Assessment of Smart Home Assistants as an IoT

Ahmed J. Obaid

Dept. of Computer Science Faculty of Computer Science and Mathematics, University of Kufa, Iraq,
ahmedj.aljanaby@uokufa.edu.iq

Abstract

A smart home personal assistant technology is an intrinsic system, which incorporates many elements such as users, Smart Home Personal Assistants (SPA) devices, cloud, skill provider and other responsive devices. Even though Smart Home Personal Assistants give a robust security and privacy options, the devices face many weaknesses, which make the system vulnerable and can be comprised by adversaries, who can capitalize on limitations to gain access to delicate information and privacy of users. In this research, the aim is to assess how invention and innovation of security and SPA can be harnessed by users to interrelate with the system. Subsequently, this write-up will address both the problems related to the system and attempt to bring in solutions, which makes the technology more adaptable and versatile to all users. Initial studies show that some of the weakness underlying the technology include the open-nature of the voice channel, complexity of the architecture, software implications, and the utility of the technology to less proficient users. As a result, the study anticipates at solving the voice squatting attack, using the SPA intelligent assistant, incorporating a filer to filter the ultrasonic attack and noise as well as trying to assess the efficacy of the elements developed against the voice squatting attacks. The study found out that there is a need to mitigate the attacks on the blockchain technology and Natural Language Processors (NLP) to assure protection of SPA from attacks.

Keywords: Internet of Things, Smart Home Personal Assistants, Natural Language Processors

1. INTRODUCTION

The influx of computers and computing was encountered with weaknesses in decoding meanings and understanding the objectives of the users. In that regard, there was a need to introduce peripheral input devices, for instance, keyboards, jockey sticks, touch monitors, and mouse, among others. As a result, there were implausible successes via the invention of versatile human-computer interfaces, for instance, the development of voice technology [1]. For that reason, using voice technology system has been confirmed to be the most effective and open communicative tool, which has expressively made an archetype shift in changing the method through which users relate with their devices [2]. Precisely, the most outstanding Internet of Things (IoT) is the Smart Home Personal Assistants (SPA) [3]. In essence, SPA technology uses intelligence in decoding and decrypting instructions, processing and evaluating them [4]. It also processes the needed task or couple of tasks. SPA as an IoT, has the advantage of eliminating hand-eye operations from the users by helping them to do diverse tasks using voice commands, thus allowing them shift their energies to other tasks [3].

Outwardly, SPA offers a quicker interaction as well as being more natural than the use of peripheral devices. Essentially, research outlines that SPA technology is dynamically gaining ascendency in homes and they estimate that more than 10% of the populace globally own these devices [1].

It is imperative to note that SPA has the ability to be embodied and customized to anchor human-machine interface. Precisely, blockchain technology and Natural Language Processors (NLP) devices in SPA presently are used in applications, which allow acquisition of goods and services, question applications, stream music, set timers, relay messages, anchor security, and facilitate making of calls, among others [5] and [6].

Essentially, SPA is a dynamically developing technology, which provides new ways through which users relate with the new innovations. Subsequently, SPA technology uses modular elements such as wake-word detection, speech-to-text, and intent-parser to generate user-interface [5]. As SPA technology is dynamically gaining popularity, it is important to recognize the threats and risks associated with the technology. It is equally important to devise ways to mitigate and enhance its utility [7]. Accordingly, this study will outline these risks later; nonetheless, it shall first assess some critical elements, which make the technology more high-end [5]. The study is structured to give an introduction to blockchain and NLP in SPA

technology and the architecture of components as well as interfaces. The next and subsequent sections provides a wide range of security and privacy issues and attacks in SPA apart from outlining an overview of attacks and mitigations [8]. The last sections will discuss the Z.

