Challenges and Issues of the Internet of Things: Factoring Elements from the Social, Political and Information Systems

Arif Ali[1](✉) and Walayat Hussian[2,3]

[1] Wellington Institute of Technology, Wellington, New Zealand
Arif.ali@weltec.ac.nz
[2] Victoria University Business School, Victoria University, Melbourne, VIC, Australia
[3] University of Technology Sydney, Sydney, NSW, Australia
Walayat.Hussain@uts.edu.au

Abstract. The concept and applications of the Internet of Things or IoT are well-known to those dealing with the technicalities and complexities of IoT. However, for most users, the understanding seems to be limited to the benefits and usability of the devices. In particular, grasping the privacy, security and other relevant issues, especially social issues, remains out of reach for most users. This paper addresses the problem of privacy, security and other relevant issues from users' perspective and suggests three areas needing greater attention in resolving the issues. First, this paper highlights social issues and emphasizes the role of business leaders in dealing with the issues surrounding IoT devices. This paper argues that the onus and obligation lie with the business leaders as social architects to perform their duty of care in a socially responsible manner. Second, IoT is simply an IS product in which people and their views are one of the key elements for achieving the common goal, in this case, of networking of things and people. Ignoring the role of end-users as a critical part of IoT does not help achieve the common purpose. Lastly, given the transnational nature of the issue, governments worldwide are essential stakeholders and hence need to have a proactive and positive approach in the fight against the use of IoT for cybercrimes.

Keywords: Cybercrime · Information systems · IoT security · IoT privacy · Leadership · User adoption of technology

1 Introduction

The Internet of Things (IoT) plays a vital role in the existing and future generation of information, communication and applications. IoT enables various technological devices to connect with sensors and software and exchange data in an intelligent way over the Internet. The technology has revolutionized the industry 4.0 technologies; therefore, the adoption is steadily increasing every next day. Small and big enterprises benefit from IoT due to its wide range of features, including – connectivity, monitoring real-time data

W. Hussain and M. A. Jan (Eds.): IoTaaS 2021, LNICST 421, pp. 73–83, 2022.
https://doi.org/10.1007/978-3-030-95987-6_5

capturing, active engagement, convenience and integrity. However, along with a wide variety of features, the IoT has limitations as well. The biggest challenge of IoT for any business is the security and privacy of data while transmitting from one device to another (Raza et al. 2021). Other challenges are – technical complexity, connectivity and power dependence.

The perception of IoT varies from person to person. The features, benefits and operations of IoT are well-known for those familiar and dealing with its technicalities and complexities (Gao et al. 2020). Therefore, their perspectives and how they look at IoT devices are from a designer, developer, or innovator's point of view. For businesses selling and distributing IoT, the devices are another line of fast selling, profitable products. However, for users, the understanding of the devices remains limited to the benefits and usability of the devices. The privacy, security and other relevant issues remain unfamiliar and unknown to the users. They simply trust the vendors and manufacturers and use the devices. Therefore, it is essential to highlight the shortcomings of IoT from a non-technical perspective.

This paper looks at the problem of privacy, security and other relevant issues from users' perspective and suggests three areas needing greater attention in resolving the issues. The contribution of this paper is that it highlights the user's perspective and emphasizes the need for a holistic approach. Specifically, considering users as key stakeholders and the business leaders as social architects who can offer different perspectives on the challenges. The study analyzes and highlights that IoT is an IS product where people and their views are key elements for achieving the goal of networking while considering the security and privacy of users.

The paper first simplifies the concept of IoT and how it works for users, mainly for domestic purposes. That is followed by highlighting the complexities and challenges for business users, which further leads to the discussion of social issues related to the use of IoT devices. The paper emphasizes the role of business leaders responsible for developing and manufacturing millions of IoT devices and developers and innovators to look at these devices from an Information Systems (IS) perspective. The paper also discusses what governments can do by highlighting the need for coordination at the global level for the fight against the use of IoT for cybercrimes. Both the groups, the business leaders and government policymakers, are social architects, expected to create a better society and consider people first over anything else.

