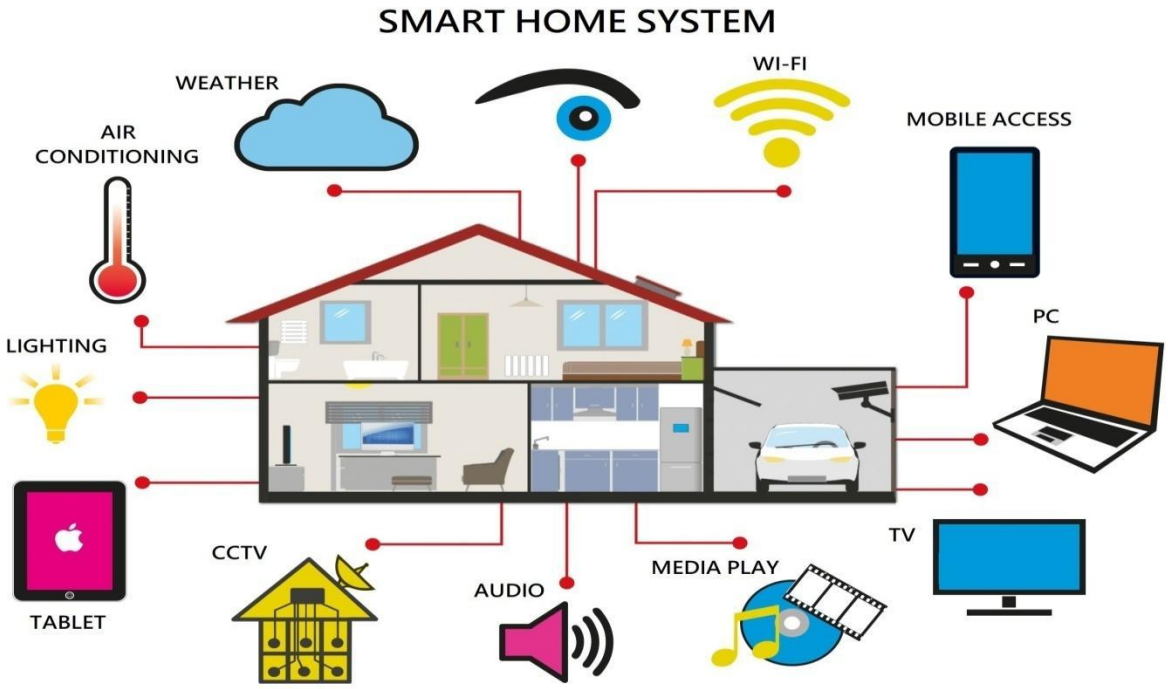


Fig 2. Human Factors in Smart Home TGechnolgy

Bayesian filtering methods are used to determine the location of residents. These methods use the last known position and the last sensor position to improve the accuracy of location prediction. Dynamic Bayesian algorithms can identify ADLs using a hierarchical detection scheme. These methods are derived from statistical inference, which classifies the information collected and filters it according to some predefined rules. Bayesian methods only consider the immediately preceding situation to predict the future.

Fuzzy logic is efficient for home appliance control. Instead of using only binary logic, fuzzy systems use multi-valued logic for logical reasoning. It is popular for controlSystem but not for home intelligence. Multigent systems are effective when different types of agents are used for different purposes, and agents must collaborate with each other by sharing knowledge. Each agent is responsible for its own domain and information, which has a significant impact on overall system performance. In smart homes, multigent systems have been used to simulate agent interactions and work interactions. This is the bestChoice in employing distributed intelligence. This increases overhead processing in cases of improper design and implementation. Algorithms are used to process information and provide services but are limited to specific tasks. Total home automation with proper intelligence is still a dream. Although various methods are being used for location detection, next event prediction, face and hand tracing, ADL recognition and pattern classification, they fail to provide reliable task automation. Bulk processing Information generated from input devices requires advanced data-processing equipment. Using only AI algorithms will never automate a system; Must use system interface The technologies of such interactive displays and voice-recognition systems to understand the needs of the user at any time.

