Smart Home based on Internet of Things and Ethical Issues

Victor Chang[1][a], Zhi Wang[2], Qianwen Ariel Xu[1,2], Lewis Golightly[1], Ben S. Liu[3] and Mitra Arami[4]

[1]*Artificial Intelligence and Information System Research Group, School of Computing, Engineering and Digital Technologies, Teesside University, Middlesbrough, U.K.*

[2]*IBSS, Xi'an Jiaotong-Liverpool University, Suzhou, China*

[3]*Department of Marketing, Quinnipiac University, U.S.A.*

[4]*EM Normandie Business School, France*

Keywords: Smart Home, Ethics, Internet of Things, Data Analytics.

Abstract: With the growing popularity of the Internet of Things, smart home applications are developing gradually and bring convenience to users' lives. In this paper, first, an overview of IoT and widely agreed and accepted three-layer architecture of IoT are introduced. Next, this paper discusses the basic features of the smart home and data analytics in a smart home with the benefits and analysis process. Security and privacy are the key ethical problems in the smart home, such as security attack, analysis of "non-sensitive" data, improper information collection and data abuse. Additionally, the user perception of privacy issues is included in this paper. Furthermore, this paper recommends suitable suggestions for improving ethical issues.

1 INTRODUCTION

The Internet of Things (IoT) is a crucial component of emerging information technologies and an extension of Internet applications. Automated work and connection of devices used in daily life via the Internet are the basic concepts behind IoT (Burhan et al., 2018). Data from the physical world collected by devices attached to each object is processed and analyzed and finally used to perform the actions. IoT has covered many areas, such as the health care domain, smart home, smart transportation, infrastructure management, etc. (Burhan et al., 2018). This paper will focus on smart home, which brings ordinary home the characteristics of intelligence, remote control and interconnection. It is one of the most representative components in the IoT era (Yassin et al., 2019). Apart from the introduction of the IoT and smart home, ethical issues, such as security and privacy, and the suggestions will be discussed in this article.

2 INTERNET OF THINGS (IoT)

2.1 Introduction of IoT

The meaning of the IoT is a vast network connected by a variety of objects or processes through various information sensing devices for intelligent recognition, positioning, tracker, surveillance, and management with the presence of the Internet (Leng et al., 2020). The aim of the IoT is to connect all physical things in communication so that they can be integrated with computer-based systems more directly and the identification, management, and control can be simplified. (De Cremer, Nguyen & Feamster, 2017). The Internet of Things can bring benefits and services to individuals, businesses and societies by capturing and analyzing data from sensors at the endpoints of connected devices and combining these data (Nguyen and De Cremer, 2016). Furthermore, IoT improves comfort and efficiency through collaboration between smart objects (Risteska Stojkoska & Trivodaliev, 2017). It can be applied in numerous aspects, including personal health, public safety, industrial monitoring, intelligent transportation, environmental protection

[a] https://orcid.org/0000-0002-8012-5852

Chang, V., Wang, Z., Xu, Q., Golightly, L., Liu, B. and Arami, M.
Smart Home based on Internet of Things and Ethical Issues.
DOI: 10.5220/0010178100570064
In *Proceedings of the 3rd International Conference on Finance, Economics, Management and IT Business (FEMIB 2021)*, pages 57-64
ISBN: 978-989-758-507-4

