Turkish Online Journal of Qualitative Inquiry (TOJQI)
Volume 12, Issue 6, July, 2021: 9454 - 9463

Research Article

Securing Green IoT Infrastructure Using Blockchain Based Machine Learning Intrusion detection system

Abdurazzag A Aburas[a], Hassan Adegbola Afolabi[b]

[a,b]School of Electrical, Electronic and Computer Engineering
University of Kwazulu-Natal Durban, South Africa

***Corresponding author:** mufid.prof@gmail.com

Abstract

Internet of Things (IoT) is an emerging technology which enables several devices to be connected together in unprecedented ways in the smart world. Regardless of the diverse benefits offered by IoT connected devices, it comes along with several environmental threats due to huge energy consumption amongst IoT devices which embraces toxic pollutions and E-waste. Hence, to optimize the advantages of IoT there lies an important need to move towards green IoT. Cloud computing on the other hand has been successfully used to provide unlimited computational storage and services for numerous IoT devices over the internet. Sadly, security issues in cloud computing for green IoT is also a challenge. Furthermore, blockchain technology is transforming several application areas of IoT by allowing a decentralized environment. IoT systems can be properly secured against threats and attacks when combined with blockchain technology. Motivated by achieving a sustainable environment for IoT and its robustness against threats and attacks, this research presents an overview regarding green IoT technologies and the strategies used to minimize energy consumption in IoT. Additionally, it presents research challenges on security and privacy issues in green IoT and focuses on how to integrate blockchain technologies in Green IoT environment to prevent attacks, and the possible combination of blockchain technology with intrusion detection systems.

Keywords: Blockchain, Cloud-computing, Energy efficiency, E-waste, IoT, Intrusion detection system

1. Introduction

Recent technology advancements in the field of Internet of Things (IoT) and cloud computing has changed the way we work and live [1]. As forecasted, IoT technology is bound to control different spheres of our lives in the 21st century by incorporating billions of smart devices interconnected with the IoT control systems. These include but not limited to smart power grid, smart transport system, smart health etc. Regardless of the number of benefits offered by IoT connected devices, the technology has also been noted to come along with several environmental threats as there is a huge energy consumption amongst IoT devices and it embraces toxic pollutions and E-waste. Due to this factor, green IoT has been considered the future IoT as it proposes the concept of energy efficiency of IoT devices and making the environment safe [2]. Hence, to optimize the advantages of IoT there lies an important need to move toward green IoT. IoT technology relies on cloud computing for the purposes of data and applications hosting.

The numerous devices employed in implementation of IoT technologies may pave way for several security vulnerabilities if proper administration of these devices is not observed. This makes Cloud computing security on green IoT a big challenge. Therefore, without proper security and authentication procedures, data security and integrity may be compromised leading to breach of data privacy policies [3].

While security in cloud computing and IoT remains a major concern, security vulnerabilities can be greatly mitigated by putting proper security strategies in place during implementation of IoT systems to utilize the full capabilities brought by these technologies. Efforts should also be made to study all anticipated security vulnerabilities and possible solutions like the blockchain technology which can be effectively applied in almost all domains of IoT.

This will ensure alertness to deal with the likely security vulnerabilities if they arise.

2. Internet of Things

Internet of Things (IoT) is an emerging concept which aims to connect billions of devices with each other anytime regardless of their location. The foundational technologies for IoT are the radio frequency identification (RFID) technology, and the wireless sensor networks (WSNs). The RFID technology enables microchips to transmit the identification information of an object to a reader through wireless communication. These readers enable the automatic identification, monitoring and tracking of objects attached with RFID tags [4].

RFID technology are widely known to be adopted in production, retailing and logistic industries. The (WSNs) mainly use interconnected smart sensors for sensing and monitoring. Its application is widely used in traffic monitoring, environmental monitoring, healthcare monitoring e.t.c [5], [6]. The advances in both RFID and WSN technologies has significantly contributed to the development of IoT.

As the use of IoT rapidly evolves and increases, our daily activities and lifestyle has been revolutionized and improved by this technology and its application has been adopted in several domains. A few of those namely:

i. Smart Homes: This is one of the most important application of IoT. Equipping our homes and offices with IoT technologies like RFIDs, allows proper decisions making in terms of saving energy, money and environment in the process of tracking activities in such a building. [7] For example, a smart fridge, a smart tv e.t.c

ii. Smart Supply Chains: Using IoT technologies, industries and businesses can track their products to the end users. A framework for such an application is proposed in [8].

iii. Smart Cities: A smart city is a combination of different smart domains like Smart Energy Saving Mechanism, Smart Transportation, Smart Security [9] e.t.c It provide users with several technological facilities all under one umbrella and puts a lot of challenges in front of researchers.