2. THEORETICAL FRAMEWORK

The Architecture and Operations of NLP in SPA

Theoretical framework of blockchain and NLP in SPA is based on its architecture and operations. In spite of the architecture for SPA being intricate as well as possessing explicit characteristics, all its systems have analogous functions and share conjoint features. Particularly, the elementary architecture of blockchain and NLP in SPA comprises of elements, which include cloud-based processing and exchangeable interaction features with other systems including, the voice-based intelligent personal agent and smart speaker (as will be discussed later) [9]. Imperatively, SPA is an internet-based technology that utilizes updates, which flourish with new internet services. The elements and architecture of blockchain and NLP explicates specific crucial elements in SPA architecture [10]. Remarkably, all parts of the component is a potential attack point for adversaries (as it will be discussed later in this write-up). In a bid to realize the complexity of the architecture of SPA, one will never miss to analyze the importance of the advancement in blockchain and NLP technology [11].

Pithily, NLP allows SPA to handle huge series of commands and responses simultaneously as well as allowing the advancement of machine Language, ML [11]. Primarily, ML is the best knowledge and usage of human language, which increase the computing supremacy and accessibility of datasets that train speech engines.

It is important to note that in processing, blockchain and Natural Language Processors performs audio sampling, feature abstraction, and speech recognition which transmutes a request into text. It is noteworthy that human language entails ambiguous words, contractions, similes, jargon, and others; therefore, it takes implausible assessment and couple of minutes for blockchain and NLP to decipher the accurate output [12] and [13]. Concisely, when the needed signal has been deciphered and cognized, an acoustic echo cancellation comes in place to negate noise from the receiver signal to ensure that only the needed and intended signal remains in the system [6], [14], and [15].

In this case, utilizes the system automatically senses and assesses the user's speech in terms pitch, amplitude, tone, and frequency, from which it extracts pattern and sends it to classifiers using machine language [12]. The extraction framework include Mel Frequency Cepstral Coefficient (MFCC) which apes human auditory system since it is constructed into audile prototype using ML such as Hidden Markov Model (HMM) to augment and correct the sound signal [1] and [16]. Essentially, HMM relates all pairs of the waveform with preceding and subsequent waveforms, and against a lexis of waveforms to decrypt the user's speech [17]. It also follows that after the SPA cloud has interpreted the user's language, it uses NLU (Natural Language Understanding), to comprehend the intent using discrete to discrete mapping (DDM) using statistical or ML models to make conventions about the intent [15]. Precisely, when the NLP system has a wider pool of data in disposal, the better the accuracy and correctness of the prediction [18]. In that case, the intent will then be processed, skill will be generated, and response will be sent to the natural language generation (NLG), where it is transformed into natural language representation [18]. Lastly, the response is communicated back to the user and played by the smart speaker.

As will be discussed in the subsequent sections in the next study, the components of blockchain and NLP in SPA will include morphological and lexical analysis, syntactical analysis, semantic analysis, discourse integration, and pragmatic analysis [18] and [19]. Ultimately, pragmatic analysis outlines the overall communicative and social content and its effects on interpretation.

2.1 INDUSTRY DESCRIPTION

Blockchain and NLP in SPA is developing home based security. Essentially, research outlines that SPA technology is dynamically gaining ascendency in homes and they estimate that more than 10% of the populace globally own these devices [1] and [20]. Concisely, the number is continually puffing up because the technology differs from the traditional voice-actuated devices, which only use built-in commands and responses [21]. In contrast from the ancient voice-actuated devices, SPA utilizes internet-based services, thus take the advantage of blockchain technology and Natural Language Processors (NLP), which are made to handle several series of commands, responses, as well as questions[22].

2.2 LITERATURE REVIEW

As earlier clarified that the use NPL framework is an open source smart home assistant (OSPA) though is gaining fame; nonetheless, it faces several attacks and risks. As a result, the objective of the study is to assess these weaknesses, aiming at adding filters and calibrating modules to alleviate attacks and risks [17]. Earlier studies show that NPL can be assessed on the efficacy of SPA and NPL filter modules created to fight against attacks and validate how the near future blockchain and NLP systems can be anchored to mitigate attacks [23]. That makes sense when the literature review of the study will focus on voice squatting attack and also filtering [24] and [25]. It will also feature the weak authentication, blockchain and NLP, user awareness, SPA security and privacy issues, the framework of SPA, blockchain and NLP weaknesses on security, peripheral security threats, and internal security problems [21]. Hence, the study utilized prevalent studies to generate new methodologies, and bring forth a theoretical argument on how to shape and anchor the prevailing knowledge with novel data and new ways in a bid to ease SPA from threats and attacks.

