IOT BASED LIVING SCENARIO IN INDIA: CRITICAL THINKING PERSPECTIVE

Abstract

IOT based technologies be it in the segment of Healthcare, Mobility, Traffic control, Navigation, Smart home, Smart community, Smart city, Banking, Agriculture, Social media, Education has been well researched upon. In depth research for IOT based scenarios is required for - Special needs, Politics and journalism, Entertainment, Retail, Manufacturing, e-Governance, Surveillance and Geriatric care. There are several security issues, threats and challenges with IOT based living scenarios. The paper presents views on Living Scenarios of IOT based Applications, Critical thinking and cyber laws that regulate the IOT powered systems.

Keywords: Future, India, Connectedness, Security, Law, Scenarios

Authors

Deepshikha
Design and Innovation
Jamia Millia Islamia, Okhla
Delhi, India
emaildeepshikhajha@gmail.com

Avinav Krishna
International Relations
South Asian University, Delhi
Delhi, India

I. INTRODUCTION

IOT based technologies be it in the segment of – Healthcare (Bhunia, 2015), Mobility (Xiao, 2017), Traffic control, Navigation, Smart home (Balakrishnan, et al 2018; Khawla and Tomader, 2018), Smart community (Ramesh, 2019), Smart city (Guan and Pei, 2022), Banking, Agriculture (Mishra, et al 2019; Celestrini, et al 2019), Social media (Ayele and Skielse, 2017), Education (Diaz, et al 2018; Magnus, et al 2021; Jean, et al 2021; He, et al 2017; Lian, 2021) – has been well researched upon. In depth research for IOT based scenarios is required for - Special needs (Ferati, et al 2016; Baykal, et al 2020), Politics and journalism, Entertainment, Retail (Kahlert and Constantinides, 2017), Manufacturing, e-Governance (Hedestig, et al 2018; Prakash and Gunalan, 2020; Musyoka, 2008), Surveillance and Geriatric care. There are several security issues, threats and challenges with IOT based living scenarios (Hwang, 2015; Venkatraman, et al 2020; Loi, et al 2017; Chow, 2015; Conti, et al 2017; Salim, et al 2018). The paper presents views on Living Scenarios of IOT based Applications, Critical thinking and cyber laws that may regulate the IOT powered systems.

II. LIVING SCENARIOS OF IOT BASED APPLICATIONS

The scenarios could be from a common man's perspective or from an administrator's point of view. From the perspective of a common man the scenario could be rural or urban. The authors first five scenarios posit the life in urban settings, then rural setting, manufacturer's and government's point of view.

Scenario 1: A young working male, 26-year-old wakes up to his alarm in the morning. The AC is auto controlled for temperature, geyser automatically heats the water optimally and stays on instant mode. He steps on the ground, the rug on the floor measure body fitness with health sensors. The curtains/blinds automatically roll up. He enters kitchen, morning news and weather report tunes in on radio, he makes his coffee, drink and breakfast. By the time, he gets ready, his cab (auto booked from a navigation app facility) is waiting at door step. He leaves the house, all appliances shut, door lock enabled with recognition, safety sensors around the house with wifi connectivity are on the run. Smart home and navigation were IOT connected applications for this scenario.

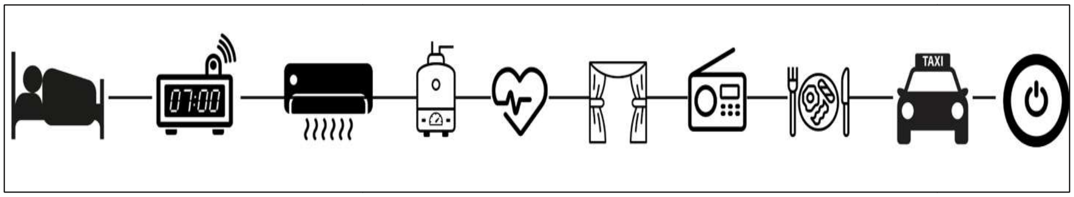

Figure 1: Scenario 1: Routine of the user as depicted through icons

Scenario 2: An adolescent female, 13-year-old, studies in class 8th of a private school. Reaches home at 2 pm, finishes lunch, takes shower, rest for a while. 3.30 pm to 5.00 pm revises lesson learnt in class today uploaded on a shared platform. 5 – 7pm goes out to play, hopefully children play as was done in 80s or 90s or takes yoga or swimming lessons. 7.30 to 9.30 pm completes homework and uploads on the connected platform. 10-12 pm fills her time with social media and entertainment. 12pm retires to sleep. IOT connected applications used were smart home, educational platform, social media and entertainment.