Case Based Reasoning (CBR) and prediction algorithms make decisions based on previous states. Context awareness, a common feature of smart environments, can be achieved byCBR. Active LeZi and other predictive algorithms also work with previous history to predict the ADL of the resident. Recent changes in user behavior take time to reflect back to the system. Statistical predictive algorithms are used to model circadian activity rhythms. The frequent and periodic activity miner (FPAM) algorithm was developed by CASAS at WSA to detect frequent and periodic activity patterns. The user can set policies andprovide feedback to customize the system. SVM can also be applied for activity recognition.

Hidden Markov Models (HMMs) can be applied to create and evaluate behavioral models. Markov models depend on several previous states for prediction. HMMs are used when some states of a Markov model are missing or hidden from the information system. A HMM must be optimized according to the number of states and accuracy.

The C4.5 algorithm is used to build the spatiotemporal context of the home user. C4.5 is a popular machine learning algorithm that is used to classify data according to different data attributes to predict future behaviors. Smart home researchers have applied C4.5 to match the current behavior patterns of inhabitant to a class of previous patterns to recognize states of activity. A major disadvantage of C4.5 is that it requires long CPU times and additional memory for rule sets.

TABLE I
ALGORITHMS AND METHODS USED IN SMART HOMES

Category	Algorithms	Methods
Artificial Neural Network	Artificial Neural Network	Prediction of the future states of homeenvironment [20] Create and evaluate behavioral model [26] Detect and recognize activities of daily life [12]
Multiagent System	Distributed intelligent system	Health monitoring from remote location [22]
	Multiagent system	Simulation of agent interactions and task interactions [14]
Statistical methods	Hidden Markov model To create and evaluate behavioral model	To create and evaluate behavioral model [25]
	Bayesian statistics	ADL recognition [24] To determine location of the inhabitants [29]
	Summarization algorithm	To track any changes in the system [23]
	Statistical predictive algorithm	To model circadian activity rhythms (CARs) [13] To predict activities of daily life(ADL)[19]
C4.5	C4.5	Build spatiotemporal context [11]
Data	Compression	Next Active LeZi[9]
CBR	CBR	Context awareness [30]
Fuzzy logic	Fuzzy logic	Recognize routines and also derivations from routines [20]
		Control lighting system [10]
SVM	SVM	Activity recognition [14]

5. The future home is an attitude, not a technology

House of the Future is not just a collection of Internet-connected gadgets and protocols. A house of the future is a vision - this is why companies must understand the complex emotional motivations inherent in a home. Coupled with this is the fact that we are spending more time at home.

There has been a significant increase in the array of quality services that previously required people to leave home for access to the latest releases on Netflix, from fitness apps and extended delivery services. For many people, there are now very few necessary reasons for leaving home.

When the participants were asked what words they would use to describe the house, they said that darling is the three top things like "comfort", "safety" and "control", but what do those words mean that smart Are far beyond traditional thinking about the house. .
We took a deep plunge into our minds to find out what it means to be comfortable, safe and in control, what makes a person feel "at home", and how the home reflects a person's identity.

6. Smart Home Challenges

Security: Smart home also comes with some security concerns. For instance, hackers can access the network system. They have the ability to control all smart devices especially the security appliances.

Adaption to New Environment: Owning a smart home means having to learn how to use your home that requires you to adapt to many innovations around you such as security systems and many sensors that always detect your movement. Accordingly, it will take reading manuals and learning about how-to of your home.

High Cost of Intelligence: Although smart homes have many properties that makes human's lives convenient, these smart properties are in a higher price tag. The cost of an intelligent home is high because some of the technology is relatively new. However, mostly of home automations are just a few advances that are standard in a new home, the cost of other aspects can be expensive as well.

