Improving Internet Privacy, Data Protection and Security Concerns

Calvin Chong Kun Lee

CQUniversity Melbourne, Australia, c.c.lee@cqu.edu.au

Gouher Ahmed

Skyline University College, UAE, gouher@usa.net

Abstract

IoT has continued to evolve over the years with a promise to provide the users with effective means to interact, communicate, transact and create strong relationship. The invention and the development of IoT have created benefits for many businesses and individuals. However, as the IoT continues to evolve and develop, it has been subjected to certain threats and vulnerabilities. The common vulnerabilities notable in IoT include the security, privacy and data protection concerns. These issues have not been addressed by many scholars thus necessitated the need for this research study. Therefor the research study was concerned with the developed of a new IoT model that can enhance the security and privacy of the users of the IoT. The results indicate that the new model can be effective in addressing the needs of the IoT users. However, it noted that future research studies are still needed to improve the performance of the IoT security models.

Keywords: Internet of Things, Privacy, Data, Security Concerns, Users, Threats. Cyber.

Introduction

The current global environment is characterized with the rapid growth in the Internet of Things. The Internet of Things (IOT) have changed the way people communicate do business, work, interact, educate, and transact with each other. Although the rapid growth in IoT has been beneficial to many individuals and businesses, it has been subjected to certain challenges that affect its effectiveness in meeting the established goals [1]. Internet of things was initially developed to help connect the globe to an internet platform. Since its introduction, millions of businesses, individuals, and other devices have been connected via IoT [41]. This shows that it has been a major technological innovation that has shaped the global business landscape. Many of the current research studies have exposed that the IoT has many vulnerabilities that has compromised its usage in many areas [42]. Currently, the IoT technology is synonymous among many industries that are making significant attempt to gain a competive edge in the market. A research study by [2] shows that the major threat for the application of IoT is the privacy issue. It is a concern for many of the information technology experts to come up with an appropriate technology to address the issue of the privacy. The other study on IoT vulnerabilities indicated that it is critical to design an appropriate IoT infrastructure that can improve the data protection of individuals [41]. The effectiveness of the IoT relies on its ability to protect the data of users. In particular, the protection of data and information that are personal and confidential to users should be apriority to the software developers. The software developers should ensure that they come up with appropriate design that can enhance the security of the internet users [43].

The popularity of IoT has rapidly increased over the past decades since these technologies are used to serve various purposes such as transportation, communication, business development, and education. According to [43], IoT introduced the concept of hyperconnectivity, which implies the individuals and businesses are able to communicate with each other effortlessly from remote places. IoT was initially invented in 199 for the primary purpose of promoting the concept of Radio Frequency Identification (RFID), which included the embedded actuators and sensors. However, the original concept of the IoT was introduced during 1960s and was initially referred to as the embedded Internet or pervasive computing [44]. The IoT concept was introduced to enhance the supply chain processes and activities. However, the growth in diverse functionality and applications of IoT has helped achieve the strong popularity in 2010. As the concept of IoT continues to expand and gain popularity globally, many countries accepted its implementation as a means to achieve a competitive edge in the market. As an example, the government of China gave the strategic priority on the development of IoT and introduced a five-year expansion plan. The massive explosion of IoT started in 2011 with the introduction of devices that include the smart-energy meters, wearable devices and home automation [45]. This rapid development of IoT has benefitted many organizations across different industries in various ways. In addition, it has helped improve and support the business strategies and market research. Similarly, IoT has helped enhance the individual’s lifestyles through the introduction of automated services. However, the uncontrolled expansion of the IoT has comprised its privacy and security [43].

Various activities such as failure to change passwords, unconscious us, and lack of device updates has typical increased the risks of cybersecurity and accessibility to malicious application in the IoT system's data. Such threats and intrusion in the IoT data system increases the likelihood of data breach and other security vulnerabilities. Majority of the security professionals argues that IoT is the vulnerable platform for cyberattacks because of the weak security policies and protocols [46]. Although several mechanisms have been implemented to protect the IoT system and devices from attacks, there is inappropriate documentation of the security guidelines. As a result, the end users might not be in a position to use the protected measures to counter the data attack. In essence, hackers have developed various types of malware to attack the IoT applications from 2008 [7]. In particular, they have designed the phishing techniques, which they use to provoke individuals or employees to share and reveal sensitive data and information. Thus, the personal devices and corporate workstations frequently face privacy and confidentiality violation due to the high profile risks [40]. If the manufacturers of the devices and security experts assess the cyber threats accurately, they can design and develop an efficient and effective protective system and mechanism to neutralize or prevent the cyber threats [43].

Theoretical Framework

The research is based on the theoretical framework that focuses on general framework architecture. The general framework architecture is designed to help in monitoring and surveillance of activities to address the issue of trust among the parties transacting via blockchain. The general framework was developed by [8] to reduce the threats and vulnerabilities regarding the internet of things. The research paper will meet most of the requirements of IoT systems and block technology by design appropriate architecture that combines the IoT and the block chain [47]. The main layers of the system architecture include devices, data, applications, security, integrity, IoT, SQL and program interface bbb. The framework developed for this research study follows the nomenclature of the International Electro-technical Commissions or the System Committee Acted Assisted Learning [9].