The rest of the paper is organized as follows. Section 2 discusses related literature and concepts. Section 3 highlights common issues of IoT in different sectors. Section 4 discusses possible solutions, and finally, Sect. 5 concludes the paper with future research directions.

2 Related Literature and Concepts

This section discusses existing literature and related concepts that are used in our study. The section is divided into three subsections, as presented in Fig. 1:

– Simplifying IoT
– Applications and Challenges
– Complexities of IoT for Users

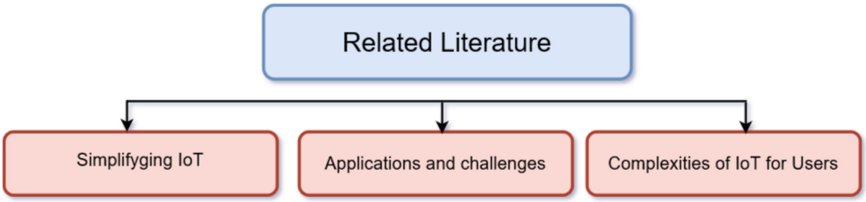

Fig. 1.

The discussion for each subsection is presented as follows:

2.1 Simplifying IoT

Internet of Things, or IoT, is generally defined as devices with network connectivity, collecting user data and sending it over the Internet into the cloud for processing and analyzing and then returning it to the user (Escamilla-Ambrosio et al. 2018; Petrakis et al. 2018). Some examples of the devices could be smartphones, smart fridges, thermostats, baby monitors, smartwatches, other wearables, car Bluetooth, and other similar devices connected with the Internet.

Beyond the physical devices, IoT also includes a person with a heart monitor implant or a farm animal with a chip transponder (Chacko and Hayajneh 2018). The connected devices have their unique identifiers and sensors collecting and transferring data over a network. The devices connect back to a central device such as a smartphone, or a laptop, known as the anchor device, used to control the connected device (Aldahiri et al. 2021).

Across businesses and industries, IoT enables the automation of business processes; it offers analysis and insight based on the data it collects, hence supporting resource monitoring and performance improvement. For example, the aviation industry uses IoT sensors for real-time reporting on the status of an aeroplane engine, i.e. the condition of their equipment. Similarly, city councils use IoT as a part of their smart city projects. For example, city councils use IoT to monitor and gain insights on traffic flow and parking spaces and predict any traffic issues sooner. As a result, the technology helps councils better address bottlenecks, long traffic queues and increase revenue from parking spaces.

2.2 Applications and Challenges

Nowadays, almost every digital product is connected with the Internet as a part of the ‘modern technological revolution’. The number of devices is estimated to be around 20 billion (Almadhoun et al. 2018). The devices are transitioning from being an optional luxury feature to being the baseline. That is because we feel technology is beneficial as it saves time, offers convenience and is reliable.

The real application is connecting people to things and things to things in real-time (Coetzee and Eksteen 2011). A typical Internet of Things network can proliferate, resulting in an exponential increase in the variety, velocity, and overall volume of data. The products collect data about the users and store that data in the cloud, where artificial intelligence (AI) enabled analytical programs continuously analyze, make sense out of the data and make conclusions or decisions for the user (Hussai et al. 2021a). For businesses, this data and its subsequent insights open significant value creation and revenue generation opportunities while users enjoy convenience (Showkat et al. 2018).

For example, many users use a smartwatch that collects information about daily activities and every movement and sends that to the cloud. Information such as running speed, number of steps, even heart rate and stress level are collected and stored in the cloud, where powerful servers diagnose the future status of our hearts and health conditions. Another similar example is that the smart fridge with lovely displays offers convenience, allowing users to check the fridge via mobile phone from the office and get items needed for dinner on the way home. In addition, the fridge can help users order groceries 'Just in Time' and notify them about expired products, what users eat, and when. The smart TV is also connected to the Internet and allows users to access videos and contents automatically compiled by the AI from the cloud (Hussain et al. 2020; Hussain et al. 2021b). Similarly, new cars, including their accessories, are already fully connected with the Internet at the time of purchase.