In a similar research, voice squatting became a threat and risk trajectory for Voice-Users-Interfaces (VUIs) that exploits on word sentence structure, which have the same sound but dissimilar word spelling and subsequently recording errors on the information [23]. It is of essence that researchers argued and outlined that voice squatting is an attack in a situation that the enemy utilizes the way through which a skill is invoked by means of a malicious and forged skill with analogous “pronounced name or phrased name” to capture the voice command envisioned for a different skill [4]. In that essence, via a voice concealed attack, the malicious skill mimics the SPA framework or the genuine skill to steal the user’s data and in other ways spy on the conversation [26] and [27]. Greatly to note that there are dual skills that appertains SPA framework; native and third-party skills. Both the skills are inclusive of home control skill, accounting and finance skill, communal skills, security and fitness, and sporting skill, among others [28] and [29]. Initial reports show that SPA will acquire the user’s choices, records, and facts, for instance, etymology, conduct, behavior, words, and searches using search engine optimization and machine learning techniques to make them more proficient and shrewder with time[30]. Succinctly, the choices and information, among others, are the ones that are vulnerable to attacks from enemies [31]. According to a new research, attacks as depicted by Amazon Echo's Alexa, comprises of adversary who registers a deceitful and non-genuine third party application with a voice keyword that mimics the user’s real application [32]. Truthfully,

when the user demands for the real and legitimate application, the deceitful app opens. Initial and traditional devices recognized the speech accuracy and functionality, however, it experienced regular misconception rendering it the most ineffective system [33] and [34]. It is important to note that, this type of squatting is rightfully dangerous, because it runs in the background in couples of time without being detected [35]. Also, such background squatting can be utilized to capture the user's information and private indulgence without permission [36]. Such information and privacy info can easily be used by the adversaries to broadcast wrong prompts for users to divulge personally identifiable information (PII).

2.3 PROBLEM STATEMENT & RESEARCH GAP & RESEARCH CONTRIBUTION

Primarily, earlier studies show that voice squatting attack could be encountered during computer's change and deciphering procedure connected to the skill name. Accordingly, the susceptibility in SPA as IoT emanates from the misconstruction pertaining blockchain and NLP and initial transition due to enunciation, tone, and homophone [9][37]. In an instance, born and bone can be misconstrued incorrectly by blockchain and NLP unit. If a user wants to invoke skill named 'YY born' but NLP module misinterpret it as 'YY bone' skill, an adversary skill, SPA will invoke skill incorrectly and leak user's delicate information or give wrongful feedbacks [38]. In traditional invocation, there is another voice squatting attack that takes advantage of corresponding skill appellation length [39]. Essentially, when a user has an idiomatic use of speech such as use 'thank you' for polite or use 'please again', an adversary can register skills based on this model [40] and [41]. For example, a savvy SPA enemy can record a skill named 'calm please' to mimic the skill 'come'. In essence, when the user calls for calm skill by saying 'please be calm', SPA will return skill 'come please' instead of 'calm' because SPAs tend to invoke skill that fit best. Consequently, skill with longer fit name will be invoked and the enemy skill is waked up in this situation causing revilement of information.

Many initial studies failed to cognizes that blockchain and NLP uses voice structure draws responses from contextual patterns [42]. In that spirit, to achieve a concise and precise response from any machine SPA and NLP, considerable data needs to be given to the system for it to learn and decode from experiences; through this the system will provide a vector via which it can decipher from many datasets, utilize deep learning algorithms, and use surrounding words to give an accurate response [38]. Therefore, this study ascertains the use of blockchain and

NLP in SPA (IoT) to generate a systemic writing system utilized for an expressive language as the ultimate approach for text pre-processing; writing being logographic system, which uses symbols to represent a word [43]. Of importance, ultimately, is the use of alphabetic symbol approach that utilizes distinct symbols from the alphabets to denote a sound.

3. RESEARCH MODEL & HYPOTHESES

Therefore, using mixed research methodology, the study found out that there is a need to mitigate the attacks on the blockchain technology and NLP to assure protection of SPA from attacks. Hypotheses for this research was for the system to address security and privacy issues at the end of the study.