6.1 Standards: Standardization is very essential for IoT environment as it is expanding globally. Challenges are comes related which standard should be used, which will provide secure medium, how it will make system more reliable.

6.2 Identification: Identification is required for each device so that each device can identify uniquely.

6.3 Privacy: The user's data should be confidential. Connection should be done with providing privacy.

6.4 Authentication: Authentication is must to secure Smart Home system from an attacker. Server has to give access only authentic users.

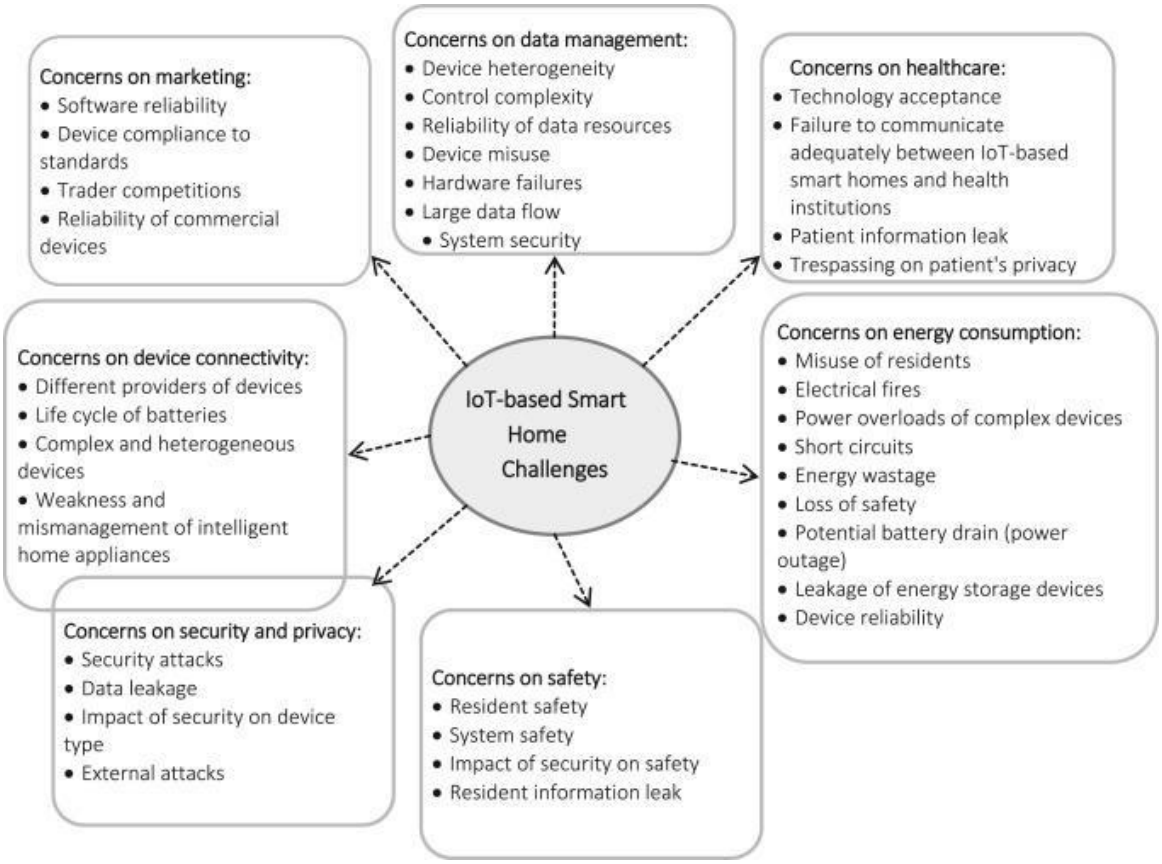
6.5 Security: The system should able to take appropriate actions on security threats. And system should be able to reconfigure by itself after attacks.