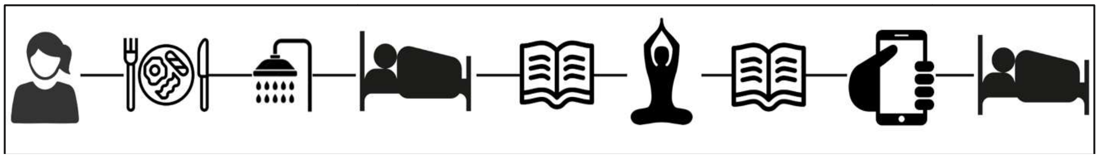

Figure 2: Scenario 2: Routine of the user as depicted through icons

Scenario 3: 60-year-old man has uneven heartbeat. He lives alone in the house. The data is picked up by his textile sensor/ smart band and transferred to his daughter working 10 kms away in the same city. She arranges an appointment with cardiologist, arranges a cab for pick up and drop and calls domestic help for ushering her father to the hospital. She joins him after four hours. The checkup has been done by then and data uploaded in patient's history for record keeping. IOT connected applications used were smart textile, healthcare and navigation.

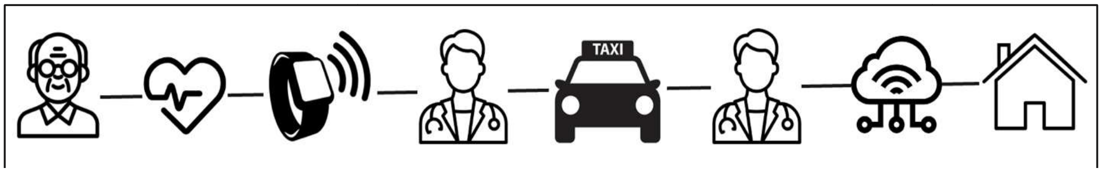

Figure 3: Scenario 3: Depicted through icons

Scenario 4: A 32-year-old woman, works Mon-Fri 9am – 5 pm. It is a Saturday and she has to buy grocery, fruits and vegetables, clothes for herself, her son and husband and small desk for her son. She opts for online purchase of the entire list of things she has to buy, makes online payment. The contactless delivery will be received at the door and kept by the delivery person in a cabinet securely locked which can be accessed only through password. The lady herself will not be available at home when the deliveries come home. IOT connected applications used were smart retail and smart home (Furniture – sealed cabinet for contactless deliveries).

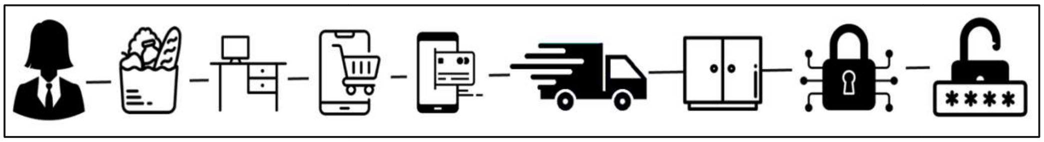

Figure 4: Scenario 4: Depicted through icons

Scenario 5: A working professional, 40-year-old, who has recently lost his job is seemingly depressed. An abrupt change in everyday living patterns as observed by his personal health app, in addition to an increased use of words expressing emotional turmoil as picked up by the sensors used for entertainment and language input and the above two corroborated by the recent search engine queries made by the person alerts a feedback mechanism, inbuilt in the IOT system, which oversees the mental health of the concerned person. He is suggested to avail counselling/therapy or reach out to friend or family or take a vacation by finding the best deals to the nearest tourist attraction. IOT based health services are applied in this scenario (Figure 5).