Other applications of IoT includes Smart Grid, Wearables, Smart Health Care (Digital Health and Telemedicine) e.t.c

3. Green Internet of Things

There could be billions of devices connected to the Internet by 2025. However, the most significant challenge that we will face in implementation of IoT will be energy. Energy consumption of these devices may be a limitation for its widespread despite its numerous benefits. This is a huge concern because carbon emission and E- Waste due to ICT products will increase rapidly. This will damage our environment if appropriate measures are not put in place [10]. To address this problem, there is a critical need to move towards green IoT because it is environmentally safe. Green IoT is defined as the energy efficient ways in IoT either to reduce the greenhouse effect caused by existing applications or to eradicate the same in IoT itself [11]. It basically focuses on the energy efficiency in the IoT principles. In green IoT, every step in the IoT should be made green, It should focus on green design, green production, green utilization and green disposal or recycling to have a very little or no impact on the environment. In order to implement the Green IoT, a number of strategies should be adopted. A framework was proposed in [12] for the energy efficient optimization of IoT devices. The summary of a few of these strategies provided in this paper are Green RFIDs, Green Datacentres, Green Wireless Sensor Networks, Green Machine to Machine (M2M), and Green Cloud Computing.

i. Green RFIDs: The RFID tag is a small microchip attached to a radio (utilized for receiving and transmitting the signal), with a unique identifier. The purpose of RFID tags is storing information regarding the objects to which they are attached. RFIDs can either be active or passive, in order to achieve greener solutions for RFID systems, reduction in the sizes of RFID tags should be considered to decrease the amount of non-degradable material used in their manufacturing. Other initiatives to be considered include printable RFID tags [13], biodegradable RFID tags and paper- based RFID tags.

ii. Green data centre: The main purpose of a data centre is to store, manage, process and disseminate all types of data and applications created by users, things and systems. In dealing with various data and applications, data centres consume huge amounts of energy with high operational costs and large CO2 emissions. Hence, to achieve a green DC, the following techniques as discussed in [14]-[18], such as the use of renewable and green sources of energy (e.g. water, wind, solar energy etc.), the design of a more energy efficient hardware, utilization of efficient dynamic power-management technologies, the design of a novel energy-efficient data centre architecture to achieve power conservation, etc. should be considered.

iii. Green wireless sensor networks: A WSN is a network that consists of a large distributed autonomous sensor node and a base station (BS) known as the sink. These sensor nodes cooperatively monitor the physical and environmental conditions such as temperature, sound, vibration, level of humidity, pressure, motion, etc. to fully optimise the full benefits of WSNs, there is a need to pave way for greener systems that is environmentally safe. This can be achieved by ensuring data communication occurs at low power, adopting techniques discussed in [11], [19], [20] such as; energy depletion (e.g., wireless charging) and utilizing energy harvesting mechanisms which generate power from the environment (e.g., sun, kinetic energy, vibration, temperature differentials, etc.), radio optimization techniques (e.g., transmission power control, modulation optimization, cooperative communication, directional antennas, energy-efficient cognitive radio (CR)), data reduction mechanisms (e.g., aggregation, adaptive sampling, compression, network coding), energy-efficient routing techniques (e.g., cluster architectures, energy as a routing metric, multipath routing, relay node placement, node mobility).

iv. Green cloud computing: Depending on user’s demands, cloud computing offers different resources to users. These resources are treated as services, i.e., IaaS (Infrastructure as a Service), PaaS (Platform as a Service) and SaaS (Software as a Service). Therefore, with increasing applications moved to cloud, more resources need to be deployed and more power are consumed, resulting in more environmental issues and CO2 emissions. Therefore, a greener approach to cloud computing is necessary for the reduction of energy consumption. This can be achieved by efficiently using the resources in the cloud.

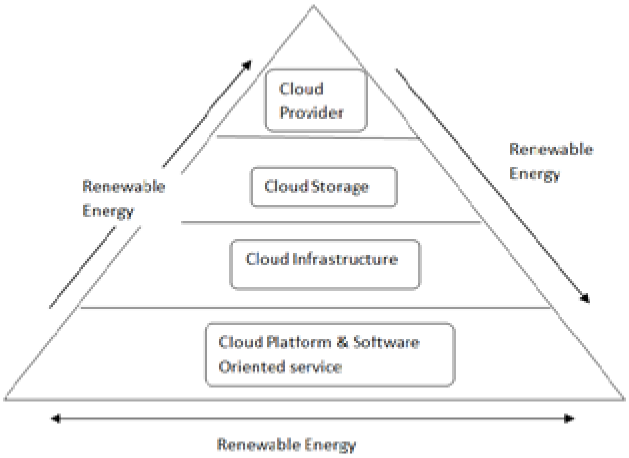

Fig. 1 Green Cloud Computing [21]