However, there are many challenges for vendors and manufacturers. The real challenge for the Internet of Things environments is how to analyze the large volume of information from all sources and take action in real-time (Davenport et al. 2012; Rathore et al. 2016). The challenge combined with the high expectations created by the Internet, mobile and 24/7 IT environment has made the need for new analytics approaches and technologies more urgent. Achieving desired business objectives requires acting in real-time to take advantage of opportunities and address problems quickly. As identified by Tanford et al. (2012), in the pre-Internet of Things era, an issue in a typical supply chain scenario could be addressed in two to three-day cycles for satisfactory results. However, in the Internet of Things, the time to act is in minutes, seconds or microseconds (Tanford et al. 2012). This explosion of data and the high expectations in the Internet of Things environment means the value of data slips away quickly. Therefore, for businesses, the importance of time to action for Internet of Things applications is crucial. Addressing the critical time to action requirements for businesses and the Internet of Things demands an advanced analytics solution that can unify historical real-time streaming predictive and prescriptive analytics and provide faster analytics and more innovative actions.

2.3 Complexities of IoT for Users

For the business, taking action in real-time based on the IoT-gathered data is crucial. Users at the receiving end of the supply chain have concerns and complexities. Imagine a user arriving home and sitting in front of the fire during winter; the user receives an instant message, an infringement notice from police for driving while intoxicated. While the user is trying to comprehend what is happening, the smartwatch has collected data about the heart rate and translated that into the amount of alcohol in the blood. As the car is connected to the Internet, based on the car and smartwatch data, it was concluded

that the user was driving with a certain alcohol level in their blood. While the user has broken the law, the real question is, how did the police know that the user was driving while intoxicated?

As another example, every connected car sends its location to its cloud service provider (Kwak et al. 2015). If somebody manages to hack into the cloud service provider, the hacker can know the location of many cars in a specific country. There is value in this information. First, the hacker can analyze this data and know where the person is living, working, and pinpoint the location of every BMW. Therefore, there is a need for an intelligent prediction system to perform complex predictions. Some recent approaches (Hussain et al. 2021c) introduced a novel ordered weighted aggregation operatore (OWA) in neural network structure to perform complex nonlinear predictions.

These are some examples of what may happen if somebody manages to compromise either the IoT device or the content of information that was delivered from the device to the cloud. As we get many more devices connected with the Internet, the devices can make decisions for users and offer the users services.

Users are aware of the connectivity as it informs their decision to adopt and use. However, they do not necessarily know how the data is exchanged and how the devices can collectively form a digital copy of the user. In fact, IoT devices have been used for cyber-attacks and to act as their proxy without any knowledge of that happening. The recent New Zealand Stock Exchange attack is an example where thousands of devices were used to connect with the Exchange, creating a traffic blockage and resulting in distributed denial of service (DDoS) attacks (New Zealand's Exchange 2020).

That is why it is so essential for innovators and developers to be socially responsible in the development and adoption of information systems devices, including IoT. It is equally important to actively educate the users about the security of their data and devices and possible misuse.

3 Common Issues

Although there is a significant increase in adopting IoT to improve customer service and decision-making efficiency across businesses and industries, all these connected devices have potential technical and non-technical issues. Most importantly, the devices can be hacked and used for committing cybercrimes. In fact, because of the vulnerability of the IoT devices, Meneghello et al. (2019) refers to IoT as the Internet of Threats. The section has divided the common issues into two main sub-sections:

- Security issues
- Privacy issues

3.1 Security

In every device, by default, users are left with no choice but to purchase and integrate the device into their lives. The problem is that the manufacturers expect users to be expert systems administrators. Without any monitoring and standardization and with the race to the top with no boundaries, it is not a matter of if, but when a hacker gains access to

one of the IoT devices; often they can access all the user devices and the whole home network gets compromised. First, they access the anchor device and then get everything that is hosted on the anchor device. They can even commit crimes remotely from hacked devices.