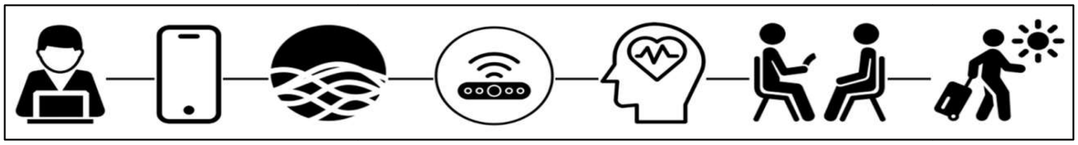

Figure 5: Scenario 5: Depicted through icons

Scenario 6: A Businessman, 50-year-old lives in urban setting, needs to access bank details for transfer of certain amount of money for business purposes. Accesses bank account via face recognition/fingerprint identification. Voice to text command is identified by the system for transaction of specified amount to beneficiary. Confirmation via face recognition/fingerprint is done. Amount is transferred (Figure 6). IOT connected applications used were smart banking controlled by a device like app operated smart phone/tab.

Figure 6: Scenario 6 depicted through icons

Scenario 7: A tax consultant, who deals with in ternational payments and investments, is to make a payment on behalf of his client to an entity which has recently been sanctioned for violating international norms. Ignorance of facts can be excused but not ignorance of law. In such dynamic fields IOT applications, maintained and updated by international organisationscan help professionals to follow the law, avoid breaking a law and simultaneously maintain the integrity of their profession (Figure 7).

Figure 7: Scenario 7: Depicted through icons

Scenario 8: A farmer in a rural region in India needs daily weather report, waters the farms automatically, sprays pesticides automatically as prescribed and regularly updated by agricultural department, manages the entire farm, vertical farm and hydroponic farm through IOT based services. Taking care of the dairy cattle health, washing area for cattle, maintaining temperature, spraying repellants, etc. done by IOT based system (Figure 8).

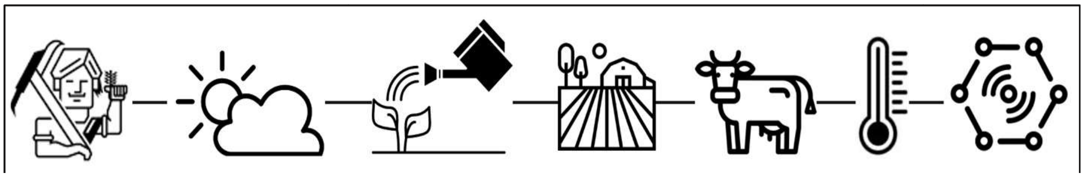

Figure 8: Scenario 8: Depicted through icons

Scenario 9: A Manufacturer who owns a unit in a semi urban region, records information of - marketing, operations, sales, finance, purchase, HR departments meticulously – attendance of the workers, health of workers, daily operations, purchase, dispatch, financial transactions, production records, machinery failure, machinery repair, production loss, running time and breaks, night shift operations, client profile and all other daily information on one connected IOT platform securely accessed by the administrators authority (Figure 9).

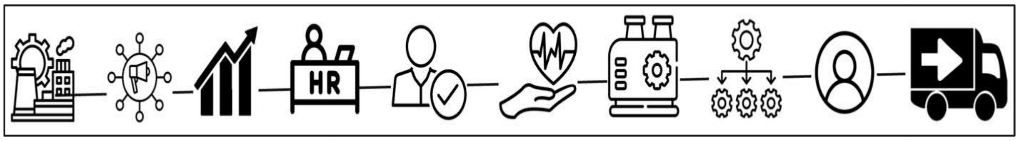

Figure 9: Scenario 9: Depicted through icons

Scenario 10: Government has a rather complex system to monitor. It is highly debatable whether all the data from every aspect of daily life should be accessed and stored by government or not or if at all, then up to what level of information should be accessible. Nevertheless, e-governance might lead to a highly scrutinized and regulated life in coming future. The case is only a hypothetical scenario of government's control on people's data. So, the respective Ministries have their respective online repositories where daily activities of the departments, organizations and workforce within them is monitored. Personal data of citizens is stored with the cyber security cell locally and centrally. Private institutions have their own repositories where data is stored and secured.

III. ONE DEVICE THAT CONTROLS ALL

As we continue further from the scenarios presented earlier, all the information is accessible through a web based or app-based service that is monitored by the government or a defined supreme authority. The data is accessible and controlled by a tab, laptop, smart phone, smart watch or smart band. Voice based, gesture based and text-based commands are read by the operating system. Fingerprint based or face recognition based secure access is provided by the user to unlock the system. The data can be accessed through internet connectivity only.