As illustrated in figure 2 above [21]. The green cloud computing model is fully based on the cloud environment with an adjustment on renewable energy usage and usage of available resources efficiently with reduction in carbon emissions from both cloud providers and users. The green cloud computing goal is reached once the reduction of carbon emissions from machines are implemented.

v. Green machine to machine: M2M is a technology that allows both wireless and wired devices to communicate with other devices of the same type. There are massive machines involved in M2M communications which enables it to consume a lot of energy. Therefore, energy efficiency should be increased to achieve a green M2M as discussed in [22]-[26] by (but not limited) to the following techniques; Intelligently adjusting the transmission power to the minimal necessary level, designing an efficient communication routing protocols with the application of algorithmic and distributed computing techniques, activity scheduling (switching some nodes to sleep mode ‘low-power operation’ so that only a subset of connected nodes remain active while keeping the functionality of the original network).

4. Green Cloud Computing and Internet of Things

Cloud computing provides computing capabilities, storage capacity, services and applications over the Internet. On the other hand, Internet of things is also an emerging technology which allows billions of physical objects to be connected for the purpose of collecting and exchange of data for offering various applications. Both concepts have seen an independent evolution in their hardware and software aspects over the years and have evolved separately. Researchers found that cloud computing could solve the dilemma of computational capabilities, storage capacity and energy efficiency that are experienced by IoT devices. As a result, the need to integrate CC and IoT technologies emerge and the concept of Cloud of Things (CoT) was founded [27], [28]. Its integration has since generated a lot of advantages for them both as CC is usually involved during the processing of data generated by IoT devices. As a result of tremendous growth of CoT, there's is an increase in demand for energy by the billions of devices connected together due to very large amount of data and information exchange amongst them.

A report published by Gartner [29], estimated that the global ICT industry accounted for approximately 2% of global CO2. Therefore, there lies the critical need to move towards green cloud computing and green IoT to optimize the benefits of CoT. Green cloud architecture was presented by Liu et al. [30], it aims to decrease energy consumed by data centre. This would be financially beneficial and an effective approach for environmental safety. However, green computing is not limited to the energy consumption of computer devices only, it also includes all other environmental issues, such as CO2 emissions, (e-)waste management, and consumption of natural resources. The evolution of this research was determined by the increase in interest in the environment and by the extended use of cloud computing.

5. Implementation of Green IOT Infastructure

The green processes include both green computing technologies and green communication. Green computing focuses more on the utilization of ICT equipment in an environment friendly manner. This can be achieved by reduction of the amount of energy and greenhouse gas emissions, reduction in the number of devices needed by servers and data centers, improving storage space and cost efficiency, better time management and efficiently recycling of equipment's. Green communication focuses more on the reduction of energy consumption and carbon dioxide emissions during communication which makes it a more challenging issue. The main objectives under green communication process include but not limited to efficient wireless communication, green routing, developing communication architectures etc.

This section presents a brief study on how green IoT can be implemented. Aside from ensuring that the above discussed IoT enablers are green, several literatures have adopted different techniques to implement green IoT. These techniques include:

i. Software based techniques: The energy efficiency of an IoT network predominantly depends upon the energy management in the data centers. An e-policy using Orchestration Agent (OA) proposed in [22] intelligently selects the servers based on their energy consumption. The selected servers then process the data and send them back to their clients.

ii. Hardware based techniques: Changes can be made to the hardware devices in IoT in order to achieve a green IoT. A dual core processor developed with CoreL and CoreH, CoreLH [23] for low and high computation tasks respectively for IoT. This framework reduces energy consumption by assigning different tasks to the CoreL and CoreH depending upon the resources they require.

iii. Policy based techniques: Several policies and strategies can be put in place for efficient conservation of energy. These techniques include the monitoring of energy consumption in different scenarios.

iv. Awareness based techniques: Many awareness can be held to inform IoT users about their energy consumption, this technique can save almost 10% energy [24] i.e the provision of Smart Metering Technology to homeowners will inform them of their energy consumption in real-time and enable them control and minimize it.

v. Changing habits towards green IoT: Users can change habits and routine to save energy. Energy can be saved by keeping track of its consumption through various automation systems as discussed in [25], [26] and [31]. As little as its impact may seem on an individual level, it can make a big difference when taken as a whole.

vi. Recycling for green IoT: The devices used in the IoT network can be made with environmentally friendly and recyclable materials. For instance, some non-biodegradable materials are used in mobile phones manufacturing such that they exist in billions when discarded and thereby leading to greenhouse effect. A significant difference can be made in the reduction carbon footprint if recyclable materials are used. Several approaches are made in [32] for the performance improvement of smart phones and effective recovery of electric and electronic equipment.

