Convergence Between Blockchain and The Internet of Things

Alma Emerita

Far Eastern University Roosevelt, Philippines, avdelacruz@feu.edu.ph

Abstract

The objective of this study was to determine the effectiveness of a particular convergence model for IoT and blockchain. Multiple regression model was selected to determine the effective of a specific convergence model. Three convergence models were selected for this study, including the hybrid approach, the IoT-blockchain approach, and the IoT-IoT approach. The findings indicated that there are issues with convergence between two different technologies. The other finding was that the hybrid model provided the best convergence platform for integrating IoT with blockchain. Regarding the IoT and blockchain, convergence challenges included the limited capacity of IoT devices to handle the nature of distributed ledgers. The recommendation is that the aspects of traditional blockchain should be redesigned because of new requirements of IoT, including smart contracts, consensus protocol, data privacy, and security.

Keywords: Internet of Things, Blockchain, Privacy, Data.

Introduction

As a concept, the Internet of Things (IoT) is exciting and fascinating. One of the challenging features of IoT, however, is possessing a secure ecosystem that covers all the building blocks in the IoT design [1]. Blockchain denotes the database holding a seamless and growing dataset. Generally, blockchain has a distributive nature, indicating that there is no single or master PC controlling the entire chain. Instead, the involved nodes feature a copy of the entire chain.

Understanding the diverse building blocks of blockchains and IoT can determine the vulnerability areas in each unit [2]. Accordingly, exploring the different technologies required to address each of the emerging weaknesses are crucial to tackling the convergence issues between IoT and blockchain technologies [45].

In a typical architecture of IoT, the blockchain functions to maintain an immutable data record of the entire history of device operations. The benefit of this feature is that it allows the independent functioning of the devices within the system without the demand for any centralized authority [2]. Consequently, the blockchain provides an avenue to a sequence of IoT contexts that were previously complex or impossible to deploy [46].

Despite the ever-increasing agreement on the likelihood of IoT and blockchain convergence, the principal issue is the actual place in which the blockchain will be housed [3]. The direct hosting of blockchain on resource-deficient IoT systems and devices is not appropriate because of limited bandwidth, limited computational infrastructure, and the need for power preservation [47]. Concerning latency and computational resources, the fog and cloud are among the two suggested service platforms for hosting blockchain [3]. Founded on the challenges, characteristics, and constraints of IoT device, the wide range of architectures suggested for IoT and Blockchain combination include the hybrid approach, IoT-blockchain, and IoT-IoT.

The architectural elements of blockchain and IoT convergence control myriad elements in determining the effectiveness of transaction control. Aspects such as Hyperledger Fabric-based blockchain designs, hybrid models, and IoT-blockchain models have enabled users to establish communication channels, view transaction history, and manage assets [3]. The benefit of integrating blockchains to IoT systems is that the transaction occurring via blockchain are secure because they are routed between diverse peers within the model. Each IoT device, in this regard,

initiates a transaction by getting a registration certificate from the certification authority (CA) of the fabric. These considerations are important they function to enhance the overall effectiveness of the integrated system [48].

Theoretical Framework

The current study is founded on the principle that the blockchain technology is one of the main missing links that can settle the reliability and privacy issues of the IoT. Conceptually, blockchain could act the silver bullet required by the whole IoT sector. Blockchain can be adopted to track innumerable connected devices, allowing the ease of processing and coordinating transactions between the devices [4]. Several studies have addressed the issues associated with the effective framework for the integration of IoT with blockchain to limit the emerging vulnerabilities in their operations. Accordingly, this study is focused on identifying the best convergence structure to integrate IoT with blockchain [49].

Operational Definitions

IoT – Internet of Things

Blockchain – a distributed set of records comprised of a chain of blocks that has three fundamental aspects: decentralized, transparent, and recorded.

CA – certification authority

Industry Description

Based on its decentralized nature, along with its multi-phased procedures, blockchain provides a useful approach that can address several challenges facing IoT. Research highlight that

until a few recently, blockchain was only understood and applied in the context of online transactions and payments, including Ethereum and Bitcoin [5]. Over the past years, however, multiple non-financial contexts have incorporated or considered the deployment of blockchain technology, including digital identities and supply chain management [6]. As a result, there is the need to identify an appropriate convergence model to link IoT with blockchain [49].

