An Empirical Study on Data Privacy and Security Protection

ISBN: 978-1-943295-20-3

Shubham Kumar Shaw
Sahil Shaw
Shreya Periwal
Kirti P Sharma
Techno India University
(shawshubham2003@gmail.com)
(sahilshaw389@gmail.com)
(periwalshreya27@gmail.com)
(kirtipsharma8525@gmail.com)
Debolina Chakraborty
Future Institute of Technology
(debolina19619@gmail.com)

The privacy protection Principles of the tech industry are designed to protect user privacy while ensuring that the industry grows. This is evident in the field of artificial intelligence (AI). There are security and privacy issues with IoT devices that need to be addressed. IoT technology could lead to users' personal data being shared without their consent, which could lead to them avoiding using the technology. This paper tries to provide a comprehensive overview of the state of the art of IoT and AI, with a focus on privacy and security threats, attack surface, vulnerabilities, and countermeasures.

Keywords: - Privacy, Security, Internet of Things, Artificial Intelligence

1. Introduction

Data inside the contemporary business environment has a specific financial worth. One could recover files that may not only identify a particular individual but also evaluate one's population, institutional factors, behavioural, or psychological qualities, gain knowledge of one's purchasing patterns, and monitor one's work routine or lifestyles from burgeoning pairs of unorganized, apparently disengaged data. Because IoT devices require a constant Broadband connection to transfer information, the 5G network is a fantastic option owing to its low latency and rapid high transfer speeds (Neves et al., 2017). IoT technology allows for access to various machines and gadgets using both wired and wireless networks. Currently, 5G networks can accommodate up to 106 devices per square kilometre, with up to 10Mbps per square kilometre and 1ms of round-trip latency. People are becoming increasingly familiar with the terms "Internet of Things" and "Internet of Energy" as they realize how innovation may enhance daily living. The technology makes it easier to distribute products and make more efficient energy transactions (Devabalaji et al., 2020). In order to track many aspects of city life, you will need a variety of devices such as detectors, webcams, meters, motors, and RFID tags. The Internet of Things (IoT) and software are making it easier and more convenient for people to connect things in their lives. Our research has shown that these models have been created and used. (Moustaka et al., 2018a).

According to recent statistics, 12.3 billion things are connected to the internet in 2021, and this number is projected to grow to 30 billion by 2025 (Marr, 2017). The shared information collected by nation-states presents important moral concerns. policymakers, researchers, companies, and utilities must pay attention to these issues in order to provide the best possible service to the people of their nations (Bianchini and Avila, 2014; Cobb, 2016; Kitchin, 2016). There have been times when the data recorded for the common benefit was used by both governmental and commercial groups in order to achieve their own goals. For example, mass control, market supremacy, data surveillance, etc.), compromising people's private information and casting doubt on SC's mission (Bianchini and Avila, 2014; Cobb, 2016; Greenfield, 2013; Kitchin, 2014; Kitchin, 2016; Townsend, 2013).

Investments in data privacy and security might help reduce concerns about personal data being mishandled. There is uncertainty about whether the benefits of making BDA investments more than other types of investments by firms are greater than the benefits of not making BDA investments. Studies have looked at the worth of types of information technology investments, such as e-commerce and social media (X. Luo et al., 2013, I. Bose et al., 2019, S. Dewan et al., 2007). This paper assessed the security implications of interconnections between different system components and considered how they could impact the overall security of the platform. The researchers studied how four interactions with the internet can affect security. These include privacy, trust, identity, and access control (Riahi et al., 2018).

We recommend imposing high-security measures on IoT technologies used in the SC industry in order to prevent third-party exploitation and the segregation of urban and personal data (Bartoli et al., 2011). The IoT-ARM Reference Model and its companion app provide a secure way to use your IoT devices while still feeling confident in the knowledge that your privacy is protected (Beltran et al., 2017). The (Mazhelis et al.,2016) study suggested a two-level privacy architecture in order to protect sensitive personal data from intelligent applications while keeping any location information from being leaked, (Solomon et al.,2016) compared three encryption-based approaches. These three approaches included a proximity detection feature.