From the technical point of view, as the number of connected devices and sharing of information increase, so do issues. Security and privacy remain the top two issues (Atlam and Wills 2020). As described by Atlam and Wills (2020), any bug in a single device can potentially affect an entire IoT system and compromise users' private data. These connected devices produce a considerable amount of data that can be difficult to manage, let alone analyze and gather insights. In addition, competing IoT standards create challenges of getting different devices from different manufacturers to communicate with one another. For example, all standards and frameworks, including IPv6, ZigBee, LiteOS, OneM2M, DDS (data distribution service), and AMQP (advanced messaging queuing protocol), have standardization for IoT devices. While the IoT market is booming exponentially without any limits and users are adopting these devices without any comparison, a lack of standardization and monitoring and control are simply brewing chaos.

3.2 Privacy

We are living in a database society where data about our every move and second is captured. Due to that, there is an increasing likelihood of identity theft. Companies and thieves are making money from every kind of personal information (Labong 2019). For the users, the misuse of their devices and the privacy of their data are significant issues. What most people do not realize is how deeply identity theft can affect their lives. The effect of ID theft on victims is disastrous, taking hundreds of hours to clean up, being emotionally draining and leaving people feeling vulnerable (Weber 2015).

Essentially data is the new oil, and data trafficking is one of the top revenue-generating crimes globally and is just getting worse. Examples of the data breaches such as Equifax, Uber, and alter X are only the tip of the iceberg (Electronic Privacy Information Centre n.d.). The problem is getting worse as there is so much money to be made from identity theft.

Users think that an IoT device like a light bulb, thermostat, or a baby monitor is theirs and that the information is private. However, there are no regulations on almost any consumer device or the data that they collect. Currently, companies do not have to tell users what out of their data collection they are selling, to what third party companies they are sharing information with, and how they are storing the information. Most do not even have to tell users when they or their partner companies have been hacked and that private information is now public. Hence, the bottom line is that users have no clue what information is being sold and who is selling and/or stealing it.

Users assume that the purchaser also owns the information collected by a device. The device software and hardware companies might store our information; however, they have no legal grounds to sell or transfer the information. At the very least, users ought to have the right to opt-out of a company collecting their information and sharing it with others. However, realistically, some companies are spending hundreds of thousands

of dollars lobbying their governments to reduce further and relax regulations on data privacy.

The idea of making everyday objects smart is fascinating, however, but the issue is that the information is not stored locally on the user's device and is on the web to communicate with the cloud. Smart devices, such as autonomous lawnmowers, and smart heaters automatically adjusting the room temperature before a user arrives home, are making life easier. However, the devices also let companies analyze the user data mainly for the benefit of their business. The collection and transmission are mainly invisible to ordinary users. The worst case is that companies can remotely control smart devices. These are the most significant concerns with this new technology. Currently, the biggest challenges in the Internet of Things space are security and privacy. Imagine someone with access to a stove could cause it to overheat and maybe even start a home fire, or someone with control over a power plant could cut the power to an entire city. The possibilities seem endless, and the risks involved are not to be taken lightly.

While enjoying the digital assistance and convenience, users should think twice about how much smart technology they want for their homes and family. Users are expected to be expert network administrators and employ expert level measures to ensure their identities remain uniquely theirs. Whoever uses smart technology at home should know what they are dealing with. Smart technology requires smart handling and basically becoming a System Administrator, cataloguing the devices, installing security patches, checking for software updates, changing passwords, and perhaps even setting up protocols to ensure there were no hacking attempts.

4 Possible Solutions

Working on technical solutions is an obvious option; however, the effort is only one part of the solution and requires more comprehensive coverage. Therefore, it becomes short-sighted to only attempt to resolve the issues technically and overlook other possible avenues which can offer solutions. This paper highlights three areas that can complement and offer comprehensive solutions and eventually safe devices to end-users. The areas are related to social and non-technical aspects and are missing from the IoT literature, indicating a gap. The study categorized possible solutions into three sub-sections:

- Leaders as Social Architects
- Treating IoT as an iS Product
- Role of the Government

The discussion of each solution is presented as follows:

4.1 Leaders as Social Architects

Today's human society is being confronted by all sorts of global challenges and issues. Growing digital inequality, the devastation of the natural environment due to e-waste, data privacy breaches and the growing number of cyber security threats are just a few. As mentioned above, with the exponential adoption of IoT devices, security and privacy

issues are obviously going to rise. Furthermore, since competition between organizations is increasing and conflicting pressures from stakeholders are mounting, the environmental, social, and ethical impacts of IoT devices will rise. The question is about the role of businesses and business leaders: are they part of the solution or the problem?