IV. CRITICAL THINKING

Prime security challenges for IOT based networks include - Lack of visibility, Limited security integration, Open-source code vulnerabilities, Overwhelming data volume, Data Storage, Poor testing and development, Unpatched vulnerabilities, Vulnerable Application programming interfaces, Malware, Ransomware, Data leaks, Escalated cyberattacks, Information theft and unknown exposure, Device mismanagement and misconfiguration, Cost to user, Cost to administrator, Complex environments, increase in remote working, and Weak passwords, among others. Can we avoid IOT from encroaching into our lives? Can we avoid surveillance? Who owns the data? Does the administrator assure security? Does it make life seamless with smooth operations? Do the disadvantages outweigh the advantages? How bad is present, if that remains the future? – Are some of the questions that often come into users' mind when thinking of IOT living scenarios. Data breach happens due to either an error in technology or mistake via user behavior. Present internet usage by millions across the globe suggest that users prefer convenience over security which allows cyber criminals to attack and escape since the laws are not very speedy to provide remedial measures. The law needs to get as speedy as the internet generation gets speedier in activities across the internet. Data breach may occur due to an accidental insider, a malicious insider, lost or stolen device or malicious outsider. Phishing, brute force attack or malware may be the reason for data breach. Few common vulnerabilities can include – weak credentials, stolen credentials, compromised assets payment card frauds or third-party access.

V. CYBER LAW REGULATIONS

Indian law deals with cybercrime through - Information Technology Act, 2000 and Indian Penal Code, 1860. Clearly it needs careful revision and amendments since the laws from 1860 might not serve contextual purposes of needs of IOT userbase generation of present times. The IPC's Most Pertinent Section Addresses Cyber Frauds: Forgery (Section 464), False documentation (Section 465), Forgery pre-planned for cheating (Section 468), Reputation damage (Section 469), Presenting a forged document as genuine (Section 471). Few prominent sections of IT act include - Section 43, 66, 66B, 66C, 66D. Cyber law may be defined broadly as a legal system that covers internet, computer systems, cyberspace and aspects of information technology. Cybercrime may largely include - Child Pornography, Hacking, Denial of service attack, Virus dissemination, Computer Forgery, Card fraud, Phishing, Spoofing, Cyber Stalking, Threatening, Salami Attack, Email bombing, Data Diddling, Virus Attacks, Logic Bombs, Trojan Attacks, Internet time thefts, Cybersquatting, Cyber Defamation, Keystroke Logging, Data-driven attacks, DNS spoofing, Dumpster diving among others. Advantages of cyber law include - Protecting personal information, Combatting cybercrime, Promoting fair competition, Facilitating e-commerce and Protecting intellectual property. Disadvantages of cyber law include - Complexity and confusion, time taking lengthy procedures, Limited jurisdiction, Encroachment on civil liberties, Slowing down innovation and Lack of universal standards. Cyber crime investigation may not be affordable to everyone, security patches may backfire, needs constant monitoring, slows down the system, difficult to track fake-ids, streaming platform surveillance is needed, age identification and authentication is required and investigation can prove risky for the victim or user.

VI. SUMMARY

The life in IOT scenarios will certainly be very different from present times. Communication, lifestyle, transportation, environment, retail, education, healthcare will see transformational changes. The sense of privacy will definitely be compromised as technological gadgets will record every data and transmit to the IOT cloud storage. Being under constant surveillance will become a common phenomenon. Life might become more sedentary as everything will be readily available and people might lose personal touch with people and planet. The positives of living in IOT scenario may not be able to outweigh the negatives of living in IOT scenario. In healthcare it may help in smart diagnosis, remote diagnosis and treatment, error reduction in treatment, reduce cost of treatment and accessibility. In agriculture it may help in precision farming, drone based monitoring and smart greenhouses. In automotive industry solar powered driverless cars and metros may become a common scenario. In education, remote education and home education might become a common phenomenon. Yet several issues might remain difficult to fix such as – standardization, mobility support, transport protocol, traffic characterization, authentication, data integrity, privacy and digital forgetting. Lot of training might also be needed for the users to get accustomed to the new IOT services and devices which have to be created by authorized agencies and monitored and updated from time to time. IOT encourages M 2 M communication, i.e. Machine to Machine communication which may reduce the need to communicate with individuals. IOT will certainly lead to over-reliance on technology and loss of jobs as smart machines start taking over manual jobs. IOT also presents wide variety of challenges such as - Identification in the IoT environment, Authenticating devices, Data Combination, Scalability in IoT, Secure Setup and Configuration, Critical Infrastructure, Conflicting market interest, Human-IoT Trust relationship, Data management and Lifespan of IoT's entities needs to be determined. IOT living scenarios are inevitable and the control is not in common man’s hand as the data will be controlled by either the government or multinationals with competing interests. Hence, it is required to generate awareness of how to’s and do’s and don’t’s strictly governed by law for maximum protection and speedy remedial services in case of failure or breach of safety protocols.