Literature Review

The struggle to use an effective convergence platform for IoT and blockchain technologies has never been more urgent than the current issues of urbanization and efficiency of transactions. For example the shift towards constructing smart transportation systems and cities has increased daily [6]. Intelligent transportation systems (ITS) can improve user experience and offer intelligence to understand road safety level, efficiency, security, decentralization, and autonomy [50]. However, the lack of convergence between IoT and blockchain means that ITSs are currently facing countless challenges linked with trustful communication, centralization, and integrity [7]. One of the main areas that the use of effective convergence between IoT and blockchain can encompass the work of [8] to stage the prediction of Hepatitis C via the Fine Gaussian SVM technique. Issues addressed in the study performed by [8] have always involved the contribution of the Center for Cyber Security, CCSIS, and Departments of Computer Science from various universities, including Lahore Garrison University, School of Systems and Technology, Government College University, Skyline University College, and numerous other universities across the developing and developed economies [42].

Because of the diversity of alternatives guiding blockchain convergence with IoT, along with various kinds of IoT applications and devices, designers of IoT should choose a suitable

option based on their requirements and restrictions [9, 10]. Despite the availability of research options, however, there is the lack of comprehensive resolutions and analyses for IoT developers and vendors to implement an appropriate blockchain platform to guide the integration requirements [11].

Several shreds of literature have supported the implementation of a decentralized architecture to enhance convergence between IoT and blockchain [12, 13]. A decentralized framework can lessen the overall charges of the IoT system compared to centralized models [14]. Nonetheless, the decentralized nature of blockchain means that it is affected by a new form of resource wastage, which introduces new challenges to its convergence with IoT [15, 26, 17]. The requirements of materials, equipment, or resources rely on the specificity of the consensus protocol in a particular blockchain network. Primarily, alternatives often assign these roles to gateways and autonomous devices that can offer this functionality [18].

Numerous other challenges have also affected the integration requirements of blockchain and IoT [19]. Regarding scalability issues, the size of blockchain has increased with the growing number of connected devices [20]. This is one of the key blockades to the integration needs because IoT networks serving these devices are required to contain a large set of nodes that can produce massive data amounts in real-time [23]. Furthermore, some current implementations of the blockchain can only handle or process a limited number of transactions per second [43]. Generally, this is a potential challenge for IoT performance [24]. Tackling scalability issues of blockchain has involved suggestions such as storage optimization by removing or deleting old transaction records [24, 26].

Problem Statement, Research Gap, and Research Contribution

The Internet of Things (IoT) has emerged an integral part of people's daily lives because of its ability to enhance the monitoring and control of objects and processes that revolutionize the manner in which people interact [27,28]. Concerning the requirement for ensuring that all the aspects of IoT are full and effectively functional, there is the need to address the numerous obstacles that have developed overtime [29]. Major issues have included, among others, scalability, consumption, data privacy, and cybersecurity [52].

Research Model and Hypothesis

Similar to other studies performed on the integration and convergence between blockchain and IoT, the research model employed in this study is the analytical model [30]. The selected model considers the existing architectures that have been used to connect blockchain to IoT [31]. The adopted analysis involves elements such as the efficiency, trust level, accuracy, scalability, and legitimacy of the blockchain and IoT architecture [32, 33]. The principle purpose of analyzing the existing architecture is to understand the opportunities and challenges that can influence the effective convergence and performance of these two technologies [53].

Methodology and Research Design

The multiple regression approach was chosen for the current study. The rationale for selecting linear regression was founded on the fact that almost all the existing shreds of research on the integration of block chain and IoT have relied on exploratory studies [54]. The benefit of linear regression approach is that it strives to model the connection between different variables by fitting the observed to a linear equation. The multiple regression will rely on data collected from a group of companies that have integrated IoT with blockchain and their performance based on the

chosen convergence method, including the hybrid approach, IoT-blockchain architecture, and IoT-IoT model [55].

About the appropriate sampling approach and research design, purposive sampling was utilized to understand the best timeframe and data on the possible implications of the independent variables (type of convergence model) on the dependent variable [56]. Similarly known as subjective sampling, the selected sampling technique (purposive sampling) relies on the decisions or observations of the researcher concerning the selection of data features [34].