2. Literature Review

The advantage of having Some degree of control over the gathering and use of personal data is referred to as information privacy. Information privacy refers to the capacity of a person or group to prohibit information about oneself from being known to anybody other than those to whom the information is supplied. An important user privacy issue is the identification of personal information while it is being transmitted over the Internet. (Porambage P, et al.) Data privacy is concerned with how individual data is used and governed, including things like having rules in place to make sure that customers' personal information is collected, shared, and utilized in ways that are appropriate. (Jing Q, et al)

Businesses and government entities generate and constantly collect massive quantities of data. The present emphasis on massive volumes of data will undoubtedly offer possibilities and avenues for understanding how such data is processed across a wide range of sectors. However, big data's potential comes at a cost.; individuals' privacy is routinely jeopardized. (Han J, Ishii M, Makino H) Privacy has grown more crucial to both individuals' and organizations' daily lives as a result of the increased personal data that has recently attracted commercial interest. Rapid technological advancement has resulted in the collection, storage, and processing of private information on an unprecedented scale. One of the concepts is artificial intelligence, for which information is like oxygen and which, even though most of its operations are normally hidden, needs a tremendous quantity of information to advance. The application of Artificial intelligence is also present in practically every aspect of modern life. This increases concerns regarding transparency and privacy. Most internet users are concerned about their privacy and strongly feel the need to preserve it (Bédard, 2016).

Using technology, procedures, and training, security is the practice of preventing unauthorized users from accessing, disclosing, disrupting, altering, inspecting, recording, or destroying data and information assets. Data protection against malicious attacks and the commercial exploitation of stolen data are the main security-related concerns. (Jing Q, et al.)

In a CoT system, it is imperative to efficiently regulate user access, IoT resource usage, and inter-entity communication. Resources must be used and accessed in a secure, transparent, and effective way. In the context of CoT, secure communication between IoT devices and cloud infrastructure is necessary to protect personal privacy and security. Communication security requires a protocol that enables consensus among all parties to communicate over the cryptographic method and keys that will be applied to encrypt the communication in the exchanged messages. (V. Vasic)

The authors suggested a novel approach to address the CoT's privacy and security concerns. Private cloud refers to the establishment of a virtual infrastructure within the enterprise firewall. Only authenticated users can easily access the cloud-based data and apps in this situation, If the content you add to a database is accessed from the outside, content encryption aids in protecting its confidentiality. Just the data in the storage area is subject to encryption, by assisting the user in establishing an end-to-end connection that is reasonably secure, session containers serve to assure the security of public clouds, monitor user authentication paths, and offer higher security, cloud access brokers are utilized (B. Alohali).

Millions of people worldwide rely on social networking sites and applications to connect and share information with one another. social media platforms are characterized as group-based web applications that enable users to interact with others online, form new relationships, join groups, share images, organize events, and network with people in their local areas. Platforms for social networking are used to connect people who have similar preferences and interests (S.C. Margaret, M. Atilano, C.L. Arnold). Websites called online social networks to give users the chance to communicate with and form bonds with other online users.

Social networks come in a variety of shapes and sizes and categories. LinkedIn is a great resource for professional networking and for keeping in touch with old friends and beloved co-workers. Your LinkedIn profile is like a digital portfolio where you might showcase your credentials, and provide information regarding your service history, college education, and career goals, electronic mail, more often known as email or fax, is a method of transmitting digital communications from a sender to one or more recipients. You can access digital email over the Internet or other online networks, Skype Technologies S.A. developed the Voice over Internet Protocol (VoIP) program Skype. It is a peer-to-peer network that distributes voice conversations via the Internet, as opposed to a dedicated network. YouTube is a platform set up for exchanging content, including music, images, and videos. These websites foster partnerships and user interaction through comments by allowing users to create personal profiles (D. Diaz-Sanchez, A. Marin, F. Almenarez, A. Cortés)

Both the online and offline worlds now constantly require identification and authorization. A sizable number of public and commercial sector organizations need personal identification before allowing visitors entrance to their facilities. Utilizing biometrics is one method of getting this recognition. The technology that employs automatic personal recognition based on physiological or behavioral traits is known as biometric identification or biometrics. (ISO/IEC 2382-37)

Any human characteristic may be considered a biometric if it satisfies the criteria listed below: Every human person possesses this quality, which makes it universal and distinctive. A few criteria must be met for a trait to be considered permanent: 1) it must be unique, 2) it must be present in an unchanging state over time, 3) it must be permanent, and 4) it must exist in an amount that can be measured. Biometrics include fingerprints, iris prints, hand geometry, face, voice, gait, and signatures (Prabhakar S., Pankanti S and Jain A) Since a real person can be identified or recognizable using biometric data as described above, they are typically regarded as personal data.