The solutions discussed may have some shortcomings, so there is a need to look for more realistic and applicable ways to reduce the energy consumption. Based on the above discussed techniques, we propose the following strategies to achieve a Green IoT infrastructure:

i. Reducing the IoT network size by the use of optimum routing methods and efficiently placing nodes

ii. Sensing data selectively in a particular scenario by collecting only the required data

iii. Putting in place proper energy efficient strategies and policies for IoT infrastructure i.e smart building.

iv. The use of architectures that contain both passive and active sensors for discrete tasks.

v. Intelligently choosing trade-offs and prioritizing communication and/or cost accordingly.

6. Security and Privacy Threats in Green Cloud of Things

Just like IoT technology, green IoT relies on cloud computing for purposes data and applications hosting. The billions of connected devices in IoT technologies may cause several security vulnerabilities and expose it to cyber threats. Thus, making security in cloud computing for green IoT a big challenge. A threat can be defined as the ability of an adversary on an asset of a system with an intent to invade the privacy of users in a system or the security of the system as a whole [33]. The aim of this section is to identify possible threats in relation to two categories: security and privacy. Security entails the mechanisms used to ensure the integrity, availability and confidentiality of data at different points in a system. Whereas privacy is the ability to control privileged access to a certain data that may contain very sensitive information of a user within a system [33]. An overview of several security and privacy threats for any CoT system is made as shown in the figure below.

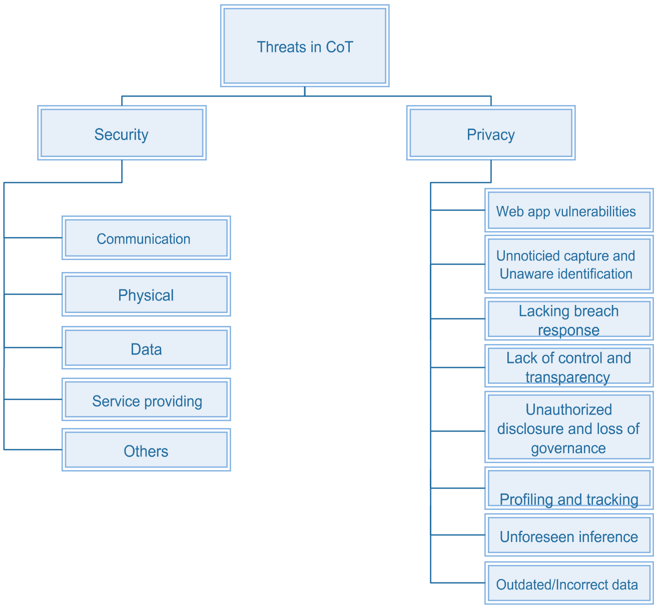

FIGURE 3. Taxonomy of Threats in CoT. [34]

i. Security threats: Threats that can compromise the security of a CoT system belongs to this category and they are communication threats, physical threats, data threats, service provisioning threats and other threats. Each of these sub-categories along with the identified threats is discussed below. [33].

In communication threats, communication channel can be abused by an attacker to initiate several threats. A typical example is the denial of service attacks (DoS). This attack can reduce or remove the capacity of a network to execute its expected function through hardware failures, resource exhaustion, software bugs and malicious broadcasting of high-energy signals. CoT is vulnerable to Dos attacks because of the limitation of devices. [35] [36].

Physical threats are Incidents that may lead to physical damage on connected devices or loss are categorized under physical threats. These threats can either be Internal (fire, unstable power supply etc), external (lightning, earthquakes etc) and human (theft, vandalism, errors which can be intentional or accidental, etc) [34].

Data threats are one of the most common threats to cybersecurity. Spamming, disabling security settings, stolen and/or corrupted data all falls in this category. Data breaches, data loss and leakages and false data injection are examples of threats that relies on data generated by CoT systems.

Other top threats which are not related to any of the previous categories are malicious Insiders, shared technology vulnerabilities, abuse and nefarious use of cloud services etc. [37], [38].

ii. Privacy threats: Since the issue of privacy mainly affects the users of a system, privacy threats are more focused on breaching and invading the privacy of the users within the CoT system. Several threats can be exploited to pervade the privacy of some users in a CoT system [34].