Population, Sample, and Unit of Analysis

The sample collected for this study was the performance of 10 firms that have integrated blockchain with IoT to improve performance. Three convergence models were considered for this study: hybrid approach, IoT-blockchain, and IoT-IoT. Generally, the data involved gathering the level of positive ratings of the companies between 2009 and 2020 from the appropriate social media sites. The final data for analysis entailed constraints such as the level of positive customer reviews concerning functionality of the company, company profit margin, and the apparent brand image (Table 1). The dependent variable was the positive customer rating, with the independent variables being the type of convergence models available for use by organizations desiring to integrate IoT with blockchain.

Analyzing Data

The collected data comprised of elements, including decentralization, immutability, access and identity management, resiliency, reliability, security, autonomy, anonymity, and cost-saving for the three suggested convergence models. Table 1 illustrates the dataset utilized in this study.

Table 1: Dataset showing the independent and dependent variables

Year	Average Positive Customer Response	IoT-IoT Model	IoT-blockchain model	Hybrid model
2020	1.5	561	3178	3750
2019	1.3	5578	5203	2792
2018	1.35	3011	4486	2834
2017	1.37	3301	7136	7975
2016	1.13	2014	6094	8119
2015	1.28	4484	4652	7078
2014	1.20	2971	4799	7781
2013	1.26	3788	8653	2452
2012	1.12	1302	1965	3278
2011	1.21	950	3549	4510
2010	1.1	3239	8128	1378
2009	1.07	4832	1452	4844

SUMMARY OUTPUT								
Regression Statistics								
Multiple R	0.89132177							
R Square	0.79445449							
Adjusted R Square	0.6376666							
Standard Error	2802.88436							
Observations	12							
ANOVA								
	df	*SS*	*MS*	*F*	*Significance F*			
Regression	3	273283812.4	91094604	11.59531	0.002773			
Residual	9	70705446.6	7856161					
Total	12	343989259						
	Coefficients	*Standard Error*	*t Stat*	*P-value*	*Lower 95%*	*Upper 95%*	*Lower 95.0%*	*Upper 95.0%*
Intercept	0	#N/A	#N/A	#N/A	#N/A	#N/A	#N/A	#N/A
IoT-IoT model	3485.40929	1772.758677	1.966093	0.080848	-524.849	7495.668	-524.849	7495.668
Iot-blockchain model	0.1197548	0.535532849	0.223618	0.828048	-1.0917	1.331214	-1.0917	1.331214
Hybridmodel	-0.00973166	0.388838106	-0.02503	0.980579	-0.88934	0.869881	-0.88934	0.869881

Figure 1: Multiple regression analysis output

The results of the multiple regression analysis shows interesting trends concerning the connection between the effectiveness of the specific convergence models. Based on the positive ratings of customers over the highlighted period, the results are described comprehensively as described in the next sections. Firstly, the adopted regression model depended on three independent variables denotes as n. the series of the variables or constraints selected is presented in Equation 1, which also highlights the whole regression equation based on the three variables.

$$\mu_y=\beta_0+_1x_1+ \beta_2x_2+ \beta_3x_3\ldots.+ \beta_nx_n \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\text{Equation } 1$$

Equation 1 demonstrates that the response of positive customer rating of a company (dependent variable), represented by the mean of the left-hand side (μ_y), shifts with the change in the value of the predictor variables (IoT-IoT architecture, IoT-blockchain model, and Hybrid model). According to the equation above, the result of the predicted variable y will differ as per

the mean of the independent variables [35]. The analysis assumed that the predicted variable will have a similar standard deviation as the predictor variable.

The study findings indicate that the intercept or slope of the regression model is 0. This finding highlight that the expected mean of y (dependent variable) is 0, especially when all the predictor variables have a mean of 0. Secondly, R-squared (the coefficient of determination) is approximately 0.79. R-squared defines the variance percentage in the predicted variable that the independent variable can affect. Regarding the findings above, 79% of the variance of positive customer ratings (dependent variable) is influenced by the predictor variables. Thirdly, the estimate of the standard error is approximately 2802.90. The value of the standard error highlight the projected standard deviation of the sample. Precisely, the standard error of estimate outlines the ambiguity associated with the estimate. Finally, at the 95% confidence interval, the t-statistic for the IoT-IoT architecture, IoT-blockchain model, and Hybrid model were 1.97, 0.22, and -0.03, respectively.