Operational Definitions

- IoT is used to refer to the Internet of Things
- Security refers to the threats in IoT

- Privacy refers to the confidentiality of the IoT users
- Data protection is the protection of data for the users of IoT

Industry description

The IoT industry is currently evolving fast to incorporate the changes in technology. Blockchain is emerging as a powerful industry that supports the operation of many firms and businesses across different sectors [10]. The emergence of blockchain as an innovative and disruptive technology has evidently helped revolutionize the information, communication and transactions [39]. Currently, there are several attempts and research studies aimed at integrating blockchain technology with IoT. The research thus considers various models that have been used to align the blockchain technology with the past and recommend the best model that can help improve the accuracy and accountability of the blockchain technology [11].

Literature Review

Several scholars have suggested that there exist various challenges of IoT that include spoofing attack and jamming as well as the unauthorized access, which can compromise the integrity of the user’s data [12]. However, potential solutions that can help users to secure their IoT data can be designed and implemented [37]. The implementation of the various security and threat measures can prove effective in securing the IoT devices and applications. Accordingly, there are various privacy threats and vulnerabilities that have emerged over the past few decades and pose a significant threat in penetrating and attacking IoT devices and applications in organizations and businesses [13]. As a result, the organizations and businesses should deploy appropriate scanning and monitoring tools and techniques to for all their IoT applications and devices that can help in detecting any type of threats related to data privacy and attempt to mitigate the risk associated with breaching [38]. In essence, the traffic analyzers and interceptors help in the identification and investigation of the various cyber threats.

There are various research studies and services that have been conducted to identify the current trends in IoT security and threats [14]. The multiple applications, services and devices present certain attack vectors and challenges to different IoT devices and their applications. The existence of the various simulation tools, availability of several platforms, and presence of modelers to conform to the security protocol can help produce the protocol associated with the novel IoT privacy and security [15]. It is argued that the rapid progress and growth in the research associated with the IoT security and privacy has supported the research on appropriate IoT infrastructure that can protect the privacy and security of the users [16]. The aim is to ensure that the IoT devices and application succeed in serving individuals and businesses across the globe [48].

Although there are enormous benefits of IoT to the users, it is believed that there are several challenges attributed to its usage. The privacy risks and cyber security issues are the main concerns that have been cited by many scholars [17]. The two challenges are posing enormous threats and predicament to the majority of individuals and organizations in their attempt to conduct different activities and obligations. The common high profile cyber-attacks are an indication of the vulnerabilities of the IoT applications and devices [18].

Problem statement & Research Gap & Research Contribution

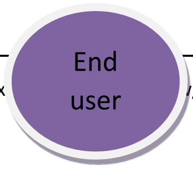
The main problem is to reduce the security vulnerabilities and threats of the IoT devices. It is important that IT professionals to develop appropriate IoT design that can effectively reduce the security vulnerabilities [19]. Currently, the rapid growth on the seucirity vulnerability exposes the firms to various threats that can affect their operation [20]. The contribution of the current research study plays an important role in enhancing the future design of the IoT infrastructure.

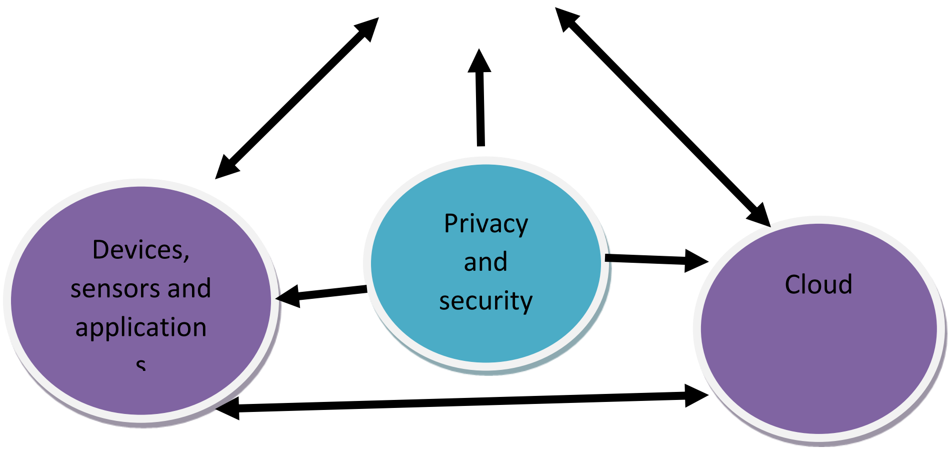
Research MODEL & Hypotheses

The research study emphasized on the two main models to help analyses the privacy and security of the IoT devices and applications [21]. The work proposes the new view of the IoT models that includes the generic and stretched. Both the proposed models have security and privacy components and the layers of separation and identification. The research is completed by building cloud or edge supported IoT application and system to help in the implementation of the proposed IoT models. The research starts by first introducing the generic and stretched models. It then describes the experimental set up as well as the implementation of the environment which primarily consists of the layered model implementation [22]. Lastly, the research presents and discusses the findings and results of the study. The research model is appropriate as it enables the assessment of the various privacy and security issues in the design of the IoT infrastructure.