6.6 Integration: The main challenge with IoT is to integrate applications in IoT environment.

6.7 Coordination: Coordination is required between the globally connected objects, humans, programs, process, etc.

6.8 Data Storage: As applications of IoT are increasing, the amount of data getting collected is huge. The challenge is where to storage the huge data. Huge database can solve this problem. Artificial intelligence algorithms must be applied to extract meaning data from redundant data.

6.9 Network Self-Organization: Network structure should be created in such a way that every device connected to it could self-organize them. Actually it is network which should be able to self-organize.



7. Smart Home Tech Influences

The world of architectural design can change dramatically with these new freedoms, requirements and trends:

1. Reducing the visibility of outlets and switches. Smart homes will be built on wireless infrastructure, with almost every device located in a fixed location and connected to the Internet. We will be able to control lights and devices remotely via mobile devices, and we may be able to wirelessly thank those devices for wireless electrical charging. As a result, architects will take additional measures to reduce the visibility of outlets and switches within the home for greater aesthetic value.

2. Making the space more open and accessible. When a house is tightly interconnected and every aspect is controlled from any place, dividing the space is less necessary and less functional. This will become easier and more conducive to creating larger, more open, accessible locations within homes. It also helps that our appliances can be smaller and more compact, allowing easy accommodation of TVs, ovens and other appliances without cramping any individual room.

3. Allow more room for room integration. Since the characteristics of the house can be controlled from anywhere, the balance of power between the rooms will be constant. Rather than being the central focal point of a single room, architects will do more with each other to work with other rooms, creating a smoother foud between rooms in the home, and allowing more room-to-room integration.

4. Lowering limits for wires. Again, since most smart home technology will be wireless, architects will have less to worry about power and wiring. Since an architect's job is to strike a balance between form and function, the elimination of a key function provides more breathing

space for the form, lending power and prioritizing more artistic designs and greater freedom when arranging home layouts. Will do.
5. Seasonal and dependent facilities. Because smart homes can adapt automatically to a variety of situations (such as closing the blinds on hot summer days or running the fans automatically when it reaches a certain temperature), architects are especially concerned about the exterior of the home. May include flexible or transformative housing facilities. The possibilities here are limitless, and may eventually involve changing the entire design of the exterior based on mood, weather, or other variables.
It is difficult to say how the architectural landscape is going to change, as it is difficult to say how smart home technology is going to evolve. For the past few years, a fully fledged, integrated digital home system seemed right around the corner, but most smart devices still disappoint. And yes, it is a technical breakthrough to change the game forever. We can all see at this point how technology and architecture develop and influence each other, and stay active while adopting new trends.

CONCLUSION

This paper based on the meaning of smart home and the details of smart home elements. And the main objective of this paper is to give a survey for these smart home researches and summarily describe the details about smart home. This paper based on the meaning of smart home and the details of smart home elements. And the main objective of this paper is to give a survey for these smart home researches and summarily describe the details about smart home.

Smart-homes are the requirement of today's fast moving life and busy schedules. There must be some systematic arrangement for the daily routine jobs so that one can easily concentrate on his/her other significant jobs. This paper proposes an architecture for IoT enabled smarthomes.This work also addresses the job Instruction set required to perform the tasks in an efficient and mannered way. This work focuses on the efficient structure and necessary services expected by the smart-homes.

References

[1] K. Moser, J. Harder, and S.G.M. Koo, "Internet Of Things In Home Automation And Energy Efficient Smart Home Technologies," *Proc. 2014 IEEE Int'l Conf. Systems, Man, And Cybernetics* (SMC 14), 2014; doi.org/10.1109/SMC.2014.6974087.

[2] M. Meeker, "Internet Trends Of 2016—Code Conference," blog, KPCB, June, 2016; http://www.kpcb.com/blog/2016-internet-trends-report.

[3] R.H. Jensen et al., "Designing The Desirable Smart Home: A Study Of Household Experiences And Energy Consumption Impacts," *Proc. 2018 CHI Conf. Human Factors In Computing Systems* (CHI 18), 2018; doi.org/10.1145/3173574.3173578.