7. Blockchain Technology

Blockchain is a kind of decentralized database, which keeps record of every transaction made on a network. It can be implemented in a peer-to- peer network eliminating the need for trusted third party. Blockchain can be implemented in three categories namely consortium, public and private [39]. In consortium blockchains, a predefined consortium of peers is responsible for maintaining the chain whereas in public blockchains like Bitcoin and Ethereum [40] [41], all participants can read and maintain the ledger and a single participant controls the system in private blockchains.

The process of updating the blockchain takes place via a protocol, which achieves consensus, i.e. gives guarantees that there is uniformity between participants in view of the ledger that contains only valid transactions ensuring the integrity and consistency of the ledger [42]. This protocol depends on the type of the blockchain implementation and the threat model and may vary a lot.

8. Integrating Green IOT With Blockchain Technology to Prevent Attacks

The blockchain technology can effectively be applied in almost all domains of IoT. It can be used to provide access control in green IoT-based environment [43]. The application of blockchain technology for IoT is to ensure privacy-preserving and for encrypted data sharing. There are several factors that have to be considered to establish a secure IoT using blockchain technology

i. Secure communication: IoT devices have to communicate for the purpose exchanging data required to process a transaction and to store it in a ledger which can also be used to store encryption keys to make the exchanges more private. i.e. IoT node sends an encrypted message using the public key of the destination node, which is then stored in the blockchain network. The sending node gets the public key of the receiver from the ledger and it encrypts the message using public key of the receiving node [44].

ii. Authentication of users: The sending node digitally signs the message before sending them to other nodes. The receiving node then gets the public key from the ledger and uses it to verify the digital signature of the received message.

iii. Discovering legitimate IoT Device: Billions of IoT devices are to be connected on the same network in the coming years, there is an urgent need to get the ability to discover and differentiate between legitimate and illegitimate nodes [45]. Immediately a new IoT device joins a network, it asks root servers to give a list of trusted nodes in the network, it then registers itself in a node and can begin the exchange of information with other nodes in the network. The new device itself will be efficiently authenticated in private blockchain network to confirm its legitimacy.

iv. Configuring IoT: Blockchain technology assists in establishing a trusted and secure configuration for IoT devices. For example, Configuration details and the hash value of latest configuration file for every IoT device can be hosted on the ledger. To get the configuration details, the blockchain node is asked to get it from the ledger during bootstrap. Also, the IoT device will have to download the latest and trusted configuration file after every fixed interval of time using a cloud service. Then it can use the blockchain node API to retrieve and match the hash value, which is stored in the blockchain. Securing IoT devices interconnected with each other on a network with a blockchain technology makes the system decentralized because no single authority can approve any transaction. All devices have access to the ever-growing chain of data. Therefore, access to any device must be validated by all members of the network. The performed transaction is stored in a block and sent to all nodes in the network after validation. This process strengthens the security of the system and makes unauthorized access impossible.

9. Intrusion Detection System

Intrusion detection system is a well-known technique to protect networks against attacks. The task of an IDS is to detect unusual activities that potentially indicate ongoing attacks or malicious activities. it can provide two main functions

Alarm generation: An Ids generate alarms to inform the system administrator of identified anomalies. The effectiveness of an IDS can be determined by the measurement of false alarm rates.

Information gathering: An IDS can monitor the network and systems and gather information locally. Then, the gathered data can be sent to other systems for analysis.

There are different types and classes of IDS which employs different detection technique to detect different forms of attacks/malicious activities. For this research paper, our main focus will be on machine learning based collaborative IDS.

Collaborative Intrusion Detection System: Collaborative intrusion detection (CIDS) are IDSs with an enhanced performance of a single IDS. The system enables collaboration among participating IDS to prevent complicated and advanced attacks like denial of service (DoS) attack. Unfortunately, data and trust management are two main research challenges for current CIDS architectures which may reduce the effectiveness of such systems.

10. Blockchain-Based Intrusion Detection System

There is a chance of solving the challenges in intrusion detection with the emerging blockchain technology because of its design. For several decades that intrusion detection has been studied, there are still challenges of trust management and computation and data management especially in a collaborative IDS environment. Blockchains are one of the solutions that can be used to mitigate these challenges. For example, in data sharing issue, blockchains can help build mutual trust among participating parties and preserve data privacy.

Also, Machine learning (ML) techniques have been widely used in many IDS including collaborative IDS. CIDs have proved to be robust against common insider attacks. However, there is a need to improve the robustness of such system because of a few challenges. i.e it may still be prone to a more advanced insider attack. Also, without enough data, it is unable to optimize detection algorithms and to build a robust model for identifying suspicious events.