REFERENCES

[1] Bhunia, S.S. 2015. Adopting internet of things for provisioning health-care. UbiComp/ISWC'15 Adjunct: Adjunct Proceedings of the 2015 ACM International Joint Conference on Pervasive and Ubiquitous Computing and Proceedings of the 2015 ACM International Symposium on Wearable Computers. Pages 533–538. https://doi.org/10.1145/2800835.2801660

[2] Ramesh, M.N. 2019. Integration of participatory approaches, systems, and solutions using IoT and AI for designing smart community: Case studies from India. TESCA'19: Proceedings of the 1st ACM International Workshop on Technology Enablers and Innovative Applications for Smart Cities and Communities. November 2019. Pages 4–5. https://doi.org/10.1145/3364544.3371501

[3] Guan, W and Pei, Z. 2022. An Integrated Social-Technical Framework of Smart City based on Internet of Things and Cloud Computing. ICIT '22: Proceedings of the 2022 10th International Conference on Information Technology: IoT and Smart City. December 2022. Pages 197–203. https://doi.org/10.1145/3582197.3582231

[4] Xiao, B. 2017. Self-evolvable knowledge-enhanced IoT data mobility for smart environment. IML '17: Proceedings of the 1st International Conference on Internet of Things and Machine Learning.October 2017. Article No.: 28. Pages 1–14. https://doi.org/10.1145/3109761.3109789

[5] Balakrishnan, S, Vasudevan, H and Murugesan, R.K. 2018. Smart Home Technologies: A Preliminary Review. ICIT '18: Proceedings of the 6th International Conference on Information Technology: IoT and Smart City. December 2018. Pages 120–127. https://doi.org/10.1145/3301551.3301575

[6] Khawla, M and Tomader, M. 2018. A Survey on the Security of Smart Homes: Issues and Solutions. ICSDE'18: Proceedings of the 2nd International Conference on Smart Digital Environment. October 2018. Pages 81–87. https://doi.org/10.1145/3289100.3289114

[7] Mishra, D, Pande, T, Agarwal, KK, Abbas, A, Pandey, A and Yadav, RS. 2019. Smart agriculture system using IoT. ICAICR '19: Proceedings of the Third International Conference on Advanced Informatics for Computing Research. June 2019. Article No.: 39. Pages 1–7. https://doi.org/10.1145/3339311.3339350

[8] Celestrini, J, Rocha, RN, Saleme, EB, Santos, Cs, Filho, J G and Andreao, RV. 2019. An architecture and its tools for integrating IoT and BPMN in agriculture scenarios. SAC '19: Proceedings of the 34th ACM/SIGAPP Symposium on Applied Computing. April 2019. Pages 824–831. https://doi.org/10.1145/3297280.3297361

[9] Hedestig, U, Skog, D and Soderstrom, M. 2018. Co-producing public value through IoT and social media. dg.o '18: Proceedings of the 19th Annual International Conference on Digital Government Research: Governance in the Data Age. May 2018. Article No.: 22. Pages 1–10. https://doi.org/10.1145/3209281.3209349

[10] Ayele, WY and Skielse, GJ. 2017. Social media analytics and internet of things: survey. IML '17: Proceedings of the 1st International Conference on Internet of Things and Machine Learning. October 2017. Article No.: 53. Pages 1–11. https://doi.org/10.1145/3109761.3158379

[11] Diaz, JSS, Zambrano, EC and Zapater, JJS. 2018. State of the art about use of IoT in education. EATIS '18: Proceedings of the Euro American Conference on Telematics and Information Systems. November 2018. Article No.: 22. Pages 1–5. https://doi.org/10.1145/3293614.3293655

[12] Magnus, JP, Lopez, MG and Govea, JMO. 2021.Remote Challenge-Based Education through IoT.DSDE '21: 2021 4th International Conference on Data Storage and Data Engineering. February 2021. Pages 117–128. https://doi.org/10.1145/3456146.3456165