Hypotheses Formulation Based on the research insights in the literature review, the following research hypotheses can be developed

- **H1:** Data Privacy and Security Protection is dependent on the gender of customers.
- **H2:** Data Privacy and Security Protection is dependent on the age group of customers**.**

- **H3:** Data Privacy and Security Protection is dependent on the monthly income of customers.
- **H4:** Data Privacy and Security Protection is dependent on the occupation of customers
- **H5:** Data Privacy and Security Protection is dependent on the educational qualification of customers**.**

3. Objective of Study

To study the connection between demographic factors and satisfaction between customer towards Data Privacy and Security Protection.

4. Research Methodology

This research is done with the help of structured questionnaires, 150 samples were collected from the metro city, of Kolkata via one-to-one interaction with the consumers related to Data Privacy and Security Protection. The primary data for the study was collected from men, and women, of different age groups, belonging to different income brackets, from various occupation backgrounds like business, service, and others. Each parameter study for the survey was calculated using five points like a scale (from 1-strongly disagree, to 5-strongly agree). We used the chi-square test to find out the significant connect of the demographic factors to the satisfaction among consumers towards Data Privacy and Security Protection.

Analysis

We have used the Chi-square test using SPSS 21.0 to prove the hypothesis given below:
H0: Data Privacy and Security Protection is independent on gender of the customers. Ha: Data Privacy and Security Protection is dependent on gender of the customers.
H0: Data Privacy and Security Protection is independent of age group of the customers. Ha: Data Privacy and Security Protection is dependent on age group of the customers.
H0: Data Privacy and Security Protection is independent of monthly income of the customers. Ha: Data Privacy and Security Protection is dependent on monthly income of the customers.
H0: Data Privacy and Security Protection is independent of educational qualification of the customers. Ha: Data Privacy and Security Protection is dependent educational qualification of the customers.
H0: Data Privacy and Security Protection is independent of occupation of the customers. Ha: Data Privacy and Security Protection is dependent on occupation of the customers.

Satisfactory Variables

V10**:** We have mechanisms in place to destroy or delete data if requested to do so.
V13: Users' levels of privacy concern do affect the amount of information they disclose on social networking sites.
V16: The identification of personal information during Internet transmission is a critical user privacy problem.

5. Results and Analysis

Gender

Table 1 *Chi-Square Tests & Symmetric Measures*

		Value	df	Asymp. Sig. (2-sided)			Value	Approx. Sig.
V10	Pearson Chi-Square	15.264[a]	4	.004	Nominal by Nominal	Contingency Coefficient	.257	.004
	Likelihood Ratio	15.467	4	.004				
	N of Valid Cases	216			N of Valid Cases		216	
V13	Pearson Chi-Square	31.921[a]	4	.000	Nominal by Nominal	Contingency Coefficient	.359	.000
	Likelihood Ratio	41.660	4	.000				
	N of Valid Cases	216			N of Valid Cases		216	
V16	Pearson Chi-Square	34.191[a]	**4**	.000	Nominal by Nominal	Contingency Coefficient	.370	.000
	Likelihood Ratio	38.215	**4**	.000				
	N of Valid Cases	216			N of Valid Cases		216	

From the above table (Table 1) we see that the chi-square value for V10 is 15.264[a] and the asympsig is .004 which is less than 0.05. Similarly, the chi-square value for V13 is 31.921a and the asymp sig is .000 which is less than 0.05, and the chi-square value for V16 is 34.191[a] and asymp sig is .000 which is less than 0.05. This implies that the null hypothesis is rejected, and the alternate hypothesis is accepted. Thus, gender has a significant association with data privacy and security protection with respect to variables V10, V13, and V16. Similarly, it can be seen that the Contingency Coefficient of variable V10 is .257 and for variable V13 is .359, and for variable V16 is .370 this indicates the relationship between gender and consumer satisfactions low with the variable.