3.1 METHODOLOGY & RESEARCH DESIGN

The research mainly used mixed research methodology as well as utilizing literature review and earlier technologies to develop more robust system. It also utilizes weakness of the existing technologies to address the problem in a more versatile way. The main aim of the study was to address weaknesses in security and privacy in SPA system.

The research therefore assumed the following format

1) Identification of the weakness in SPA technology by interacting with the users.

2) Developing a major blockchain and NLP using machine language.

3) Introduction of filers to filters so as to cancel noise which could be used by adversaries

4) The extraction framework include Mel Frequency Cepstral Coefficient (MFCC) which apes human auditory system since it is constructed into audile prototype using ML such as Hidden Markov Model (HMM) to augment and correct the sound signal

5) Final basing the system architecture in internet network.

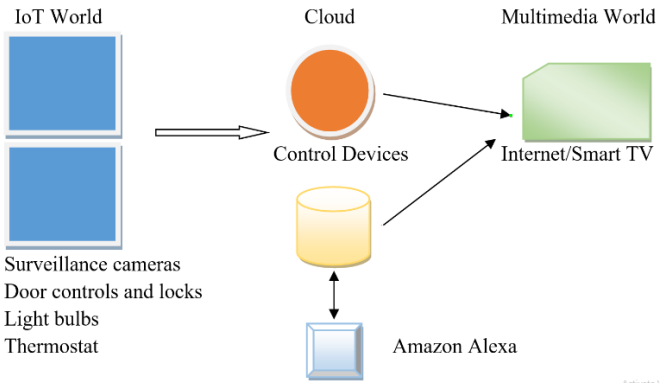

Fig. 1. Conceptual Model

Fig. 2.

3.2 Population & Sample & Unit of Analysis

The research considered user sample unit to assess the infiltration rate of security and privacy. It, therefore, took samples of SPA users' complaints to assess the weakness in the technology. More than 20 users were used as the sample space and unit of analysis. All the twenty users had either complaints security and privacy infiltrate or challenges in using the technology. The effectiveness of the technology was weighted using percentages on privacy, security and challenges in using SPA technology as following;

Where security = n

Privacy = p

Challenges = c

Effectiveness of SPA = n + p + c

The effectiveness was calculated with an assumption that the same relative weight of up to 100%. Thus the sum of the three variables forms the average weight. Essentially, the selected users were required to give details on the three variables; privacy, security and challenges in using SPA technology, which gave to give the relative weight.

4. ANALYZING DATA

The equation for effectiveness = n + p + c was used in the analysis of the data. Validation and reliability of blockchain and NLP in SPA was subjected to a couple of test to enhance accuracy.

Privacy was captured through questionnaire which was filled by the twenty users either online or manually.

The user privacy = (number of complaints in privacy (pt) + number of satisfied users (st)) divide by sample space (ss)

$$(p) = (pt + st)/ss$$

On the other hand, security Issues (n) = number of security complaint (sc) – number of satisfied users (st) divide by sample space (ss)

$$S= (sc – st)/ss$$

Number of challenges (c) = number of challenges complaint (cc) – number of satisfied users (st) divide by sample space (ss)

$$C = (cc – st)/ss.$$

4.1 DISCUSSION OF THE RESULTS

The result of the research study emanated from three variables; privacy, security and challenges in using SPA technology, which gave to give the relative weight. In this case, relative weight and formula above was used to give accurate, valid and reliable results as follows;

It was found that blockchain and NLP in SPA was found to have high infiltration rate with security and privacy issues being higher at up to 88% and 90% respectively, while challenges in the use of technology was lower at 25%.

It can assessed, that the use of filers and filters can only solve the problems of the three variables. The challenges, security and privacy issues are attributed to architectural issues,

which are main features that contributes to the differences in the weighted percentages. As a result, it is changing the architecture by introducing filers to filters and introducing acoustic and noise cancellation buzzers through HMM, will solve the weaknesses in blockchain and NLP in SPA.