The onus and obligation lie with the leaders as the social architects to create a safe environment by performing their duty of care and acting in a socially responsible manner (Muralidharan and Pathak 2018; Siddique and Joseph 2021). The sense of social responsibility is essential and must be considered before any technical adventurism; that is, the crucial requirement and element of human nature before anything else. As described by Nicholson and Kurucz (2019), what makes a person a great leader is their sense of responsibility for people and everything they do. Without such a characteristic, the person is just managing continuous operations and stability of the business with no eyes on the future.

Business leaders shape our future. Twenty years ago, who knew about the social media, social connectivity, and the social dilemma we are living in today? For all those years, the platforms have manipulated our social instincts. The whole younger human generation is being controlled at large and reshaped by social media. Unfortunately, knowingly or unknowingly, social media giants and leaders busy developing the '*social'* networking technology somehow have ignored the '*social'* element. They have started accepting how their social networking platforms have been involved in unethical business activities and have ignored the consequences of social damage. As a result, our society has become more asymmetric.

Therefore, this paper suggests that the business leaders in the IoT industry have the power to design a future without repeating those mistakes of social networking giants. Otherwise, another global issue due to IoT devices is awaiting.

The question is what business leaders in the IoT industry can do to avoid the issue. Besides their business continuity, the leaders can reconceptualize a sustainable growth opportunity for their business. In other words, they can develop a strategy to transition to responsible business practices with sustainability at the forefront of innovation – people first. Admittedly, the road is challenging; however, in the long run, sustainable practice guarantees profits and develops a strong business portfolio that is fit for the future with a positive impact on society.

4.2 Treating IoT as an IS Product

Another avenue and way forward to resolving the issues is to deal with IoT as a product of information systems (IS) instead of a tool. Information Systems is a set of integrated elements that work together towards achieving a common purpose (Papavasiliou 2020). Within the collection of integrated elements, users are a key part of the system (Tambunan et al. 2020).

Moreover, from a systems thinking point of view, systems thinking involves looking at the interconnections between parts of a whole rather than concentrating just on the parts. As described by Wright and Meadows (2008), a system is not just any collection of things, rather an interconnected set of elements that is coherently organized in a way that achieves something – a purpose. Therefore, users or people and their viewpoints are an equal part of a system that enables it to resolve complex situations. Therefore,

considering the relationship between people and things is as meaningful and necessary as the structure of the equipment and the particular situation.

Based on that line of thinking, this paper suggests that urgent collective action is needed to tackle cybercrime and the misuse of IoT devices. For that collective action, the users must play a key part in the whole process, from production to the use of the devices. The collective action can be in the form of better information and communication with the users about the vulnerability of the devices. Another possible strategy can be more education on the safe use of the devices. Such kinds of collective action can help minimize, if not eliminate, the unlawful uses of IoT as a service for cybercrime. Most importantly, that is needed because the users need to know about the possible hacking and misuse of their devices if not used securely.

4.3 Role of the Government

Given the transnational nature of misuse of IoT devices for cybercrime and the extent of the damage the criminals can cause, governments around the world are one of the obvious stakeholders. They have significant influence over regulations and policies. However, they seem to be slow in taking a greater level of interest. One can speculate that on the one hand, the nature of Information and Communication Technologies (ICT) is fast-moving; on the other hand, the movement of the machinery of government is slow. The only commonality between both is the complex nature of both – the ICT and machinery of government.

In terms of international conventions, the Budapest Convention adopted by the European Union increased cooperation and sharing of information and knowledge for tackling the challenge of cybercrime. More recently, in December 2019, the United Nations General Assembly adopted a resolution to establish a committee for working towards a comprehensive convention for countering the use of ICT for cybercrimes. The negotiations are starting in January 2022 and are scheduled to conclude in 2024.