[4] A. Pradhan, K. Mehta, and L. Findlater, "'Accessibility Came By Accident': Use Of Voice-Controlled Intelligent Personal Assistants By People With Disabilities," *Proc. 2018 CHI Conf. Human Factors In Computing Systems* (CHI 18), 2018; doi.org/10.1145/3173574.3174033.

[5] M. Porcheron et al., “Voice Interfaces In Everyday Life,” *Proc. 2018 CHI Conf. Human Factors In Computing Systems* (CHI 18), 2018; doi.org/10.1145/3173574.3174214.

[6] B. Ur et al., “Practical Trigger-Action Programming In The Smart Home,” *Proc. SIGCHI Conf. Human Factors In Computing Systems* (CHI 14), 2014, pp. 78–82.

[7] J.-b. Woo and Y.-k. Lim, “User Experience in Do-It-Yourself-style Smart Homes,” *Proc. 2015 ACM Int’l Joint Conf. Pervasive And Ubiquitous Computing* (UbiComp 15), 2015, pp. 78–82.

[8] Mohd Sallauddin, "IoT Middleware for Device Privacy on Big Data" in *International Journal of Innovative Research in Science, Engineering and Technology*, Volume 5, Issue 6, Page No(s) 10266 - 1027, JUN. 2016, ISSN. 2319-8753.

[9] C. Sas and C. Neustaedter, “Exploring DIY Practices Of Complex Home Technologies,” *ACM Trans. Computer-Human Interaction*, vol. 24, no. 2, 2017; doi.org/10.1145/3057863.

[10] J. Brich et al., “Exploring End User Programming Needs In Home Automation,” *ACM Trans. Computer-Human Interaction*, vol. 24, no. 2, 2017; doi.org/10.1145/3057858.

[11] Noah Apthorpe, Yan Shvartzshnaider, Arunesh Mathur, Dillon Reisman, and Nick Feamster. 2018. Discovering smart home internet of things privacy norms using contextual integrity. Proceedings of IMWUT 2, 2 (2018), 59.

[12] Singh, Rajesh, Gehlot Anita, Shiv Capoor, Geeta Rana, Ravindra Sharma, and Shivani Agarwal. "Internet of Things Enabled Robot Based Smart Room Automation and Localization System" In Internet of Things and Big Data Analytics for Smart Generation, pp. 105-133. Springer, Cham, 2019.

[13] G. Sunil, Sallauddin Mohmmad, Kanegonda Ravi Chythanya, “The Current Status and Research in Industrial Bigdata Analysis in Smart Intelligent Systems”, Vol. 8, Issue No. 8, 2017, doi.org/10.26483/ijarcs.v8i8.4859.

[14] Lohan, Vibha, and Rishi Pal Singh. "Home Automation using Internet of Things." In Advances in Data and Information Sciences, pp. 293-301. Springer, Singapore, 2019.

[15] Somayya, R.; Ramaswamy, R. Smart homes. In Proceedings of the 2nd International Symposium onComputational and Business Intelligence, New Delhi, India, 7–8 December 2014.

[16] Noah Apthorpe, Dillon Reisman, and Nick Feamster. 2016. A smart home is no castle: privacy vulnerabilities of encrypted IoT traffic. Workshop on Data and Algorithmic Transparency (2016).

[17] Noah Apthorpe, Yan Shvartzshnaider, Arunesh Mathur, Dillon Reisman, and Nick Feamster. 2018. Discovering Smart Home Internet of Things Privacy Norms Using Contextual Integrity. Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies (2018).

[18] Abdullahi Arabo, Ian Brown, and Fadi El-Moussa. 2012. Privacy in the age of mobility and smart devices in smart homes. In Privacy, Security, Risk and Trust (PASSAT),

2012 International Conference on and 2012 International Confernece on Social Computing (SocialCom). IEEE, 819–826.

[19] K. Seena Naik and E. Sudarshan, Smart Healthcare Monitoring System Using Raspberry Pi on Iot Platform, ARPN Journal of Engineering and Applied Sciences, Vol. 14, No. 4, Feb 2019, pp 872-876.