Age

Table 2 *Chi-Square Tests & Symmetric Measures*

		Value	**df**	**Asymp. Sig.(2-sided)**			**Value**	**Approx.Sig.**
V10	Pearson Chi-Square	45.365[a]	16	.000	Nominal by Nominal	Contingency Coefficient	.417	.000
	Likelihood Ratio	54.588	16	.000				
	N of Valid Cases	216			N of Valid Cases		216	
V13	Pearson Chi-Square	105.284[a]	16	.000	Nominal by Nominal	Contingency Coefficient	.572	.000
	Likelihood Ratio	101.902	16	.000				
	N of Valid Cases	216			N of Valid Cases		216	
V16	Pearson Chi-Square	26.427[a]	**16**	.048	Nominal by Nomina l	Contingency Coefficient	.330	.048
	Likelihood Ratio	29.808	**16**	.019				
	N of Valid Cases	216			N of Valid Cases		216	

From the above table (Table 2) we see that the chi-square value for V10 is 45.365[a] and the asympsig is .000 which is less than 0.05. Similarly, the chi-square value for V13 is 105.284[a] andthe asymp sig is .000 which is less than 0.05, and the chi-square value for V16 26.427[a] is and asymp sig is .048 which is also less than 0.05. This implies that the null hypothesis is rejected, and the alternate hypothesis is accepted. Thus, age has a significant association with data privacy and security protection with respect to variables V10, V13, and V16. Similarly, it can be seen that the Contingency Coefficient of variable V10 is .417 and for variable V13 is .572, and for variable V16 is .330 this indicates the relationship between age and consumer satisfactions low with the variable.

Income

Table 3 *Chi-Square Tests & Symmetric Measures*

		Value	df	Asymp. Sig.(2-sided)			Value	Approx.Sig.
V10	Pearson Chi-Square	95.749[a]	20	.000	Nominal by Nominal	Contingency Coefficient	.554	.000
	Likelihood Ratio	103.890	20	.000				
	N of Valid Cases	216			N of Valid Cases		216	
V13	Pearson Chi-Square	79.974[a]	20	.000	Nominal by Nominal	Contingency Coefficient	.520	.000
	Likelihood Ratio	93.668	20	.000				
	N of Valid Cases	216			N of Valid Cases		216	
V16	Pearson Chi-Square	49.435[a]	**20**	.000	Nominal by Nomina l	Contingency Coefficient	.432	.000
	Likelihood Ratio	53.425	**20**	.000				
	N of Valid Cases	216			N of Valid Cases		216	

From the above table (Table 3) we see that the chi-square value for V10 is and the 95.749[a] asympsig is .000 which is less than 0.05. Similarly, the chi-square value for V13 is 79.974[a] andthe asymp sig is .000 which is less than 0.05, and the chi-square value for V16 is 49.435[a] and asymp sig is .000 which is less than 0.05. This implies that the null hypothesis is rejected, and the alternate hypothesis is accepted. Thus, income has a significant association with data privacy and security protection with respect to variables V10, V13, and V16. Similarly, it can be seen that the Contingency Coefficient of variable V10 is .554 and for variable V13 is .520, and for variable V16 .432 is this indicates the relationship between income and consumer satisfactions is mid with the variable.

Occupation

Table 4 *Chi-Square Tests & Symmetric Measures*

		Value	df	Asymp. Sig.(2-sided)			Value	Approx. Sig.
V10	Pearson Chi-Square	14.044[a]	8	.081	Nominal byNominal	ContingencyCoefficient	.247	.081
	Likelihood Ratio	17.256	8	.028				
	N of Valid Cases	216			N of Valid Cases		216	
V13	Pearson Chi-Square	37.135[a]	8	.000	Nominal byNominal	ContingencyCoefficient	.383	.000
	Likelihood Ratio	42.198	8	.000				
	N of Valid Cases	216			N of Valid Cases		216	
V16	Pearson Chi-Square	52.333[a]	**8**	.000	Nominal by Nomina l	ContingencyCoefficient	.442	.000
	Likelihood Ratio	63.742	**8**	.000				
	N of Valid Cases	216			N of Valid Cases		216	

From the above table (Table 5) we see that the chi-square value forV10 is 14.044[a] and the asympsig is .081 which is more than 0.05. Similarly, the chi-square value for V13 is 37.135[a] and the asymp sig is .000 which is also less than 0.05, and the chi-square value for V16 is 52.333[a] and asymp sig is.001 which is also less than 0.05. This implies that the null hypothesis is rejected, and the alternate hypothesis is accepted. Thus, occupation has a significant association with data privacy and security protection with respect to variablesV10, V13, and V16. Similarly, it can be seen that the Contingency Coefficient of variableV10 is .247 and for variable V13 is .383, and for variableV16 is .442 this indicates the relationship between occupation and consumer satisfactions low with the variable.