The generic IoT layered data is the main perceptive of the research study. The generic architecture of the IoT model consists of a group of the wireless connection, cloud, devices, and end user layers [23]. In this model, the device layers include the pool of the internet-enabled sensor devices, communication protocols and data acquisition circuitry [36]. It also has the communication protocols that typically send the data and information to remote or local storage to enable further processing, removal of noise, data massaging, and feature extraction [24]. In addition, the devices allow for the real time collection of data and information using different frequencies of acquisition. The cloud layer typically hosts the data and information collected from the sensor [49]. The figure 1 below shows the generic layered model.

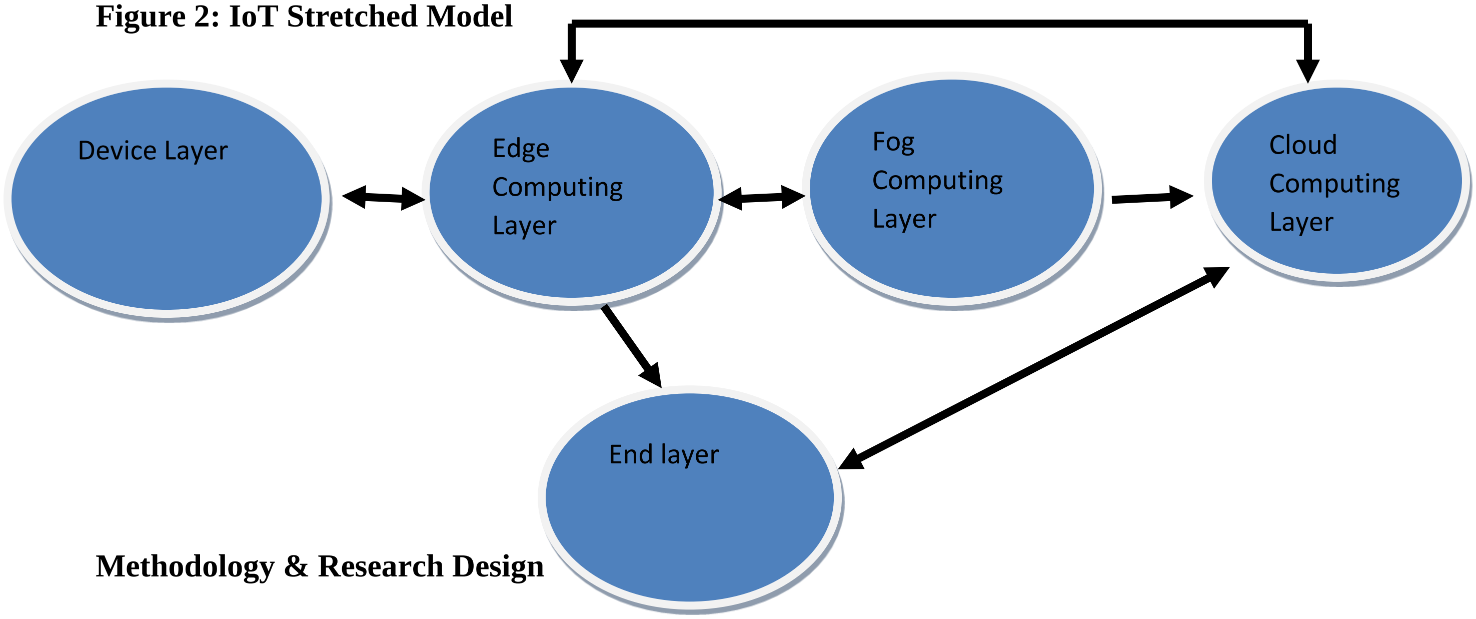
Figure 1: IoT Generic Layered Model





The stretched layered model is another IoT architecture proposed for this research study. The stretched layered model has the additional features to the generic layered model [25]. It is a stretched version of the generic layered model with additional features which include edge, new layers and fog [50]. The three layers can typically overcome and address the latency concerns due to the dependence on the cloud layer services and can make faster decisions [35]. The edge commuting basically occurs to the devices and applications attached to the sensors [26]. They can provide the real-time information, control and decisions to the data sources and also communicate with the other layers in order to transfer the collected data for fusion. It is also note that the fog computing layer moves the edge computing activities to a powerful computing resources connected to the local area network [27]. The added benefits on the model help improve the level of security and privacy issue on the IoT devices and applications.