Discussion of Results

The findings or results indicate the connections between the effectiveness and ineffectiveness, thereof, of convergence models in ensuring security, trust, and seamless communication between IoT devices. Different models of convergence highlighted performance regarding anonymity, autonomy, reliability, security, and cost-saving issues when blockchain and IoT are integrated. From the outcomes of the multiple regression, the equation offers some insights into the association between the study variables. According to the research hypothesis, positive customer rating of a company on the social media sites relates positively with the type of a convergence approach. The p-values of the independent variables are 0.98, 0.83, and 0.08. In

particular, the p-values of the predictor variables exceed 0.05, the alpha value. This implies that the null hypothesis should be accepts that the type of convergence relates to a positive and strong company performance, which echoes positive customer ratings.

Commensurate with the dataset and selected analysis technique, the value of Adjusted R of about 64% highlights that the independent variables control consumer intentions to rate a company positively based on the strategic approach to integrating blockchain with IoT. However, the considerably extreme value of SEE insinuate that there is the need to use a larger sample of data [41]. Founded on the outlined regression output, the aspects connected to the selected convergence framework have significant effects on the type of rating assigned by customers to a company [36].

As supported by the analyzed data and information from the companies and customers, the hybrid approach only deals with specific aspects of the integration that the blockchain can handle [17, 18]. In the hybrid approach, only some sections of the interactions occur in the blockchain, with the other parts taking place directly between the involved IoT devices [37]. It appropriate to contend that one of the challenges of the hybrid approach is selecting the type of interaction that should occur via the blockchain while offering a means to decide in the run-time [38]. The hybrid model is an excellent way to balance the benefits of both actual IoT interactions and blockchain [38].

The other two models, IoT-IoT and IoT-blockchain also have their benefits and drawbacks [38]. The IoT-blockchain design, for example, involves the entire interactions as well as associated data to occur via the blockchain, including gathering traceable and immutable interaction records 39]. This design is specifically important for renting and trading scenarios because of its security

and reliability [40]. The main drawback of the approach, however, is that recording and storing all forms of interactions often increase data resource and bandwidth consumption.

The final model (IoT-IoT) that affects its ineffectiveness as a convergence alternative is its reliance on the routing and discovery mechanism [40] As a result, only some section of data transferred between IoT is stored inside a blockchain while the interactions occurring in the IoT happen without the blockchain. The method, however, is useful in contexts in which the IoT interactions are reliable are have low latency.

Conclusions and Recommendations

With the sporadic increase in the number of devices connected to the Internet of Things (IoT), innumerable hindrances have developed that can potentially slow down the implementation of the IoT across diverse sectors. Firstly, the IoT platforms and devices' market is greatly differentiated, with many vendors and standards. Secondly, concerns have developed concerning interoperability because of the implemented solutions tend to generate new data records. Data created and stored by an IoT device is secure in the cloud platform, but these data cannot be safeguarded when the source is tampered or the integrity device is compromised. Specifically, the centralized design of several IoT alternatives means that the device owner should trust the vendor or manufacturer to ensure the security of their data, especially if hackers compromise the central server. Blockchain, on the other hand, can address the resiliency issues of the IoT as an emerging technology.

Blockchain offers a distributed ledger that helps users to avoid centralized design issues. Additionally, it stores transaction information securely through its unique features. As a new system, blockchain establishes trust between all the devices within an IoT system, which helps in

reduction of treats associated with tampering the cryptography of blockchain. Additionally, blockchain has in reducing the expenses of management and overhead IoT because it eliminates intermediaries and middlemen. Subsequently, it is appropriate to contend that blockchain can offer a promising alternative that addresses several of the emerging IoT challenges. However, any convergence or integration between two different technologies have often created new obstacles and issues. For example, IoT devices possess limited storage devices and power that can handle the distributed ledgers, which are often resource intensive. Other issues have included the limited ability to perform node encryption, consensus execution of protocol, and full copy storage.