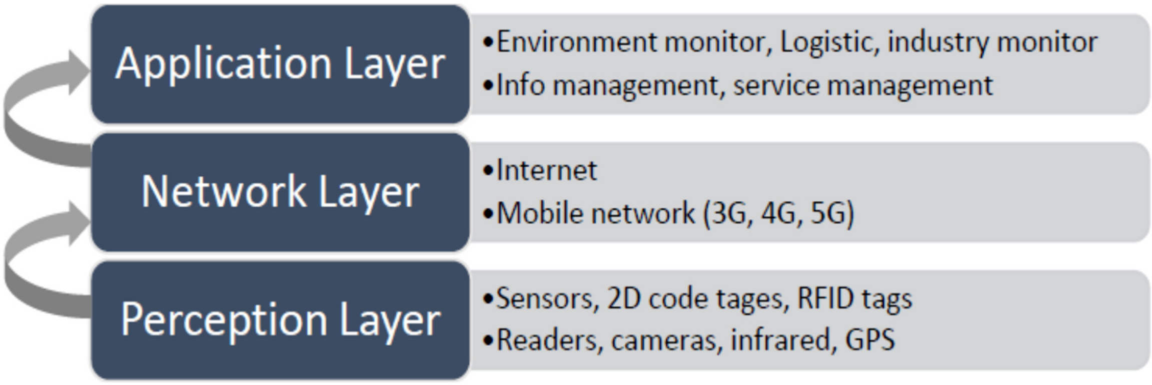
Application Layer
•Environment monitor, Logistic, industry monitor
•Info management, service management
Network Layer
•Internet
•Mobile network (3G, 4G, 5G)
Perception Layer
•Sensors, 2D code tages, RFID tags
•Readers, cameras, infrared, GPS

Figure 1: Three-layer architecture of IoT.

and other fields. For example, in the manufacturing field, the equipment can be remotely monitored, upgraded and maintained from a long distance away by installing IoT based sensors on the equipment. Moreover, the equipment manufacturers are able to learn the use of the products in a better way, collect the data of the product life cycle completely, thereby guiding the product design and after-sales service (Lee and Fumagalli, 2019).

2.2 IoT Layered Architectures

Building a capable IoT architecture is beneficial to the fast, reliable, and secure integration of information technology and communication technologies (Kumar & Mallick, 2018). In general, as is shown in Fig. 1, the architecture of the IoT has three layers, namely, the perception layer, the network layer and the application layer.

The three-layer architecture is a fundamental and widely agreed architecture proposed at the beginning of the development of IoT (Burhan et al., 2018).

The perception layer is named the sensing layer as well, whose feature is to identify objects and gather environmental data. It contains a variety of sensors, consisting of RFID tags and readers, temperature and humidity sensors, Global Positioning System, cameras, infrared, two-dimensional code tags, as well as other sensing terminals. It is similar to the role of skin and facial features in the human body structure. The network layer is the whole IoT's hub, which is in charge of the transmission and processing of data obtained by the perception layer with the internet connectivity of devices (Kumar & Mallick, 2018). It contains a number of networks, consisting of the Internet, WAN, a network management system, and a cloud computing platform. The network layer is similar to the nerve center and brain of the human body structure. The application layer is the interface, which connects the IoT with users. Its primary function is to analyze and process the information from the network layer, make correct control and decision, and realize intelligent management applications and services.

3 SMART HOME BASED ON IoT

A smart home (SH) is an essential application of IoT and it comes into the picture to control and monitor the home (Geneiatakis et al., 2017). The trends of search popularity since 2013 for the terms: smart home, IoT are shown in Fig. 2. It is demonstrated that there is an increasing trend for smart home and IoT, according to Fig. 2. By combining different kinds of IoT based, the smart home provides a variety of functions, e.g., lighting control, household appliances control, telephone remote control and others (Alaa et al.,2017). Compared to conventional homes, the smart home has ordinary residential functions and is also equipped with functions of home establishment, networking, intelligent appliances, and equipment automation. Additionally, all-around interaction capabilities are provided, and even related costs are reduced on various energy consumption (Marikyan et al., 2019).

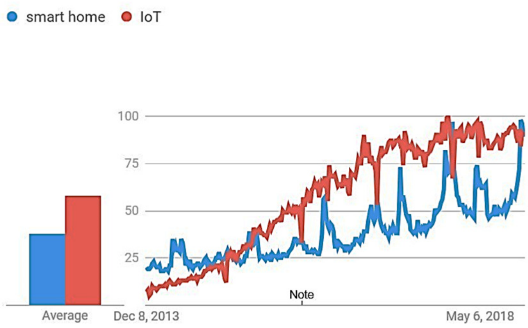

Figure 2: Interest over time according to Google trends since 2013 for terms: Smart home and IoT.