Motivated by the blockchain emerging technology, there is need to propose an advanced CIDS which will adopt blockchain technology for its collaboration and Machine learning algorithms for accuracy and effectiveness.

11. Conclusion

Although there is a tremendous research effort to achieve a green technology, green IoT technology is still in its early stage and there are many obstacles and challenges that needs to be addressed. Also, this research briefly discussed the possible benefits of emerging blockchain technology by internet of things and provides guidance for the use of blockchain technology to make a more secure and trustable IoT environment. A possible research direction in this paper could be exploring the applicability and impact of blockchain technology in the field of intrusion detection for improved accuracy and effectiveness especially in a collaborative intrusion detection environment because not all IDS challenges can be mitigated with this technology. Finally, as we keep an eye on such emerging technology, more research should be encouraged on Machine Learning Techniques for blockchain based IDS and dataset for blockchain based green IoT Scenarios.

References

[1] Mohiuddin, I., & Almogren, A. (2019). Workload aware VM consolidation method in edge/cloud computing for IoT applications. Journal of Parallel and Distributed Computing, 123, 204-214. https://doi.org/10.1016/j.jpdc.2018.09.011 , [accessed on Sept. 2020]

[2] Arshad, R., Zahoor, S., Shah, M. A., Wahid, A., & Yu, H. (2017). Green IoT: An investigation on energy saving practices for 2020 and beyond. IEEE Access, 5, 15667-15681.

[3] Aazam, M., & Huh, E. N. (2014, August). Fog computing and smart gateway-based communication for cloud of things. In 2014 International Conference on Future Internet of Things and Cloud (pp. 464-470). https://doi.org/10.1109/ficloud.2014.83 , [accessed on Sept. 2020]

[4] X. Jia, O. Feng, T. Fan, and Q. Lei, “RFID technology and its applications in internet of things (IoT),” in Proc. 2nd IEEE Int. Conf. Consum. Electron., Commun. Netw. (CECNet), Yichang, China, Apr. 21–23, 2012, pp. 1282–1285 https://doi.org/10.1109/cecnet.2012.6201508 , [accessed on Sept. 2020]

[5] S. Li, L. Xu, and X. Wang, “Compressed sensing signal and data acquisition in wireless sensor networks and internet of things,” IEEE Trans. Ind. Informat., vol. 9, no. 4, pp. 2177–2186, Nov. 2013. https://doi.org/10.1109/tii.2012.2189222 , [accessed on Sept. 2020]

[6] W. He and L. Xu, “Integration of distributed enterprise applications: A survey,” IEEE Trans. Ind. Informat., vol. 10, no. 1, pp. 35–42, Feb. 2014. https://doi.org/10.1109/tii.2012.2189221 , [accessed on Sept. 2020]

[7] S. Li, L. Da Xu, and S. Zhao, “The internet of things: a survey,” Inf. Syst. Front., vol. 17, no. 2, pp. 243–259, 2015. https://doi.org/10.1007/s10796-014-9492-7 , [accessed on Sept. 2020]

[8] Z. Pang, Q. Chen, W.Han,andL. Zheng, “Value-centric design of the internet-of-things solution for food supply chain: Value creation, sensor portfolio and information fusion,” Inf. Syst. Front., vol. 17, no. 2, pp. 289–319, 2015 https://doi.org/10.1007/s10796-012-9374-9 ., [accessed on Sept. 2020]

[9] aZanella,N.Bui,aCastellani,L.Vangelista,andM.Zorzi,“Internet of Things for Smart Cities,”IEEEInternetThingsJ.,vol.1,no. 1, pp. 22–32, 2014. https://doi.org/10.1109/jiot.2014.2306328. , [accessed on Sept. 2020]

[10] E.GelenbeandY.Caseau,“ The impact of information technology on energy consumption and carbon emissions,” Ubiquity, vol. 2015, no. June, pp. 1–15, 2015. https://doi.org/10.1145/2755977 , [accessed on Sept. 2020]

[11] F. K. Shaikh, S. Zeadally, and E. Exposito, “Enabling Technologies for Green Internet of Things,” IEEE Syst. J., no. 99, pp. 1–12, 2015. https://ieeexplore.ieee.org/document/7088546 , [accessed on Sept. 2020]

[12] Huang, Y. Meng, X. Gong, Y. Liu and Q. Duan, "A Novel Deployment Scheme for Green Internet of Things," in IEEE Internet of Things Journal, vol. 1, no. 2, pp. 196-205, April 2014, https://ieeexplore.ieee.org/document/6718032 , [accessed on Sept. 2020]

[13] Y. Amin, “Printable green RFID antennas for embedded sensors,” Ph.D. dissertation, KTH School Inf. Commun. Technol., Kista, Sweden, 2013.