[20] JefAusloos, Els Kindt, Eva Lievens, Peggy Valcke, and Jos Dumortier. 2013. Guidelines for privacy-friendly default settings. ICRI Research Paper No. 12 2013 (2013).

[21] Nellie Bowles. 2018. Thermostats, Locks and Lights: Digital Tools of Domestic Abuse. https://www.nytimes.com/2018/06/23/technology/smart-home-devices-domestic-abuse.html. The New York Times (23 June 2018).

[22] AJ Brush, Bongshin Lee, Ratul Mahajan, Sharad Agarwal, Stefan Saroiu, and Colin Dixon. 2011. Home automation in the wild: challenges and opportunities. In proceedings of the SIGCHI Conference on Human Factors in Computing Systems. ACM, 2115–2124.

[23] Joseph Bugeja, Andreas Jacobsson, and Paul Davidsson. 2016. On Privacy and Security Challenges in Smart Connected Homes. In Intelligence and Security Informatics Conference (EISIC), 2016 European. IEEE, 172–175.

[24] Lina Dencik and Jonathan Cable. 2017. The advent of surveillance realism: Public opinion and activist responses to the Snowden leaks. International Journal of Communication 11 (2017), 763–781.

[25] Serge Egelman. 2009. Trust me: Design patterns for constructing trustworthy trust indicators. Technical Report. CarnegieMellon University School of Computer Science.

[26] Murray Goulden, Peter Tolmie, Richard Mortier, Tom Lodge, Anna-KaisaPietilainen, and Renata Teixeira. 2018. Living with interpersonal data: observability and accountability in the age of pervasive ICT. New Media & Society 20, 4 (2018), 1580–1599.

[27] A-Reum Jung. 2017. The influence of perceived ad relevance on social media advertising: An empirical examination of a mediating role of privacy concern. Computers in Human Behavior 70 (2017), 303–309.

[28] Jialiu Lin, Bin Liu, Norman Sadeh, and Jason I Hong. 2014. Modeling users' mobile app privacy preferences: Restoring usability in a sea of permission settings. In Symposium on Usable Privacy and Security (SOUPS).

[29] Dominique Machuletz, Henrik Sendt, Stefan Laube, and Rainer Böhme. 2016. Users protect their privacy if they can: Determinants of webcam covering behavior. In Proceedings of the European Workshop on Usable Security (EuroUSEC'16). Internet Society, Reston, VA, USA.

[30] Sandeep Ch, Kumar S Naresh, Kumar P Pramod,Security challenges and issues of the IoT system, Indian Journal of Public Health Research & Development, Vol. 9, Issue 11, pp 748-753, November 2018, ISSN 0976-0245.

[30] Kirsten Martin and Helen Nissenbaum. 2016. Measuring privacy: an empirical test using context to expose confounding variables. Colum. Sci. & Tech. L. Rev. 18 (2016), 176.

[31] Kelly D Martin and Patrick E Murphy. 2017. The role of data privacy in marketing. Journal of the Academy of Marketing Science 45, 2 (2017), 135–155.

[32] Faith McCreary, Alexandra Zafiroglu, and Heather Patterson. 2016. The contextual complexity of privacy in smart homes and smart buildings. In International Conference on HCI in Business, Government and Organizations. Springer, Proc. ACM Hum.-Comput. Interact., Vol. 2, No. CSCW, Article 200. Publication date: November 2018. User Perceptions of Smart Home IoT Privacy 200:19 67–78.

[33] Emily McReynolds, Sarah Hubbard, Timothy Lau, Aditya Saraf, Maya Cakmak, and Franziska Roesner. 2017. Toys that listen: A study of parents, children, and internet-connected toys. In Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems. ACM, 5197–5207.