References

1. Abbas, K., Tawalbeh, L. A. A., Rafiq, A., Muthanna, A., Elgendy, I. A., El-Latif, A., & Ahmed, A. (2021). Convergence of Blockchain and IoT for Secure Transportation Systems in Smart Cities. *Security and Communication Networks, 2021*. https://doi.org/10.1155/2021/5597679
2. Singh, S., Sharma, P. K., Yoon, B., Shojafar, M., Cho, G. H., & Ra, I. H. (2020). Convergence of blockchain and artificial intelligence in IoT network for the sustainable smart city. *Sustainable Cities and Society*, *63*, 102364. https://doi.org/10.1016/j.scs.2020.102364
3. Maroufi, M., Abdolee, R., & Tazekand, B. M. (2019). On the convergence of blockchain and internet of things (iot) technologies. *arXiv preprint arXiv:1904.01936*.
4. Rabah, K. (2018). Convergence of AI, IoT, big data and blockchain: a review. *The lake institute Journal*, *1*(1), 1-18.
5. Tukur, Y. M., Thakker, D., & Awan, I. U. (2020). Edge-based blockchain enabled anomaly detection for insider attack prevention in Internet of Things. *Transactions on Emerging Telecommunications Technologies*, e4158.
6. Gromovs, G., & Lammi, K. (2017). Blockchain and internet of things require innovative approach to logistics education. *Transport Problems*, *12*.
7. Sandner, P., Gross, J., & Richter, R. (2020). Convergence of Blockchain, IoT, and AI. *Frontiers Blockchain*, *3*, 522600.
8. 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. http://scholar.google.ae/citations?user=r3JPWucAAAAJ&hl=en

9. Chanson, M., Bogner, A., Bilgeri, D., Fleisch, E., & Wortmann, F. (2019). Privacy-preserving data certification in the Internet of things: Leveraging blockchain technology to protect sensor data. *Journal of the Association for Information Systems*, *20*(9).
10. Wu, Y., Dai, H. N., & Wang, H. (2020). Convergence of blockchain and edge computing for secure and scalable IIoT critical infrastructures in industry 4.0. *IEEE Internet of Things Journal*, *8*(4), 2300-2317.
11. Malviya, H. (2016). How blockchain will defend IoT. *Available at SSRN 2883711*.
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. http://scholar.google.ae/citations?user=r3JPWucAAAAJ&hl=en
13. Banafa, A. (2017). IoT and blockchain convergence: benefits and challenges. *IEEE Internet of Things*.
14. Reyana, A., Ramya, S. R., Krishnaprasath, T., & Sivaprakash, P. (2021). Blockchain for Internet of Things I. In *Blockchain, Internet of Things, and Artificial Intelligence* (pp. 65-83). Chapman and Hall/CRC.
15. Azbeg, K., Ouchetto, O., Andaloussi, S. J., & Fetjah, L. (2021). A Taxonomic Review of the Use of IoT and Blockchain in Healthcare Applications. *IRBM*.
16. Tariq, U., Ibrahim, A., Ahmad, T., Bouteraa, Y., & Elmogy, A. (2019). Blockchain in internet-of-things: a necessity framework for security, reliability, transparency, immutability and liability. *IET Communications*, *13*(19), 3187-3192.

17. Plonsky, L. and Ghanbar, H. (2018). Multiple regression in L2 research: A methodological synthesis and guide to interpreting R2 values. *The Modern Language Journal*, *102*(4), pp.713-731.
18. Sharma, P. (2021). Internet of Things and Blockchain. *Blockchain for Business: How It Works and Creates Value*, 296-336.
19. Ekramifard, A., Amintoosi, H., Seno, A. H., Dehghantanha, A., & Parizi, R. M. (2020). A Systematic Literature Review of Integration of Blockchain and Artificial Intelligence.
20. Hathaliya, J., Sharma, P., Tanwar, S., & Gupta, R. (2019, December). Blockchain-based remote patient monitoring in healthcare 4.0. In *2019 IEEE 9th International Conference on Advanced Computing (IACC)* (pp. 87-91). IEEE.
21. Torky, M., & Hassanein, A. E. (2020). Integrating blockchain and the internet of things in precision agriculture: Analysis, opportunities, and challenges. *Computers and Electronics in Agriculture*, 105476.
22. Kumar, R., Wang, W., Kumar, J., Yang, T., Khan, A., Ali, W., & Ali, I. (2021). An Integration of Blockchain and AI for Secure Data Sharing and Detection of CT images for the Hospitals. *Computerized Medical Imaging and Graphics*, *87*, 101812.
23. Reyna, A., Martín, C., Chen, J., Soler, E., & Díaz, M. (2018). On blockchain and its integration with IoT. Challenges and opportunities. *Future generation computer systems*, *88*, 173-190.
24. Ghazal, T. M., Anam, M., Hasan, M. K., Hussain, M., Farooq, M. S., Ali, H. M. A., ... & Soomro, T. R. Hep-Pred: Hepatitis C Staging Prediction Using Fine Gaussian SVM.
25. Wei, L., Wu, J., Long, C., & Lin, Y. B. (2019). The convergence of ioe and blockchain: Security challenges. *IT Professional*, *21*(5), 26-32.