[14] M. Dayarathna, Y. Wen and R. Fan, "Data Center Energy Consumption Modelling: A Survey," in IEEE Communications Surveys & Tutorials, vol. 18, no. 1, pp. 732-794, First quarter 2016, doi: 10.1109/COMST.2015.2481183, https://ieeexplore.ieee.org/document/7279063 , [accessed on Sept. 2020]

[15] T. Li, S. S. Wu, S. Chen and M. C. K. Yang, "Generalized Energy-Efficient Algorithms for the RFID Estimation Problem," in IEEE/ACM Transactions on Networking, vol. 20, no. 6, pp. 1978-1990, Dec. 2012, doi: 10.1109/TNET.2012.2192448, https://ieeexplore.ieee.org/document/6188523 , [accessed on Sept. 2020]

[16] X. Xu, L. Gu, J. Wang, G. Xing and S. Cheung, "Read More with Less: An Adaptive Approach to Energy-Efficient RFID Systems," in IEEE Journal on Selected Areas in Communications, vol. 29, no. 8, pp. 1684-1697, September 2011, doi: 10.1109/JSAC.2011.110917, https://www.infona.pl/resource/bwmeta1.element.ieee-art-000005992837 , [accessed on Sept. 2020]

[17] D. K. Klair, K. Chin and R. Raad, "A Survey and Tutorial of RFID Anti-Collision Protocols," in IEEE Communications Surveys & Tutorials, vol. 12, no. 3, pp. 400-421, Third Quarter 2010, doi: 10.1109/SURV.2010.031810.00037, https://ieeexplore.ieee.org/document/5455790 , [accessed on Sept. 2020]

[18] C. Lee, D. Kim and J. Kim, "An Energy Efficient Active RFID Protocol to Avoid Overhearing Problem," in IEEE Sensors Journal, vol. 14, no. 1, pp. 15-24, Jan. 2014, doi: 10.1109/JSEN.2013.2279391., https://ieeexplore.ieee.org/document/6584733, [accessed on Sept. 2020]

[19] G. Anastasi, M. Conti, M. Di Francesco, and A. Passarella, ‘‘Energy conservation in wireless sensor networks: A survey,’’ Ad Hoc Netw., vol. 7, no. 3, pp. 537–568, May 2009. https://doi.org/10.1016/j.adhoc.2008.06.003 , [accessed on Sept. 2020]

[20] T. Rault, A. Bouabdallah, and Y. Challal, ‘‘Energy efficiency in wireless sensor networks: A top-down survey,’’ Comput. Netw., vol. 67, pp. 104–122, Jul. 2014. https://doi.org/10.1016/j.comnet.2014.03.027, [accessed on Sept. 2020]

[21] Shanmugam, G.S. and N.C.S. Iyengar, Effort of load balancer to achieve green cloud computing: A review. International journal of multimedia and ubiquitous Engineering, 2016. 11(3): p. 317-332. http://dx.doi.org/10.14257/ijmue.2016.11.3.30 , [accessed on Sept. 2020]

[22] C. Peoples, G. Parr, S. McClean, B. Scotney, and P. Morrow, “Performance evaluation of green data centre management supporting sustainable growth of the Internet of Things," Simul. Model. Pract. Theory.

[23] Z. Wang, Y. Liu, Y. Sun, Y. Li, D. Zhang, and H. Yang, “An energy efficient heterogeneous dual-core processor for Internet of Things," in Proc. IEEE Int. Symp. Circuits Syst., Jul. 2015, pp. 2301_2304.

[24] C.McKerracher and J. Torriti, “Energy consumption feedback in perspective: Integrating Australian data to meta-analyses on in-home displays, "Energy Efficiency, vol. 6, no. 2, pp. 387_405, 2013

[25] C. Occhiuzzi, S. Caizzone, and G. Marrocco, “Passive UHF RFID antennas for sensing applications: Principles, methods, and classifications "IEEE Antennas Propag. Mag., vol. 55

[26] A. Fensel,V.Kumar, and S. D. K. Tomic, “End-user interfaces for energy efficient semantically enabled smart homes," Energy Efficiency, vol. 7, no. 4, pp. 655_675, 2014.