Educational Qualification

Table 5 *Chi-Square Tests & Symmetric Measures*

		Value	df	Asymp. Sig.(2-sided)			Value	Approx. Sig.
V10	Pearson Chi-Square	44.539[a]	12	.000	Nominal byNominal	ContingencyCoefficient	.413	.000
	Likelihood Ratio	61.197	12	.000				
	N of Valid Cases	216			N of Valid Cases		216	
V13	Pearson Chi-Square	49.794[a]	12	.000	Nominal byNominal	ContingencyCoefficient	.433	.000
	Likelihood Ratio	54.445	12	.000				
	N of Valid Cases	216			N of Valid Cases		216	
V16	Pearson Chi-Square	46.071[a]	**12**	.000	Nominal by Nominal	ContingencyCoefficient	.419	.000
	Likelihood Ratio	43.681	**12**	.000				
	N of Valid Cases	216			N of Valid Cases		216	

From the above table (Table 4) we see that the chi-square value forV10 is 44.539[a] and the asympsig is .000 which is less than 0.05. Similarly, the chi-square value for V13 is and 49.794[a] the asymp sig is .000 which is also less than 0.05, and the chi-square value for V16 is 46.071[a] and asymp sig is.000 which is also less than 0.05. This implies that the null hypothesis is rejected, and the alternate hypothesis is accepted. Thus, educational qualification has a significant association with data privacy and security protection with respect to variables V10, V13 and V16. Similarly, it can be seen that the Contingency Coefficient of variableV10 is .413 and for variable V13 is .433, and for variableV16 is .419 this indicates the relationship between educational qualification and consumer satisfaction is low with the variable.

6. Conclusion

Digital technologies have significantly improved many aspects of our lives, including our ability to communicate, work, and stay connected. These tools allow us to obtain and analyze vast amounts of data, which allows us to address pressing societal concerns that were not possible before. People shouldn't really be prevented by technology from safeguarding their data since doing so would raise everyone's standard of living. Technological innovation will continue to advance, bringing with it new, better ways to manage confidentiality capabilities. Privacy will change continually and gradually as a result. Millions of customers worldwide basically rely on social media sites to mainly collaborate and interact data with each other in a very apparently significant way, or at least that's what they basically believed. The installation of intelligent devices that may be managed by individuals using other world wide web devices is referred to as the "Internet of Things." We won't ever need to leave the comfort of our house to perform tasks like washing, grocery shopping, or even monitor your health thanks to this.

Complete absence of documentation, including privacy rules and a high number of security flaws in the code, are significant signs of a hurried development environment. We believe that this was most likely caused by a hasty choice and an insufficient amount of time in quality standards. To achieve this, technologies should include confidentiality guidelines into the development of complex software and programs, should focus the needs of end users, and in overall could apply security techniques in a considerable degree, which is typically extremely important.

7. Reference

1. 2 ISO/IEC 2382-37. Information technology – Vocabulary – Part 37: Biometrics.

A. Riahi Sfar, E. Natalizio, Y. Challal, Z. Chtourou, A roadmap for security challenges in the Internet of Things, Digit. Commun. Netw. 4 (2) (2018) 118–137.

B. Alohali, Security in Cloud of Things (CoT), in: Cloud Security: Concepts, Methodologies, Tools, and Applications, IGI Global, 1188–1212, 2019.

2. Bartoli, A., Hernandez-Serrano, J., Sorian, M., Dohler, M., Kountouris, A., Barthel, D., 2011. Security and privacy in your smart city. Proceedings of Barcelona Smart Cities Congress. Available at: http://www.cttc.es/publication/security-and-privacy-inyour-smart-city/, Accessed date: 28 December 20

3. Bédard, M. (2016). The underestimated economic benefits of the internet. Montreal: Montreal Economic Institute.

4. Beltran, V., Skarmeta, A.F., Ruiz, P.M., 2017. An ARM-compliant architecture for user privacy in smart cities: SMARTIE—quality by design in the IoT. Wirel. Commun. Mob. Comput. https://doi.org/10.1155/2017/3859836.

5. Bianchini, D., Avila, I., 2014. Smart cities and their smart decisions: ethical considerations. IEEE Technol. Soc. Mag. 33 (1), 33–40. https://doi.org/10.1109/MTS.2014. 2301854.