Table 1: Features of Smart Home.

Smart home Devices	air conditioning control, network appliances, lighting systems, digital cinema systems, security systems, audio and video equipment, curtain control, etc.
Smart Home Functions	home appliance control, lighting control, telephone remote control, indoor and outdoor remote control, burglar alarm, environmental monitoring, infrared forwarding and programmable timing control, etc.

Referring to Table 1, under the notion of SH, there are some important components, and a brief introduction to some of them is given. One is home automation, an essential system of the SH. It refers to integrating or controlling electronic appliances in the house (MIHALACHE, 2017), consisting of systems of lighting, security, video and audio, computer equipment, heating, and air-conditioning. A Central Processor Units is set to receive the data from electronic and electrical devices and then send specific information to other devices with some procedures. It can control the devices by using interfaces like mobile phones, remote controllers, computers, etc. Home Network is also a vital part of the SH. It is a family information platform that links the PCs, household electrical appliances, safety systems, lighting systems and WAN in smart homes, implements equipment management, and data and multimedia information sharing (Tetteh & Amponsah, 2020).

4 DATA ANALYTICS IN SMART HOME

4.1 Benefits of Data Analytics in Smart Home

Through intelligent devices linked to the IoT system, SH can generate a massive amount of data (El-Sayed et al., 2018). In the face of data with information, how to transmit, store, analyze, and apply, it is a tremendous opportunity and challenge in the current era for the smart home. Analyzing these data in almost real-time or off-line has a significant effect on the economy, health, and safety of the society, as the useful information implicit in the data can be derived (Yassine et al., 2019). Take an example mentioned in Yassine's paper (2019)- manufacturers can continuously analyze the data of devices under the permission of IoT applications and then take measures to develop equipment maintenance plans or replace faulty equipment immediately. It can be revealed that data analytics in a smart home can summarize the behavior rules of smart home occupants and it can enhance the convenience and efficiency of daily life.

4.2 Data Analysis Process in Smart Home

The paper will briefly introduce a kind of big general data analysis and recommendation for SH (Rathore et al., 2017). The SH generates an enormous amount of data with different formats, sources and periods because various types of sensors produce them. As the raw data is messy and has much more metadata than actual measurements, it is necessary to apply registration and filtering technology to filter unnecessary metadata and discard the repeated data. Then, by using different communication technologies through the Internet, the data is transmitted from the relay towards the gateway node, and then from the base station to the internet cloud. Tightly related data can be grouped into a collection, which can be processed more effectively. Afterward, it is filtered and classified using different algorithms. After passing through the transformer, preprocessed data will be stored in the database and processed (such as statistical analysis, professional computing, and data mining) in a stable system. Finally, the interpretation, prediction, and visualization results are used to make smart home applications and reports generated intelligently. During this process, the quality and availability of the data should also be considered, as well as the privacy-protecting-and-detecting environment (Lee, 2018). See Fig. 3.

5 ETHICAL ISSUES IN SMART HOME

Apart from the benefits of data analytics for smart homes, smart home raises substantial ethical issues in different ways and aspects when analyzing and applying data. The problems have aroused public

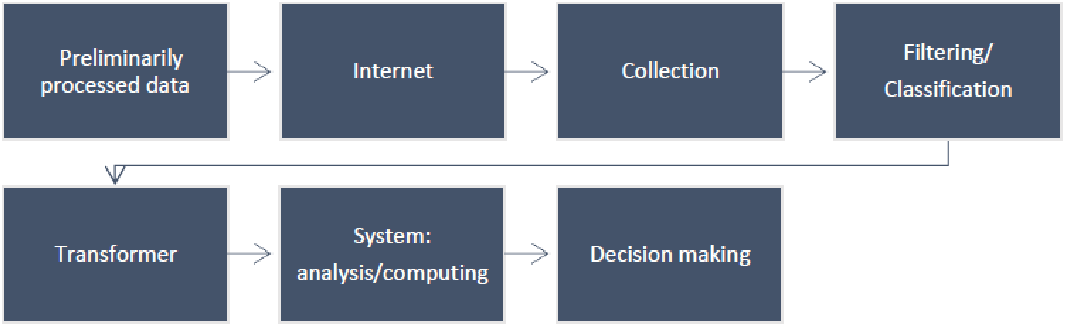
Preliminarily processed data
Internet
Collection
Filtering/ Classification
Transformer
System: analysis/computing
Decision making