[13] Jean, D. Stein, G and Ledeczi, A. 2021. Hands-On IoT Education with Mobile Devices. IPSN '21: Proceedings of the 20th International Conference on Information Processing in Sensor Networks (co-located with CPS-IoT Week 2021). May 2021. Pages 390–391. https://doi.org/10.1145/3412382.3458778

[14] [14] He, JS, Ji, S and Bobbie, PO. 2017. Internet of Things (IoT)-based Learning Framework to Facilitate STEM Undergraduate Education. ACM SE '17: Proceedings of the SouthEast Conference. April 2017. Pages 88–94. https://doi.org/10.1145/3077286.3077321

[15] Lian, Y. 2021. Smart Education: Education Reform in the Age of Intelligence. ICEEL '21: Proceedings of the 2021 5th International Conference on Education and E-Learning. November 2021. Pages 41–45. https://doi.org/10.1145/3502434.3502478

[16] Ferati, M, Kurti, A, Vogel, B and Raufi, B. 2016. Augmenting requirements gathering for people with special needs using IoT: a position paper. CHASE '16: Proceedings of the 9th International Workshop on Cooperative and Human Aspects of Software Engineering. May 2016. Pages 48–51. https://doi.org/10.1145/2897586.2897617

[17] Baykal, G, Mechelen, MV and Eriksson, E. 2020. Collaborative Technologies for Children with Special Needs: A Systematic Literature Review. CHI '20: Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems. April 2020. Pages 1–13. https://doi.org/10.1145/3313831.3376291

[18] Kahlert, M and Constantinides, E. 2017. The relevance of technological autonomy in the customer acceptance of IoT services in retail. ICC '17: Proceedings of the Second International Conference on Internet of things, Data and Cloud Computing. March 2017. Article No.: 12. Pages 1–7. https://doi.org/10.1145/3018896.3018906

[19] Prakash, S and Gunalan, I. 2020. A new business model for digital governance of public records using blockchain. ICEGOV '20: Proceedings of the 13th International Conference on Theory and Practice of Electronic Governance. September 2020. Pages 124–128. https://doi.org/10.1145/3428502.3428518

[20] Musyoka, J. 2008. Social electronic governance: re-visiting the redistribution question through coordinating relations between electronic governance and social goals. ICEGOV '08: Proceedings of the 2nd international conference on Theory and practice of electronic governance. December 2008. Pages 39–43. https://doi.org/10.1145/1509096.1509106

[21] Hwang, YH. 2015. IoT Security & Privacy: Threats and Challenges. IoTPTS '15: Proceedings of the 1st ACM Workshop on IoT Privacy, Trust, and Security. April 2015. Pages 1. https://doi.org/10.1145/2732209.2732216

[22] Venkatraman, S, Overmars, A, Fahd, K, Parvin, S and Kaspi, S. 2020. Security Challenges for Big Data and IoT. BDET 2020: Proceedings of the 2020 2nd International Conference on Big Data Engineering and Technology. January 2020. Pages 1–6. https://doi.org/10.1145/3378904.3378907

[23] Loi, F, Sivanathan, A, Gharakheili, HH, Radford, A and Sivaraman, V. Systematically Evaluating Security and Privacy for Consumer IoT Devices. IoTS&P '17: Proceedings of the 2017 Workshop on Internet of Things Security and Privacy. November 2017. Pages 1–6. https://doi.org/10.1145/3139937.3139938

[24] Chow, R. 2015. IoT Privacy: Can We Regain Control? IH&MMSec '15: Proceedings of the 3rd ACM Workshop on Information Hiding and Multimedia Security. June 2015. Pages 3. https://doi.org/10.1145/2756601.2756623

[25] Conti, M, Natale, G, Heuser, A, Poppelman, T and Mentens, N. 2017. Do we need a holistic approach for the design of secure IoT systems? CF'17: Proceedings of the Computing Frontiers Conference. May 2017. Pages 425–430. https://doi.org/10.1145/3075564.3079070

[26] Salim, J, Hammoudeh, M, Raza, U, Adebisi, B and Ande, R. 2018. IoT standardisation: challenges, perspectives and solution. ICFNDS '18: Proceedings of the 2nd International Conference on Future Networks and Distributed Systems. June 2018. Article No.: 1. Pages 1–9. https://doi.org/10.1145/3231053.3231103