26. F. Matloob et al., "Software Defect Prediction Using Ensemble Learning: A Systematic Literature Review," in IEEE Access, vol. 9, pp. 98754-98771, 2021, doi: 10.1109/ACCESS.2021.3095559.
27. 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.
28. Dai, H. N., Zheng, Z., & Zhang, Y. (2019). Blockchain for Internet of Things: A survey. *IEEE Internet of Things Journal*, *6*(5), 8076-8094.
29. 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. 13. http://scholar.google.ae/citations?user=r3JPWucAAAAJ&hl=en
30. Singh, S. K., Rathore, S., & Park, J. H. (2020). Blockiotintelligence: A blockchain-enabled intelligent IoT architecture with artificial intelligence. *Future Generation Computer Systems*, *110*, 721-743.
31. Atlam, H. F., Alenezi, A., Alassafi, M. O., & Wills, G. (2018). Blockchain with internet of things: Benefits, challenges, and future directions. *International Journal of Intelligent Systems and Applications*, *10*(6), 40-48. doi:10.5815/ijisa.2018.06.05
32. Pundir, A. K., Jagannath, J. D., Chakraborty, M., & Ganpathy, L. (2019, January). Technology integration for improved performance: A case study in digitization of supply chain with integration of internet of things and blockchain technology. In *2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC)* (pp. 0170-0176). IEEE. 10.1109/CCWC.2019.8666484

33. Zhao, S., Li, S., & Yao, Y. (2019). Blockchain enabled industrial Internet of Things technology. *IEEE Transactions on Computational Social Systems*, *6*(6), 1442-1453. 10.1109/TCSS.2019.2924054

34. Memon, R. A., Li, J. P., Nazeer, M. I., Khan, A. N., & Ahmed, J. (2019). DualFog-IoT: Additional fog layer for solving blockchain integration problem in Internet of Things. *IEEE Access*, *7*, 169073-169093. 10.1109/ACCESS.2019.2952472

35. Satamraju, K. P. (2020). Proof of concept of scalable integration of internet of things and blockchain in healthcare. *Sensors*, *20*(5), 1389. **https://doi.org/10.3390/s20051389**

36. 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. 10.1109/JIOT.2019.2952141

37. Rejeb, A., Keogh, J. G., & Treiblmaier, H. (2019). Leveraging the internet of things and blockchain technology in supply chain management. *Future Internet*, *11*(7), 161. **https://doi.org/10.3390/fi11070161**

38. 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. 10.1109/MNET.2019.1900002

39. Etikan, I., Musa, S. A., & Alkassim, R. S. (2016). Comparison of convenience sampling and purposive sampling. *American journal of theoretical and applied statistics*, *5*(1), 1-4.

40. Pieroni, A., Scarpato, N., & Felli, L. (2020). Blockchain and IoT Convergence—A Systematic Survey on Technologies, Protocols and Security. *Applied Sciences*, *10*(19), 6749.

41. 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
42. 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.
43. 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.
44. 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.
45. 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.
46. 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.
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. 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.

49. 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.

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. 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.

52. 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.

53. 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.

54. 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

55. 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.
56. 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.
57. 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.
58. 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
59. 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
60. 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
61. 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.
62. 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.

63. 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).
64. 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.