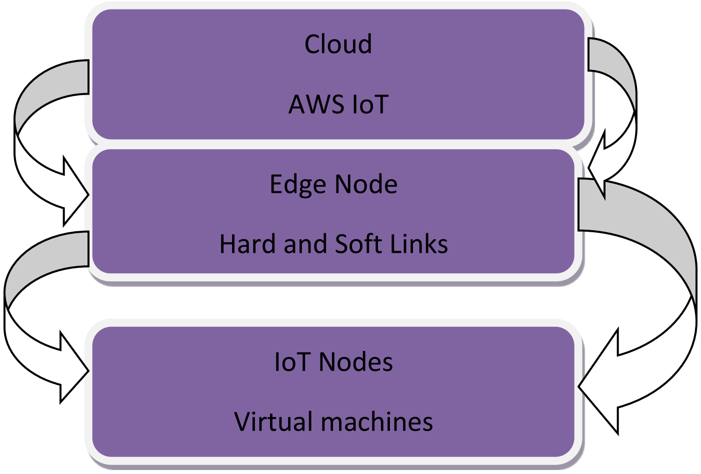
Figure 2: IoT Stretched Model



Methodology & Research Design

The methodology of the research study considered the experimental research design. The experimental research model was considered as an appropriate in improve the current security and privacy issues associated with the previous models. The study developed the proposed models, which was The Layered Cloud-Edge-Iot Model [28]. The aims of the study were to reduce the security of IoT devices and enhance the privacy of the users as well as protect the sensitive data of the users [44]. The new proposed The Layered Cloud-Edge-Iot Model is shown in the diagram 3 below.

Figure 3: The Proposed New Model



The proposed research model considers the identification of the threats and vulnerabilities in the previous models and the new models. It will compare the three aspects that include the security vulnerabilities, data protection and privacy [29]. The comparative research design was considered as an appropriate as it enables the researcher to determine which model can help in the protection of data and information of the users.

Population & Sample & Unit of Analysis

The study primary considered the various application model used by organization when adopting IoT. In the study, the five firms across different sector were considered as the sample for the research. Generally, the study population was huge and considered all the firms that have been using the IoT devices [30]. Although the population was large, selecting a sample of five firms was considered as an appropriate for the study.

The study considered three main unit of analysis that includes the privacy, security and data protection. Each of these elopements was analyzed to determine the vulnerabilities of the IoT device [31]. The main concern of this research study was to determine the appropriate infrastructure for the development of an appropriate IoT system. As a result, the study used the three unit of measurement to determine the percentage of the efficiency of the new model [51].

Analyzing Data

The analysis of data considered the three units of measurement to determine the data security for IoT devices. The main units of analysis are described in the equations below.

Privacy, P=f (x)

Security, S, = f (y)

Data protection D, = f (z)

The overall equation for reduction of security threat is given as follows.

Efficiency = f (x) + f (y) + f (z)

The overall efficiency is found by determining the total percentages of each unit for the measurements for each of the three models considered for analysis.

Discussion of the Results

The research study compared three models to determine their efficiency. The three models that include the IoT generic layered model, IoT stretched Model, and The Layered Cloud-Edge was compared to determine the one with highest percentage of efficiency that can reduce the security vulnerability of the devices [32]. The results are indicated in the table below.

Table 1: Comparison of the Security efficiency of the models

Number	Model	Security Efficiency
1	IoT generic layered model	82 %
2	IoT stretched Model	91 %
3	The Layered Cloud-Edge	94%

The table one above shows the comparison of the security model for the three proposed IoT infrastructure. From the table, it is noted that The Layered Cloud-Edge has the highest percentage (94 %) followed by the IoT stretched Model (91 %) and lastly the IoT generic layered model (82 %). The result indicates that each model has a variation with regards to the efficiency of the security. This is an indication that IoT devices are subjected to some cyber security threats that can compromise their performance. The threats of the cyber security in these models can be explained with ineffective infrastructure that can compromise their performance [33]. It shows that The Layered Cloud-Edge model is the most appropriate that can enhance the security of the users and ensure that their data remains safe and protected from various cyber-attacks and threats.

However, it is noted that there is no model that proves perfect in the protection of the user's data and information.

The comparison was also made on two models included the proposed model of the research study. The research compared the security effectiveness of the proposed model and one of the commonly used models by organizations. The table 2 below show a comparison between the proposed model and the IoT stretched Model.

Table 2: Comparison Between the Proposed Model and the IoT stretched Model

Number	Model	Security Efficiency
1	IoT stretched Model	91 %
1	The proposed Layered Cloud-Edge model	94%

The comparison from the above table indicates that the proposed model has a high percentage of the frequency. It shows that the proposed model has 94 % frequency as compared to the IoT stretched Model. This show that the proposed model can prove appropriate in addressing the needs of the current organizations that depends on the IoT does perform several activities [34]. The findings of this research study indicate that there is a need to continue developing other models to improve the security of the IoT devices.

Conclusion & Recommendations

The research study on the IoT security, threat and data protection provides insightful information on how to improve the data reliability and validity. It shows that there is a need to develop an appropriate infrastructure to enhance the security of the users of IoT devices. From the findings, it is note that the proposed model for the IoT architecture proves powerful in addressing the security vulnerabilities that organizations and businesses face in their daily operations. As a result, it is important to design appropriate information devices that can improve the security of IoT.