Figure 3: The IoT-based big data analysis process.

applying data. The problems have aroused public attention, including individuals, companies and the government. In the following paper, the basic concepts, ethical issues and the threats they pose will be discussed.

5.1 Security and Privacy Threats

Among the ethical issues in smart homes, data security and personal privacy are the most important and concerning issues (Guo et al., 2019; Butun et al., 2019). A considerable amount of sensitive personal information is collected by sensors from the occupant's private space and is transmitted through the Internet. Security is related to data protection from tampering, alteration, or disclosure for incidental or malicious reasons. Privacy mentioned in this paper is the appropriate collection, analysis and sharing of personal data (Shave, 2018). The two concepts will be discussed together in this article as they are inseparable.

5.1.1 CIA Triad Model

While speaking of information security or data security, the basic concept of information security CIA should be introduced, whose principle is to ensure data protection and information systems (Shave, 2018). CIA is short for Confidentiality, Integrity and Availability (Zheng et al., 2014). Confidentiality refers to prevent the data from being accessed by unauthorized users. In order to maintain confidentiality, several protective approaches like encryption or permission are often implemented when processing, transmitting and storing data for security control. The integrity of information refers to that the original data should be prevented from being changed arbitrarily during the process of data storage or transmission. Consequently, to maintain integrity, strict control is required on the identity authentication and data access. The availability of information stands for the information available to the legitimate owners and users of the information in a timely manner and whenever they need it (Shave, 2018). The core of information security is to make sure that the raw data can be timely and securely transferred or stored between its legal owners and users without being destroyed. It cannot be obtained or changed by those who should not obtain them.

5.1.2 Security Attacks

One of the troubles about security and privacy in the SH is the unknown vulnerabilities. With the innovation and development of big data storage, computing and analysis, it has driven a new revolution in the software and hardware architecture of information systems. Following this trend, smart home appliances are continuously being updated. It may introduce unknown vulnerabilities in software, hardware, protocols and devices because the speed of discovering and fixing vulnerabilities is not keeping up with the speed of updating. The existing security protection technologies cannot withstand the security risks of unknown vulnerabilities. Simultaneously, the development of big data technology has spawned a new type of advanced cyber-attack. Hackers can maximize the collection of useful information, such as phone calls, home addresses, even private information within the family to prepare for attacks and make attacks more accurate. Hacking and unauthorized access can pose one of the most direct threats to personal privacy in a smart home environment. Unknown vulnerabilities combined with new cyberattacks make intelligent home systems vulnerable to attacks, causing serious security and privacy concerns. According to Geneiatakis et al.'s (2017) analysis, eavesdropping, simulation, DoS, and software development attack vectors can pose serious privacy hazards to existing smart home IoT infrastructure under certain conditions. The emerging threats of security and privacy will be divided into three parts under the three-layer architecture. This paper will mainly focus on the perception layer.

First of all, security threats in the perception layer are mainly carried out in the following three ways:

- Physical Attack: The attacker implements physical damage to prevent the IoT terminal from performing properly or stealing terminal equipment and generating users' sensitive data by cracking.
- Eavesdropping: Eavesdropping is a means of network attack. It is to steal data resources and sensitive data by a variety of feasible legal or illegal approaches in real-time. In a smart home, to manage it, users generally adopt two interactive modes to interact with IoT devices through different platforms such as personal computers, smartphones, and tablets. One modality is to use the hub's connectivity and services directly and the other is to access Internet cloud services, which are interrelated with IoT hubs and linked IoT devices (Geneiatakis et al., 2017). During this process, an attacker can intercept information transmitted via a network, which means that eavesdropping happens. For example, hackers can use security holes to watch real-time home surveillance video. They can obtain a large amount of personal privacy information by monitoring videos, such as the living habits and behavior patterns of the occupants.
- Simulation Attack: Through deceiving the communication system (or user), illegal users are disguised as rightful users or privileged users. Then, attackers can control the smart home system and extract sensitive information from it; that is to say, hackers can have the same permissions as the owner and can operate various smart home components. This kind of active attack affects the user's privacy and the confidentiality of the services provided and influences data integrity (Geneiatakis, 2017).