6. Cobb, S., 2016. Data privacy and data protection: US law and legislation. Available at: https://www.welivesecurity.com/wp-content/uploads/2018/01/US-data-privacylegislation-white-paper.pdf, Accessed date: 15 March 2018.
7. D. Diaz-Sanchez, A. Marin, F. Almenarez, A. Cortés, ‘‘Social Applications in the Home Network,” in IEEE Transactions on Consumer Electronics, Vol. 56, No.1, pp.220–225
8. Devabalaji, K.R., Thangaraj, Y., Subramaniam, U., Ramachandran, S., Elavarasan, R.M., Das, N., Baringo, L., Rasheed, M.I.A., 2020. A new approach to optimal location and sizing of DSTATCOM in radial distribution networks using bio-inspired cuckoo search algorithm. Energies 13 (18), 4615. http://dx.doi.org/10.3390/en13184615.
9. Greenfield, A., 2013. Against the Smart City (The City is Here for You to Use). Do Projects, New York.
10. Han J, Ishii M, Makino H. A hadoop performance model for multi-rack clusters. In: IEEE 5th international conference on computer science and information technology (CSIT). 2013. p. 265–74.
11. Bose, A. Chung, M. Leung, Adoption of identity theft countermeasures and its short-and long-term impact on firm value, MIS Q. 43 (2019) 313–327, https://doi. org/10.25300/MISQ/2019/14192.
12. Jain A.K., Bolle R., and Pankanti S., eds., Biometrics: “Personal Identification in a Networked Society”, Kluwer Academic Publishers, 1999
13. Jing Q, et al. Security of the internet of things: perspectives and challenges. Wirel Netw. 2014;20(8):2481–501.
14. Kitchin, R., 2014. The real–time city? Big data and smart urbanism. Geo Journal 79 (1), 1–14. https://doi.org/10.1007/s10708–013–9516–8. (February 2014).
15. Kitchin, R., 2016. The ethics of smart cities and urban science. Phil. Trans. R. Soc. A 374 (2083). https://doi.org/10.1098/rsta.2016.0115.
16. Marr, B., 2017. 17 ‘Internet Of Things’ facts everyone should read. Available at: https:// www.forbes.com/sites/bernardmarr/2015/10/27/17-mind-blowing-internet-of-things-facts-everyone-should-read/#63c4bda63505, Accessed date: 25 February 2018.
17. Mazhelis, O., Hämäläinen, A., Asp, T., Tyrväinen, P., 2016. Towards enabling privacy preserving smart city apps. In: Proceedings of the 2016 IEEE International Smart Cities Conference (ISC2). IEEE. https://doi.org/10.1109/ISC2.2016.7580755.
18. Moustaka, V., Vakali, A., Anthopoulos, L.G., 2018a. A systematic review for smart city data analytics. ACM Comput. Surv. https://doi.org/10.1145/3239566.
19. Neves, Pedro, et al., 2017. Future mode of operations for 5G – The SELFNET approach enabled by SDN/NFV. Comput. Stand. Interfaces 54 (4).
20. Porambage P, et al. The quest for privacy in the internet of things. IEEE Cloud Comp. 2016;3(2):36–45
21. Prabhakar S., Pankanti S and Jain A., “Biometric Recognition: Security and Privacy Concerns”, published by the IEE Computer Society, 2003.
22. S. Dewan, F. Ren, Risk and return of information technology initiatives: evidence from electronic commerce announcements, Inf. Syst. Res. 18 (2007) 370–394, https://doi.org/10.1287/isre.1070.0120.
23. S.C. Margaret, M. Atilano, C.L. Arnold, Improving customer relations with social listening: A case study of an American academic library, 2017.
24. Solomon, M.G., Sunderam, V., Xiong, L., Li, M., 2016. Enabling mutually private location proximity services in smart cities: A comparative assessment. In: Proceedings of the 2016 IEEE International Smart Cities Conference (ISC2). IEEE. https://doi.org/10. 1109/ISC2.2016.7580757.
25. Townsend, A., 2013. Smart Cities: Big Data, Civic Hackers, and the Quest for a New Utopia. W.W. Norton & Co., New York.
26. V. Vasic, A. Antoni ´ c, K. Pripu ´ ziˇ c, M. Mikuc, I. P. ´ Zarko, Adaptable ˇ secure communication for the Cloud of Things, Software: Practice and Experience 47 (3) (2017) 489–501.
27. X. Luo, J. Zhang, W. Duan, social media and firm equity value, Inf. Syst. Res. 24 (2013) 146–163, https://doi.org/10.1287/isre.1120.0462.