Based on the result of the research study, it is recommended that further research be conducted on the security vulnerability and threats. This is because the proposed model is still not 100 % security efficient which means that there is a need for the design of new model. Also, the future research study should focus on increasing the sample size to capture adequate data that can ensure that there is full representation of the population sample.

References

1. Dai, H. N., Zheng, Z., & Zhang, Y. (2019). Blockchain for Internet of Things: A survey. *IEEE Internet of Things Journal*, *6*(5), 8076-8094. DOI: 10.1109/JIOT.2019.2920987
2. Al Shebli, K., Said, R. A., Taleb, N., Ghazal, T. M., Alshurideh, M. T., & Alzoubi, H. M. (2021, June). RTA's Employees' Perceptions Toward the Efficiency of Artificial Intelligence and Big Data Utilization in Providing Smart Services to the Residents of Dubai. In *The International Conference on Artificial Intelligence and Computer Vision* (pp. 573-585). Springer, Cham. DOI: http://scholar.google.ae/citations?user=r3JPWucAAAAJ&hl=en
3. Alrawais, A., Alhothaily, A., Hu, C., & Cheng, X. (2017). Fog computing for the internet of things: Security and privacy issues. *IEEE Internet Computing*, *21*(2), 34-42. DOI: 10.1109/ACCESS.2019.2952472
4. Tseng, L., Wong, L., Otoum, S., Aloqaily, M., & Othman, J. B. (2020). Blockchain for managing heterogeneous internet of things: A perspective architecture. *IEEE network*, *34*(1), 16-23. DOI: 10.1109/MNET.001.1900103
5. Ghazal, T., Soomro, T. R., & Shaalan, K. (2013). Integration of Project Management Maturity (PMM) Based on Capability Maturity Model Integration (CMMI). *European Journal of Scientific Research*, *99*(3), 418-428. DOI: http://scholar.google.ae/citations?user=r3JPWucAAAAJ&hl=en
6. Lee, J. H., & Kim, H. (2017). Security and privacy challenges in the internet of things [security and privacy matters]. *IEEE Consumer Electronics Magazine*, *6*(3), 134-136. IEEE. DOI: 10.1109/CCWC.2019.8666484
7. Svoboda, P., Ghazal, T. M., Afifi, M. A., Kalra, D., Alshurideh, M. T., & Alzoubi, H. M. (2021, June). Information Systems Integration to Enhance Operational Customer Relationship Management in the Pharmaceutical Industry. In *The International Conference on Artificial Intelligence and Computer Vision* (pp. 553-572). Springer, Cham. DOI: http://scholar.google.ae/citations?user=r3JPWucAAAAJ&hl=en
8. Lin, J., Yu, W., Zhang, N., Yang, X., Zhang, H., & Zhao, W. (2017). A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications. *IEEE internet of things journal*, *4*(5), 1125-1142. DOI: https://doi.org/10.3390/s20051389
9. Pal, S., Rabehaja, T., Hill, A., Hitchens, M., & Varadharajan, V. (2019). On the integration of blockchain to the internet of things for enabling access right delegation. *IEEE Internet of Things Journal*, *7*(4), 2630-2639. DOI: 10.1109/JIOT.2019.2952141
10. Al Batayneh, R. M., Taleb, N., Said, R. A., Alshurideh, M. T., Ghazal, T. M., & Alzoubi, H. M. (2021, June). IT Governance Framework and Smart Services Integration for Future Development of Dubai Infrastructure Utilizing AI and Big Data, Its Reflection on the

Citizens Standard of Living. In *The International Conference on Artificial Intelligence and Computer Vision* (pp. 235-247). Springer, Cham. DOI: DOI: http://scholar.google.ae/citations?user=r3JPWucAAAAJ&hl=en

11. Ghazal, T. M., Hasan, M. K., Hassan, R., Islam, S., Abdullah, S. N. H. S., Afifi, M. A., & Kalra, D. (2020). Security vulnerabilities, attacks, threats and the proposed countermeasures for the Internet of Things applications. *Solid State Technology*, *63*(1s), 2513-2521. DOI: http://scholar.google.ae/citations?user=r3JPWucAAAAJ&hl=en
12. Ghazal, T. M., Alshurideh, M. T., & Alzoubi, H. M. (2021, June). Blockchain-Enabled Internet of Things (IoT) Platforms for Pharmaceutical and Biomedical Research. In *The International Conference on Artificial Intelligence and Computer Vision* (pp. 589-600). Springer, Cham. DOI: http://scholar.google.ae/citations?user=r3JPWucAAAAJ&hl=en
13. Yang, Y., Wu, L., Yin, G., Li, L., & Zhao, H. (2017). A survey on security and privacy issues in Internet-of-Things. *IEEE Internet of Things Journal*, *4*(5), 1250-1258. DOI: https://doi.org/10.3390/fi11070161
14. Cao, B., Li, Y., Zhang, L., Zhang, L., Mumtaz, S., Zhou, Z., & Peng, M. (2019). When Internet of Things meets blockchain: Challenges in distributed consensus. *IEEE Network*, *33*(6), 133-139. DOI: 10.1109/MNET.2019.1900002