Second, in the network layer, there are also several kinds of security threats, including DoS Attack, Storage Attack, Exploit Attack and Fake base station attack. Among them, Dos Attack and Exploit Attack are introduced as follows:

- Denial of Service Attack (DoS): The most frequent means of a denial of service attacks is to use legitimate service requests to occupy too many service resources, thereby overloading the server and making it unable to respond to other requests typically.
- Exploit Attack: Exploiting is a crucial way to gain control of the system. The user finds a vulnerability from the target system and then uses it to obtain permission to control the target system (Burhan et al., 2018).

Finally, the False Terminal Trigger threat often takes place in the application Layer. An attacker is able to trigger the maloperation of the terminal by sending fake messages to the terminal through SMS.

All types of security threats in different layers are shown in Table 2.

5.1.3 Analysis of “Non-sensitive” Data

Another key point that needs attention is that personal data can be indirectly generated from "non- sensitive" information. The data seems to be irrelevant to personal information, but using big data techniques for in-depth correlation analysis and mining will reveal useful information. For example, it is demonstrated that even in the case of device encryption, the privacy-sensitive home activity can be inferred by analyzing the Internet traffic in smart homes through Internet Service Provider (ISP) or other network observers (Apthorpe et al., 2017). Many intelligent devices in smart homes have sensors always connected to the Internet and for some devices, and the traffic rate is affected by different user activities. By drawing the send/receive rates of the specific equipment's streams, attackers can observe fluctuations to infer the user activities (Apthorpe et al., 2017). Taking an example in Apthorpe's paper (2017), by observing the send/receive rate of Sense Sleep Monitor, it is possible to infer the user's working and sleeping time because it would reach the peak when the user activity happens.

Table 2: Security Threats in Different Layers.

PERCEPTION *LAYER*	Physical Attack, Eavesdropping, Simulation Attack, Replay Attack, Timing Attack
NETWORK *LAYER*	DoS Attack, Storage Attack, Exploit Attack, Fake base station attack
APPLICATION *LAYER*	Cross-Site Scripting, False Terminal Trigger

In Zheng's article (2018), the authors brought forward the view that not only A/V (audio/video) devices in the smart home should be paid attention to, but also the non-A/V devices should be watched out for the privacy risks. As the concepts of smart home data are generally divided into two part: "sensitive" and "non-sensitive", it is a risk to show no skepticism about "non- sensitive" data with unaware of the data analysis capabilities of inferring sensitive information from "non-sensitive" data.

5.1.4 Improper Information Collection

Whether personal information can be reasonably collected, used and cleared is also an important issue. In big data scenarios, the omnipresent data gathering techniques and numerous varied data processing techniques pose significant challenges to people's privacy protection in this area. Data information collection is basically "automatically" implemented by computer networks and smart applications in different smart home devices. As data collection becomes more convenient and low-cost, the imperfection of legal regulation leads to the confusion of the object of data collection. Some data is collected without the user's knowledge or consent. Another possibility is that although users agree with the applications or devices to collect data, they do not really understand the content and purpose of the collected data or lack sufficient freedom of choice (Mantelero, 2017). For example, users have to accept all the data collection terms if they want to use the service. If the users want to withdraw their consent, it is difficult because of the complex data processing and the unfriendly digital interfaces (Mantelero, 2017). The vast amount of information collected, coupled with increasingly intelligent analytical tools, will make big data controllers aware of almost everything related to individuals in the home, which is a situation that everyone is not willing to face.