[27] M. Aazam, I. Khan, A. A. Alsaffar and E. Huh, "Cloud of Things: Integrating Internet of Things and cloud computing and the issues involved," Proceedings of 2014 11th International Bhurban Conference on Applied Sciences & Technology (IBCAST) Islamabad, Pakistan, 14th - 18th January, 2014, Islamabad, 2014, pp. 414-419, doi: 10.1109/IBCAST.2014.6778179., https://ieeexplore.ieee.org/document/6778179 , [accessed on July 2020]

[28] M. M. E. Mahmoud et al., "Enabling Technologies on Cloud of Things for Smart Healthcare," in IEEE Access, vol. 6, pp. 31950-31967, 2018, doi: 10.1109/ACCESS.2018.2845399. https://ieeexplore.ieee.org/document/8375951 , [accessed on 18 July 2017].

[29] Mingay, S. Green IT: The New Industry Shock Wave. 2007. Available online: http://www.ictliteracy.info/rf. pdf/Gartner_on_Green_IT.pdf (accessed on 18 July 2017).

[30] Kliazovich, D., Bouvry, P. & Khan, S.U. GreenCloud: a packet-level simulator of energy-aware cloud computing data centers. J Supercomput 62, 1263–1283 (2012). https://doi.org/10.1007/s11227-010-0504-1 , [accessed on July 2020]

[31] M. V. Moreno-Cano, M. A. Zamora-Izquierdo, J. Santa, and A. F. Skarmeta, “An indoor localization system based on artificial neural networks and particle filters applied to intelligent buildings”, Neurocomputing, vol 122, pp.116-125, Dec 2013.

[32] H. Falaki, D. Lymberopoulos, R. Mahajan, S. Kandula, and D. Estrin, “A first look at traffic on smartphones," in Proc. 10th Annu. Conf. Internet Meas. (IMC), 2010, p. 281.

[33] Ferdous, M. S., Hussein, R., Alassafi, M., Alharthi, A., Walters, R., & Wills, G. (2016). Threat taxonomy for cloud of things. Internet Things Big Data Anal Recent Trends Challenges, 1, 149-191.

[34] Ari, A.A.A., Ngangmo, O.K., Titouna, C., Thiare, O., Kolyang, Mohamadou, A., Gueroui, A.M., Enabling Privacy and Security in Cloud of Things: architecture, applications, security & privacy challenges, Applied Computing and Informatics (2019), doi: https://doi.org/10.1016/j.aci.2019.11.005, [accessed on July 2020]

[35] B. Alohali, Security in Cloud of Things (CoT), in: Cloud Security: Concepts, Methodologies, Tools, and Applications, IGI Global, 1188–1212, 2019. DOI: 10.4018/978-1-5225-8176-5.ch061 , [accessed on July 2020]

[36] R. Roman, J. Zhou, J. Lopez, On the features and challenges of security and privacy in distributed internet of things, Computer Networks 57 (10) (2013) 2266–2279. https://doi.org/10.1016/j.comnet.2012.12.018, [accessed on July 2020

[37] CSA, The Treacherous 12 - Cloud Computing Top Threats in 2016, Tech. Rep., Cloud Security Alliance, https://downloads.cloudsecurityalliance.org/assets/research/top-threats/Treacherous-12_Cloud-Computing_Top-Threats.pdf , [Accessed on 10-Feb-2018], 2016.

[38] CSA, Top Threats to Cloud Computing, Tech. Rep. V1.0, Cloud Security Alliance, URL https://cloudsecurityalliance.org/topthreats/csathreats.v1.0., [Accessed on 10-Feb-2018], 2010.

[39] Nakamoto, S.: Bitcoin: A peer-to-peer electronic cash system (2008)

[40] Okada, H., Yamasaki, S., Bracamonte, V.: Proposed classification of blockchains based on authority and incentive dimensions. In: Advanced Communication Technology (ICACT), 2017 19th International Conference on, pp. 593–597. IEEE (2017)

[41] Wood, G.: Ethereum: a secure decentralised generalised transaction ledger. Ethereum Project Yellow Paper 151 (2014)

[42] Baliga, A.: Understanding Blockchain Consensus Models. Technical report. Persis- tent Systems Ltd. (2017)

[43] M. A. Ferrag, M. Derdour, M. Mukherjee, A. Derhab, L. Maglaras, and H. Janicke, ‘‘Blockchain technologies for the Internet of Things: Research issues and challenges,’’ IEEE Internet Things J., vol. 6, no. 2, pp. 2188–2204, Apr. 2019.

[44] C. Decker and R. Wattenhofer, “A fast and scalable payment network with bitcoin duplex micropayment channels,” In Stabilization, Safety, and Security of Distributed Systems pages 3–18. Springer, 2015

[45] Das, Manik Lal, "Privacy and Security Challenges in Internet of Things," Distributed Computing and Internet Technology., pp. 33-48, 2015.