15. Hiller, J., Pennekamp, J., Dahlmanns, M., Henze, M., Panchenko, A., & Wehrle, K. (2019, October). Tailoring onion routing to the internet of things: Security and privacy in untrusted environments. In *2019 IEEE 27th International Conference on Network Protocols (ICNP)* (pp. 1-12). IEEE. DOI: 10.1109/MILCOM.2017.8170858

16. Naqvi, R., Soomro, T. R., Alzoubi, H. M., Ghazal, T. M., & Alshurideh, M. T. (2021, June). The Nexus Between Big Data and Decision-Making: A Study of Big Data Techniques and Technologies. In *The International Conference on Artificial Intelligence and Computer Vision* (pp. 838-853). Springer, Cham. DOI: http://scholar.google.ae/citations?user=r3JPWucAAAAJ&hl=en

17. Ghazal, T. (2013). *Project Management Maturity Integration based on Capability Maturity Model Integration* (Doctoral dissertation, The British University in Dubai (BUiD)). DOI: http://scholar.google.ae/citations?user=r3JPWucAAAAJ&hl=en

18. Afifi, M. A., Kalra, D., & Ghazal, T. M. (2020). The Role of Training in Determining Citizen-Consumer Attitudes Towards the Use of e-Government. *Journal of Talent Development and Excellence*, *12*(1), 4812-4822. DOI: http://scholar.google.ae/citations?user=r3JPWucAAAAJ&hl=en

19. Ghazal, T. M., Afifi, M. A., & Kalra, D. (2020). Data Mining and Exploration: A Comparison Study among Data Mining Techniques on Iris Data Set. *Journal of Talent Development and Excellence*, *12*(1), 3854-3861. DOI: http://scholar.google.ae/citations?user=r3JPWucAAAAJ&hl=en

20. Liang, X., Zhao, J., Shetty, S., & Li, D. (2017, October). Towards data assurance and resilience in IoT using blockchain. In *MILCOM 2017-2017 IEEE Military Communications Conference (MILCOM)* (pp. 261-266). IEEE. DOI: 10.1109/MILCOM.2017.8170858

21. Cui, L., Yang, S., Chen, F., Ming, Z., Lu, N., & Qin, J. (2018). A survey on application of machine learning for Internet of Things. *International Journal of Machine Learning and Cybernetics*, *9*(8), 1399-1417. DOI: https://doi.org/10.1007/s13042-018-0834-5

22. Samie, F., Bauer, L., & Henkel, J. (2019). From cloud down to things: An overview of machine learning in Internet of Things. *IEEE Internet of Things Journal*, *6*(3), 4921-4934. DOI: 10.1109/JIOT.2019.2893866

23. Mendez, D. M., Papapanagiotou, I., & Yang, B. (2017). Internet of things: Survey on security and privacy. *arXiv preprint arXiv:1707.01879*. DOI: 10.1109/COMST.2018.2803740

24. Alghamdi, T. A., Lasebae, A., & Aiash, M. (2013, November). Security analysis of the constrained application protocol in the Internet of Things. In *Second international conference on future generation communication technologies (FGCT 2013)* (pp. 163-168). IEEE. DOI: 10.1109/FGCT.2013.6767217

25. Patel, P., Pathak, A., Teixeira, T., & Issarny, V. (2011, December). Towards application development for the internet of things. In *Proceedings of the 8th Middleware Doctoral Symposium* (pp. 1-6). DOI: https://doi.org/10.1145/2093190.2093195

26. Shahid, N., & Aneja, S. (2017, February). Internet of Things: Vision, application areas and research challenges. In *2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC)* (pp. 583-587). IEEE. DOI: 10.1109/I-SMAC.2017.8058246

27. Kovatsch, M., Mayer, S., & Ostermaier, B. (2012, July). Moving application logic from the firmware to the cloud: Towards the thin server architecture for the internet of things. In *2012 sixth international conference on innovative mobile and internet services in ubiquitous computing* (pp. 751-756). IEEE.DOI: 10.1109/IMIS.2012.104

28. Safaei, B., Monazzah, A. M. H., Bafroei, M. B., & Ejlali, A. (2017, December). Reliability side-effects in Internet of Things application layer protocols. In *2017 2nd International Conference on System Reliability and Safety (ICSRS)* (pp. 207-212). IEEE. DOI: 10.1109/ICSRS.2017.8272822

29. Popli, S., Jha, R. K., & Jain, S. (2018). A survey on energy efficient narrowband internet of things (NBIoT): architecture, application and challenges. *IEEE Access*, *7*, 16739-16776. DOI: 10.1109/ACCESS.2018.2881533

30. Dabbagh, M., & Rayes, A. (2019). Internet of things security and privacy. In *Internet of Things from hype to reality* (pp. 211-238). Springer, Cham. DOI: https://doi.org/10.1016/j.procs.2018.05.170