5.1.5 Data Abuse

Personal information abuse is inevitable due to the pursuit of maximizing the value of data, putting personal privacy at risk. There is an inevitable conflict between the appeal of open and shared big data resources and protecting personal privacy. Because of the unclear rights and responsibilities of data collection and use, some public departments and large companies over-collect, occupy data and infringe on data information owners' legitimate rights and interests. When data is collected, how the data will be used or analyzed is not always known or expected because of the complexity of data analytics (Mantelero, 2017). Moreover, owners lose control of the data after it has been collected. Some people or companies have the ability to occupy and utilize substantial data resources in a better way, while it is hard for others to do the same thing. This forms a data gap and creates a problem of unfair distribution of information dividends, which intensifies differences between groups and social conflicts. Back to the smart home, on the one hand, service providers need to analyze daily data generated from smart homes to improve service quality. On the other hand, over-analysis of data may reveal privacy that some residents do not want others to know.

5.2 Other Ethical Issues

Besides security and privacy issues, some other ethical issues and malicious behavior of enterprises are among them. For example, for consumers to continue to use their products, some smart home enterprises would intentionally create a complex IoT ecosystem where only their own products can be applied. In order to adapt to the system, consumers have to choose the company's products when they want to add new smart home products. The company may also sign complicated contracts with users, making it difficult for them to change to other IoT systems (Cremer et al., 2016).

6 INDIVIDUAL PERCEPTION

As there are various ethical issues in smart homes, it is vital to understand users' perceptions better. In Zheng's article (2018), researchers interviewed some smart homeowners ranging from 23–45 years about their views on the privacy of smart homes and they came to some conclusions through analysis. This paper will briefly summarize some noteworthy individual perception in Zheng's article. Smart home users can accept the risk of personal privacy leakage in exchange for the convenience and connectedness of smart homes to a certain extent. However, they hold different views on different entities collecting and accessing data, such as manufactures, advertisers, Internet Service Providers and government. Owners are most concerned about the government and pay the least attention to manufacturers because they believe it is necessary and reasonable for manufactures to improve their devices by accessing their usage data. Furthermore, smart home users tend to trust big brands before they thoroughly understand, although some do not take adequate measures to protect personal privacy. One of the implied reasons is that individuals are unwilling to spend time and energy, protecting personal privacy and rationalizing their behavior by trusting big brands.

7 SUITABLE RECOMMENDATIONS FOR ETHICAL ISSUES

As smart home gradually enters more people's lives, the ethical issues related to it have raised concerns of smart home shareholders. For the purpose of protecting data security and privacy and improve other ethical problems, many methods can be proposed in different aspects.

7.1 Data Security

For technology, personal data should be minimized for privacy protection. The privacy level of collected data by the smart home environment should be evaluated and data is supposed to be processed before implementing the SH system (Lee, 2017). Data segmentation is one of the conventional methods for data protection. It refers to the division of logically unified data into smaller, independently manageable physical units for storage. By partitioning data, personal data can be processed and analyzed separately, reducing privacy leakage risk. Another advanced method is data aggregation, referring to the process of selecting, analyzing and categorizing the relevant data, and finally obtaining the desired results. For smart homes, the greatest aggregation level and the least amount of details should apply to personal data (Lee, 2017). Additionally, differential privacy technology can be mentioned. Its function is using cryptographic algorithms to "encrypt" the user's information to the server. The company can calculate the user group's behavior patterns through the "encrypted" data, but cannot resolve the data of the individual user. This mechanism makes sure that each individual's data will not be revealed. Simultaneously, it is still not difficult for the outside world to understand the general statistical information of the dataset. (Tsou et al., 2017).

7.2 Manufacturers and Service Providers

For manufacturers of smart home devices and the service providers, they should also take responsibility. They must be responsible for protecting the collected user's personal information and preventing information leakage, damage, or loss. Personal data collected by them may not be altered since it may not be provided to others without the data owners' consent. The data information collector must use the obtained data information following the prescribed or agreed use, and may not be used for other purposes. Moreover, they should provide more natural ways for users to handle their private data. For example, it is suggested that smart home applications allow users to check and choose the data they want to be recorded or analyzed, and should also allow them to delete their data (Zheng et al., 2018).