While users need such conventions and international agreements, the issue is that the governments are more interested in the areas of national security instead of user protections. There is also a concern that the treaties allow violation of human rights and greater surveillance of people. That is evident due to the fact that some countries are reluctant to take action against cybercrimes within their borders but are showing more interest in international treaties (Brown 2021). As noted in Brown (2021), “cybercrime is dangerous, but a new UN treaty could be worse for rights”.

Therefore, it is vital that governments worldwide take vigorous steps to reduce the possibility of the misuse of the devices while preserving the rights of people. First, since governments have the mandate, more close coordination and transnational cooperation between governments are needed for effective and practical steps to minimize the illegal use of IoT devices. However, the pace of formulating and reviewing treaties and conventions has to, at least, match the pace of changes in ICT. In addition, that must not be used for violations of people’s rights. Second, they can prioritize the issue and allocate more resources to relevant government agencies fighting against crime. Treaties and conventions will have less impact if the implementing agencies on the ground lack resources. Last but not least, governments and their commerce commissions can develop better checks on the production of secure devices and sharing of information with the

users. They also need to prioritize social concerns over trade for tackling the misuse of IoT devices and ICT in general.

5 Conclusion

The objective of all stakeholders in the IoT industry should be to support and uphold broader human values and ethics for cyberspace, a space that functions based on rules, promotes rights of freedom and privacy, and where the users feel secure. For that, it is necessary to not only produce devices that are modern and offer convenience but also proactively seek avenues for discouraging unlawful and misuse of those devices.

In addition to technical solutions, business leaders need to take responsibility for ethical business practices and prioritize people over profit. Similarly, IoT devices need to be treated as a product of information systems in which humans are a key part of the system. Keeping that in mind and working with the users can help in taking collective actions against the misuse of IoT devices. Lastly, governments as crucial stakeholders and influencers can undoubtedly do more.

With all three suggestions, this paper considers that misuse of IoT devices by cybercriminals and eventual financial, social and emotional impact can be reduced, if not eliminated, entirely. In particular, governments and business leaders have the power to do so.

References

Aldahiri, A., Alrashed, B., Hussain, W.: Trends in using IoT with machine learning in health prediction system. Forecasting **3**(1), 181–206 (2021)

Almadhoun, R., Kadadha, M., Alhemeiri, M., Alshehhi, M., Salah, K.: A user authentication scheme of IoT devices using blockchain-enabled fog nodes. In: 2018 IEEE/ACS 15th international conference on computer systems and applications (AICCSA), pp. 1–8. IEEE, October 2018

Atlam, H., Wills, G.: IoT security, privacy, safety and ethics. In: Farsi, M., Daneshkhah, A., Hosseinian-Far, A., Jahankhani, H. (eds.) Digital Twin Technologies and Smart Cities. IT, pp. 123–149. Springer, Cham (2020). https://doi.org/10.1007/978-3-030-18732-3_8

Brown, D.: Cybercrime is Dangerous, But a New UN Treaty Could Be Worse for Rights (2021). https://www.hrw.org/news/2021/08/13/cybercrime-dangerous-new-un-treaty-could-be-worse-rights

Chacko, A., Hayajneh, T.: Security and privacy issues with IoT in healthcare. EAI Endorsed Trans. Pervasive Health Technol. **4**(14) (2018)

Coetzee, L., Eksteen, J.: The Internet of Things - promise for the future? An introduction. In: 2011 IST-Africa Conference Proceedings, pp. 1–9. IEEE, May 2011

Davenport, T.H., Barth, P., Bean, R.: How big data is different (2012)

Electronic Privacy Information Centre (n.d.). Equifax Data Breach https://epic.org/privacy/data-breach/equifax/

Escamilla-Ambrosio, P.J., Rodríguez-Mota, A., Aguirre-Anaya, E., Acosta-Bermejo, R., Salinas-Rosales, M.: Distributing computing in the internet of things: cloud, fog and edge computing overview. In: Maldonado, Y., Trujillo, L., Schütze, O., Riccardi, A., Vasile, M. (eds.) NEO 2016. SCI, vol. 731, pp. 87–115. Springer, Cham (2018). https://doi.org/10.1007/978-3-319-64063-1_4