31. Andoni, M., Robu, V., Flynn, D., Abram, S., Geach, D., Jenkins, D., ... & Peacock, A. (2019). Blockchain technology in the energy sector: A systematic review of challenges and opportunities. *Renewable and Sustainable Energy Reviews*, *100*, 143-174. DOI: https://doi.org/10.1016/j.rser.2018.10.014

32. Chen, G., Xu, B., Lu, M., & Chen, N. S. (2018). Exploring blockchain technology and its potential applications for education. *Smart Learning Environments*, *5*(1), 1-10. DOI: https://doi.org/10.1186/s40561-017-0050-x

33. Treleaven, P., Brown, R. G., & Yang, D. (2017). Blockchain technology in finance. *Computer*, *50*(9), 14-17. DOI: 10.1109/MC.2017.3571047

34. Saberi, S., Kouhizadeh, M., Sarkis, J., & Shen, L. (2019). Blockchain technology and its relationships to sustainable supply chain management. *International Journal of Production Research*, *57*(7), 2117-2135. DOI: https://doi.org/10.1080/00207543.2018.1533261

35. Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017, June). An overview of blockchain technology: Architecture, consensus, and future trends. In *2017 IEEE international congress on big data (BigData congress)* (pp. 557-564). IEEE. DOI: 10.1109/BigDataCongress.2017.85

36. Min, H. (2019). Blockchain technology for enhancing supply chain resilience. *Business Horizons*, *62*(1), 35-45. DOI: https://doi.org/10.1016/j.bushor.2018.08.012

37. Agbo, C. C., Mahmoud, Q. H., & Eklund, J. M. (2019, June). Blockchain technology in healthcare: a systematic review. In *Healthcare* (Vol. 7, No. 2, p. 56). Multidisciplinary Digital Publishing Institute. DOI: https://doi.org/10.3390/healthcare7020056

38. Cole, R., Stevenson, M., & Aitken, J. (2019). Blockchain technology: implications for operations and supply chain management. *Supply Chain Management: An International Journal*. DOI: https://doi.org/10.1108/SCM-09-2018-0309

39. F. Matloob et al., "Software Defect Prediction using Ensemble Learning: A Systematic Literature Review," in IEEE Access, doi: 10.1109/ACCESS.2021.3095559

40. T. M. Ghazal, M. Anam, M. K. Hasan, M. Hussain, M. S. Farooq et al. (2021). "Hep-pred: hepatitis c staging prediction using fine gaussian svm," Computers, Materials & Continua, vol. 69, no.1, pp. 191–203, 2021.Link: http://scholar.google.ae/citations?user=r3JPWucAAAAJ&hl=en

41. H. Alzoubi, M. Alshurideh, B. Al Kurdi, and M. Inairat, “Do perceived service value, quality, price fairness and service recovery shape customer satisfaction and delight? A practical study in the service telecommunication context,” Uncertain Supply Chain Manag., vol. 8, no. 3, pp. 579–588, 2020, doi: 10.5267/j.uscm.2020.2.005.

42. M. Alshurideh, A. Gasaymeh, G. Ahmed, H. Alzoubi, and B. Al Kurd, “Loyalty program effectiveness: Theoretical reviews and practical proofs,” Uncertain Supply Chain Manag., vol. 8, no. 3, pp. 599–612, 2020, doi: 10.5267/j.uscm.2020.2.003.

43. H. M. Alzoubi and R. Yanamandra, “Investigating the mediating role of information sharing strategy on agile supply chain,” Uncertain Supply Chain Manag., vol. 8, no. 2, pp. 273–284, 2020, doi: 10.5267/j.uscm.2019.12.004.

44. B. Al Kurdi, H. Elrehail, and H. M. Alzoubi, “THE INTERPLAY AMONG HRM PRACTICES , JOB SATISFACTION AND INTENTION TO LEAVE : AN EMPIRICAL INVESTIGATION,” no. August, 2021.

45. H. M. Alzoubi, G. Ahmed, A. Al-Gasaymeh, and B. Al Kurdi, “Empirical study on sustainable supply chain strategies and its impact on competitive priorities: The mediating role of supply chain collaboration,” Manag. Sci. Lett., vol. 10, no. 3, pp. 703–708, 2020, doi: 10.5267/j.msl.2019.9.008.

46. H. Alzoubi and G. Ahmed, “Do TQM practices improve organisational success? A case study of electronics industry in the UAE,” Int. J. Econ. Bus. Res., vol. 17, no. 4, pp. 459–472, 2019, doi: 10.1504/IJEBR.2019.099975.

47. H. M. Alzoubi and R. Aziz, “Does emotional intelligence contribute to quality of strategic decisions? The mediating role of open innovation,” J. Open Innov. Technol. Mark. Complex., vol. 7, no. 2, 2021, doi: 10.3390/joitmc7020130.

48. M. Alnuami, H. Alzoubi, D. Ajelat, and A. Alzoubi, “Toward Intelligent Organizations:An Empirical investigation of Learning Orientation’s role in Technical Innovation,” Int. J. Innov. Learn., vol. 29, no. 2, pp. 207–221, 2021, [Online]. Available: https://www.inderscienceonline.com/doi/abs/10.1504/IJIL.2021.112996.