7.3 Individuals

For smart home occupants, they need to raise their personal consciousness and use related security technologies. In the era of big data, it is necessary for everyone to take the initiative to learn this knowledge and understand the potential risks that may exist in this area elated to personal privacy disclosure, so as to learn the method of protecting their private data from being leaked. It is very important for the consumers to pay attention to the issues related to personal privacy and data security when they purchase smart home products and carefully check the privacy policy at the beginning of use as well.

8 CONCLUSION

This paper firstly reviews the concept and three-layer structure of the IoT and introduces the smart home established on IoT with its benefits and components. Data analytics in a smart home is mentioned, which is the core of the smart home and brings many benefits. A kind of big general data analysis implementation is discussed for understanding the data analyzing process in a smart home. Besides the convenience of smart homes, it also poses challenges in ethical areas, mainly data security and privacy. Attack and analysis of "non-sensitive" data can cause threats to personal information security. Data collectors may gather information improperly and abuse private data. Under this situation, the smart home occupant's perception is summarized, showing immature ideas in some aspects. Finally, there are some recommendations made for different objects, such as users, manufacturers. In conclusion, data analytics in the smart home makes users live more convenient and interconnected, but more considerations should be taken to solve ethical issues.

ACKNOWLEDGEMENTS

This work is supported by VC Research (grant number VCR 0000095).

REFERENCES

Alaa, M., Zaidan, AA, Zaidan, B.B., Talal, M.& Kiah, M.L.M. (2017). 'Review: A review of smart home applications based on Internet of Things', Journal of Network and Computer Applications, 97, pp. 48–65. doi: 10.1016/j.jnca.2017.08.017.

Apthorpe, N., Reisman, D., Sundaresan, S., Narayanan, A., & Feamster, N. (2017). Spying on the smart home: privacy attacks and defenses on encrypted iot traffic.

Apthorpe, N., Reisman, D. & Feamster, N. (2017). 'A Smart Home is No Castle: Privacy Vulnerabilities of Encrypted IoT Traffic'.

Burhan, M., Rehman, R. A., Khan, B. & Kim, B.-S. (2018). 'IoT Elements, Layered Architectures and Security Issues: A Comprehensive Survey', Sensors (14248220), 18(9), pp. 1–37. doi: 10.3390/s18092796.

Butun, I., Osterberg, P., & Song, H. (2019). Security of the Internet of Things: Vulnerabilities, Attacks and Countermeasures. IEEE Communications Surveys & Tutorials, vol. 22, no. 1, pp. 616-644. doi:10.1109/ comst.2019.2953364

Cremer, D. D., Nguyen, B., & Simkin, L. (2016). The integrity challenge of the internet-of- things (iot): on understanding its dark side. Journal of Marketing Management, 33(1-2), 145- 158.

De Cremer, D., Nguyen, B. & Simkin, L. (2017). 'The integrity challenge of the Internet-of- Things (IoT): on understanding its dark side', Journal of Marketing Management, 33(1/2), pp. 145–158. doi: 10.1080/0267257X.2016.1247517.

El-Sayed H., et al. (2018). 'Edge of Things: The Big Picture on the Integration of Edge, IoT and the Cloud in a Distributed Computing Environment', IEEE Access, Access, IEEE, p. 1706. doi: 10.1109/ACCESS.2017. 2780087.

Geneiatakis, D., Kounelis, I., Neisse, R., Nai-Fovino, I., Steri, G., & Baldini, G. (2017). 'Security and privacy issues for an IoT based smart home.' International Convention on Information & Communication Technology, Electronics & Microelectronics. IEEE.