Gao, H., Qin, X., Barroso, R.J.D., Hussain, W., Xu, Y., Yin, Y.: Collaborative learning-based industrial IoT API recommendation for software-defined devices: the implicit knowledge discovery perspective. IEEE Trans. Emerging Top. Comput. Intell. **6**, 667–6 (2020)

Hussain, W., Merigo, J.M., Gao, H., Alkalbani, A.M., Rabhi, F.A.: Integrated AHP-IOWA, POWA framework for ideal cloud provider selection and optimum resource management. IEEE Trans. Serv. Comput. (2021a)

Hussain, W., Merigó, J.M., Raza, M.R.: Predictive intelligence using ANFIS-induced OWAWA for complex stock market prediction. Int. J. Intell. Syst. (2021b)

Hussain, W., Merigó, J.M., Raza, M.R., Gao, H.: A new QoS prediction model using hybrid IOWA-ANFIS with fuzzy c-means, subtractive clustering and grid partitioning. Inf. Sci. **584**, 280–300 (2021c)

Hussain, W., Sohaib, O., Naderpour, M., Gao, H.: Cloud marginal resource allocation: a decision support model. Mob. Networks Appl. **25**(4), 1418–1433 (2020)

Kwak, B.I., Han, M.R., Kang, A.R., Kim, H.K.: A study on detection methodology of threat on cars from the viewpoint of IoT. J. Korea Inst. Inf. Secur. Cryptol. **25**(2), 411–421 (2015)

Labong, R.C.: Identity theft protection strategies: a literature review. J. Acad. Res. **4**(2), 1–12 (2019)

Meneghello, F., Calore, M., Zucchetto, D., Polese, M., Zanella, A.: IoT: internet of threats? A survey of practical security vulnerabilities in real IoT devices. IEEE Internet Things J. **6**(5), 8182–8201 (2019)

Muralidharan, E., Pathak, S.: Sustainability, transformational leadership, and social entrepreneurship. Sustainability **10**(2), 567 (2018)

New Zealand's Exchange: Independent reports on NZX IT and cybersecurity completed (2020). https://www.nzx.com/announcements/364459

Nicholson, J., Kurucz, E.: Relational leadership for sustainability: building an ethical framework from the moral theory of 'ethics of care.' J. Bus. Ethics **156**(1), 25–43 (2019)

Papavasiliou, S.J.: A digital transformation governance framework for eGovernment: a systemic approach. Doctoral dissertation (2020)

Petrakis, E.G., Sotiriadis, S., Soultanopoulos, T., Renta, P.T., Buyya, R., Bessis, N.: Internet of things as a service (ITAAS): challenges and solutions for management of sensor data on the cloud and the fog. Internet Things **3**, 156–174 (2018)

Rathore, M.M., Ahmad, A., Paul, A., Rho, S.: Urban planning and building smart cities based on the Internet of things using big data analytics. Comput. Netw. **101**, 63–80 (2016)

Raza, M.R., Varol, A., Hussain, W.: Blockchain-based IoT: an overview. Paper presented at the 2021 9th International Symposium on Digital Forensics and Security (ISDFS) (2021)

Showkat, D., Som, S., Khatri, S.K., Ahluwalia, A.S.: Security implications in IoT using authentication and access control. In: 2018 7th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO), pp. 689–694. IEEE, August 2018

Siddique, J., Joseph, P.: The social architect: a new framework for effective activism and social leadership. Cadmus **4**(4) (2021)

Tambunan, S.B., Lores, L., Muda, I.: Factors influencing the establishment of ISO 17799 standards. In: Proceedings of the International Conference of Science, Technology, Engineering, Environmental and Ramification Researches (ICOSTEERR 2018)-Research in Industry 4.0, pp. 1290–1295 (2020)

Tanford, S., Baloglu, S., Erdem, M.: Travel packaging on the internet: the impact of pricing information and perceived value on consumer choice. J. Travel Res. **51**(1), 68–80 (2012)

Weber, R.H.: Internet of things: privacy issues revisited. Comput. Law Secur. Rev. **31**(5), 618–627 (2015)

Wright, D., Meadows, D.H.: Thinking in systems. Earthscan (2008)