49. S. Joghee, H. M. Alzoubi, and A. R. Dubey, “Decisions effectiveness of FDI investment biases at real estate industry: Empirical evidence from Dubai smart city projects,” Int. J. Sci. Technol. Res., vol. 9, no. 3, pp. 3499–3503, 2020.

50. A. Q. M. Alhamad, I. Akour, M. Alshurideh, A. Q. Al-Hamad, B. Al Kurdi, and H. Alzoubi, “Predicting the intention to use google glass: A comparative approach using machine learning models and PLS-SEM,” Int. J. Data Netw. Sci., vol. 5, no. 3, pp. 311–320, 2021, doi: 10.5267/j.ijdns.2021.6.002.

51. T. M. Ghazal et al., “IoT for Smart Cities: Machine Learning Approaches in Smart Healthcare—A Review,” Futur. Internet, vol. 13, no. 8, p. 218, 2021, doi: 10.3390/fi13080218.

52. S. Hamadneh, O. Pederson, M. Alshurideh, B. Al Kurdi, and H. Alzoubi, “AN INVESTIGATION OF THE ROLE OF SUPPLY CHAIN VISIBILITY INTO THE AN INVESTIGATION OF THE ROLE OF SUPPLY CHAIN VISIBILITY INTO THE SCOTTISH BLOOD,” no. September, 2021.

53. M. A. Alnuaimi, H. M. Alzoubi, and N. N. Alnazer, “Analysing the appropriate cognitive styles and its effect on strategic innovation in Jordanian universities,” Int. J. Bus. Excell., vol. 13, no. 1, p. 127, 2017, doi: 10.1504/ijbex.2017.10006235.

54. Ghazal, T. M., Noreen, S., Said, R. A., Khan, M. A., Siddiqui, S. Y. et al. (2022). Energy Demand Forecasting Using Fused Machine Learning Approaches. Intelligent Automation & Soft Computing, 31(1), 539–553.

55. Ghazal, T.M. Internet of Things with Artificial Intelligence for Health Care Security. Arab J Sci Eng (2021). https://doi.org/10.1007/s13369-021-06083-8

56. Aslam, M. S., Ghazal, T. M., Fatima, A., Said, R. A., Abbas, S. et al. (2021). Energy-Efficiency Model for Residential Buildings Using Supervised Machine Learning Algorithm. Intelligent Automation & Soft Computing, 30(3), 881–888.

57. Ghazal, T. M., Hussain, M. Z., Said, R. A., Nadeem, A., Hasan, M. K. et al. (2021). Performances of K-Means Clustering Algorithm with Different Distance Metrics. Intelligent Automation & Soft Computing, 30(2), 735–742.

58. Khan, Q., Ghazal, T. M., Abbas, S., Khan, W. A., Khan, M. A. et al. (2021). Modeling Habit Patterns Using Conditional Reflexes in Agency. Intelligent Automation & Soft Computing, 30(2), 539–552.

59. Rehman, E., Khan, M. A., Soomro, T. R., Taleb, N., Afifi, M. A., & Ghazal, T. M. (2021). Using Blockchain to Ensure Trust between Donor Agencies and NGOs in Under-Developed Countries. Computers, 10(8), 98. doi:10.3390/computers10080098

60. Ghazal, T.M. Positioning of UAV Base Stations Using 5G and Beyond Networks for IoMT Applications. Arab J Sci Eng (2021). https://doi.org/10.1007/s13369-021-05985-x

61. Ghazal, T.M., Said, R.A. & Taleb, N. Internet of vehicles and autonomous systems with AI for medical things. Soft Comput (2021). https://doi.org/10.1007/s00500-021-06035-2

62. Matloob, Faseeha & Ghazal, Taher & Taleb, Nasser & Aftab, Shabib & Ahmad, Munir & Khan, Muhammad & Abbas, Sagheer & Soomro, Tariq. (2021). Software Defect Prediction Using Ensemble Learning: A Systematic Literature Review. IEEE Access. 9. 98754-98771. 10.1109/ACCESS.2021.3095559.

63. T. M. Ghazal, M. Anam, M. K. Hasan, M. Hussain, M. S. Farooq et al., "Hep-pred: hepatitis c staging prediction using fine gaussian svm," Computers, Materials & Continua, vol. 69, no.1, pp. 191–203, 2021.

64. Ghazal, T. M., Kalra, D., & Afifi, M. A. (2021). The Impact of Deploying the Internet of Things and How Will It Change Our Lives. Solid State Technology, 64(2).

65. Taher M. Ghazal, Mohammed Kamrul Hasan, Rosilah Hasan, Shayla Islam, Siti Norul Huda Sheikh Abdullah, Mohammed A.M. Afifi, & Deepak Karla. (2020). Security Vulnerabilities, Attachs, Threats and the Proposed Countermeasures for the Internet of Things Applications Solid State Technology, 63(1), 1566-1574.