Guo, S., Hu, X., Guo, S., Qiu, X., & Qi, F. (2019). Blockchain Meets Edge Computing: A Distributed and Trusted Authentication System. IEEE Transactions on Industrial Informatics, vol. 16, no. 3, pp. 1972-1983. doi:10.1109/tii.2019.2938001

Kumar, NM & Mallick, PK (2018). 'The Internet of Things: Insights into the building blocks, component interactions, and architecture layers', Procedia Computer Science, vol. 132, pp. 109–117.

Lee, C. and Fumagalli, A. (2019). "Internet of Things Security - Multilayered Method For End to End Data Communications Over Cellular Networks," 2019 IEEE 5th World Forum on Internet of Things (WF-IoT), Limerick, Ireland, 2019, pp. 24-28, doi: 10.1109/WF-IoT.2019.8767227.

Lee, M.-C., Lin, J.-C. & Owe, O. (2018). 'Privacy Mining from IoT-based Smart Homes'.

Lee, Y. T., Hsiao, W. H., Lin, Y. S., & Chou, S. C. T. (2017). Privacy-preserving data analytics in cloud-based smart home with community hierarchy. IEEE Transactions on Consumer Electronics, 63(2), 200-207.

Leng, J., Lin, Z. and Wang, P. (2020). "Poster Abstract: An Implementation of an Internet of Things System for Smart Hospitals," 2020 IEEE/ACM Fifth International Conference on Internet-of-Things Design and Implementation (IoTDI), Sydney, Australia, 2020, pp. 254-255, doi: 10.1109/IoTDI49375.2020.00034.

Mantelero, A. (2017). Regulating big data. The guidelines of the council of Europe in the context of the European data protection framework. Computer Law & Security Review.

Marikyan, D., Papagiannidis, S., & Alamanos, E. (2019). A systematic review of the smart home literature: A user perspective. Technological Forecasting and Social Change. Volume 138, 2019, pp.139-154. doi:10.1016/ j.techfore.2018.08.015

Mihalache, A. (2017) 'Wireless Home Automation System using IoT', Informatica Economica, 21(2), pp. 17–32. doi: 10.12948/issn14531305/21.2.2017.02.

Nguyen, B., & De Cremer, D. (2016). 'The fairness challenge of the internet of things.' European Business Review, January/February (pp. 31–33). Available at: http://www.europeanbusinessreview.com/?p=8588

Rathore, M. M., Paul, A., Ahmad, A., & Jeon, G. (2017). IoT-based big data: from smart city towards next generation super city planning. International Journal on Semantic Web & Information Systems, 13(1), 28-47.

Risteska Stojkoska, B. L. & Trivodaliev, K. V. (2017) 'Review: A review of Internet of Things for smart home: Challenges and solutions', Journal of Cleaner Production, 140(Part 3), pp. 1454– 1464. doi: 10.1016/j.jclepro.2016.10.006.

Shave, L. (2018). 'The CIA of security and access', IQ: The RIM Quarterly, (2), p. 18. Yassine, A. et al. (2019). 'IoT big data analytics for smart homes with fog and cloud computing', Future Generation Computer Systems, 91, pp. 563–573. doi: 10.1016/j.future. 2018.08.040.

Zheng, S. et al. (2018). 'User Perceptions of Smart Home IoT Privacy'. doi: 10.1145/3274469.

N. Komninos, E. Philippou, and A. Pitsillides, "Survey in smart grid and smart home security: Issues, challenges and countermeasures," IEEE Communications Surveys & Tutorials, vol. 16, no. 4, pp. 1933–1954, 2014.

Tetteh, N., & Amponsah, O. (2020). Sustainable Adoption of Smart Homes from the Sub-Saharan African Perspective. Sustainable Cities and Society, Volume 63, December 2020, p. 102434. doi:10.1016/j.scs. 2020.102434

Tsou, Y.-T., Chen, H.-L., Chen, J.-Y., Huang, Y., & Wang, P.-C. (2017). 'Differential privacy-based data de-identification protection and risk evaluation system' (2017) 2017 International Conference on Information and Communication Technology Convergence (ICTC), Information and Communication Technology Convergence (ICTC), 2017 International Conference on, p. 416. doi: 10.1109/ICTC.2017.8191015.