5. CONCLUSION AND RECOMMENDATION

Conclusively, confirms that SPA as an IoT is a more adaptable and versatile technology to users and it is dynamically gaining popularity across the globe. The architecture of the technology is unwavering the best, however, it has traditional technologies failed to address some pertinent issues on security and privacy of users. The weaknesses included the open-nature of the voice channel, complexity of the architecture, software implications, and the utility of the technology to less proficient users, among others. It can be depicted from the write-up that the use of blockchain and NLP in SPA can address these weaknesses. From the mixed research methodology, the study found out that there is a need to mitigate the attacks on the blockchain and NLP to assure protection of SPA from attacks. It can be deduced succinctly that acoustic echo cancellation in signal transmission negates noise from transmission, which in turn reduces the vulnerability of SPA. In that regard, it can be firmly affirmed that the use of SPA becomes the best solution in home base smart personal systems. It can also be deduced that weaknesses and threats in SPA can be addressed through the use of interaction interfaces that impede adversaries from gaining access to users' personal information.

REFERENCES

[1] S. Chen, K. Ren, S. Piao, C. Wang, Q. Wang, J. Weng, L. Su, and A. Mohaisen, "You Can Hear but You Cannot Steal: Defending Against Voice Impersonation Attacks on Smartphones," in Proceedings - International Conference on Distributed Computing Systems, Jul. 2017, pp. 183–195. doi: 10.1109/ICDCS.2017.133.

[2] E. Alepis and C. Patsakis, "Monkey Says, Monkey Does: Security and Privacy on Voice Assistants," IEEE Access, vol. 5, pp. 17841–17851, Aug. 2017, doi: 10.1109/ACCESS.2017.2747626.

[3] G. Iliev and N. Kasabov, "Adaptive Filtering with Averaging in Noise Cancellation for Voice and Speech Recognition," IEEE, vol. 99, Nov. 1999.

[4] M. I. Jordan and T. M. Mitchell, "Machine learning: Trends, perspectives, and prospects," Science, vol. 349, no. 6245, pp. 255–260, Jul. 2015, doi: 10.1126/SCIENCE.AAA8415.

[5] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things (IoT): A vision, architectural elements, and future directions," Future Generation Computer Systems, vol. 29, no. 7, pp. 1645–1660, Sep. 2013, doi: 10.1016/J.FUTURE.2013.01.010.

[6] T. M. G. D. K. Mohammed A. M. Afifi, "The Impact of Deploying the Internet of Things and How Will It Change Our Lives," Solid State Technology, vol. 64, no. 2, pp. 2049–2055, Feb. 2021, Accessed: Nov. 16, 2021. [Online]. Available: https://solidstatetechnology.us/index.php/JSST/article/view/9517

[7] V. Kepuska and G. Bohouta, "Next-generation of virtual personal assistants (Microsoft Cortana, Apple Siri, Amazon Alexa and Google Home)," in IEEE 8th Annual Computing and Communication Workshop and Conference, CCWC, Feb. 2018, vol. 2018-January, pp. 99–103. doi: 10.1109/CCWC.2018.8301638.

[8] T. T. A. Dinh, R. Liu, M. Zhang, G. Chen, B. C. Ooi, and J. Wang, "Untangling Blockchain: A Data Processing View of Blockchain Systems," IEEE Transactions on Knowledge and Data Engineering, vol. 30, no. 7, pp. 1366–1385, Jul. 2018, doi: 10.1109/TKDE.2017.2781227.

[9] F. Matloob, T. M. Ghazal, N. Taleb, S. Aftab, M. Ahmad, M. A. Khan, S. Abbas, and T. R. Soomro, "Software defect prediction using ensemble learning: A systematic literature review," IEEE Access, vol. 9, pp. 98754–98771, Jul. 2021, doi: 10.1109/ACCESS.2021.3095559.

[10] T. M. Ghazal, M. Anam, M. K. Hasan, M. Hussain, M. S. Farooq, H. M. A. Ali, M. Ahmad, and T. R. Soomro, "Hep-pred: Hepatitis C staging prediction using fine gaussian SVM," Computers, Materials and Continua, vol. 69, no. 1, pp. 191–203, Jun. 2021, doi: 10.32604/CMC.2021.015436.

[11] A. Easwara Moorthy and K. P. L. Vu, "Privacy Concerns for Use of Voice Activated Personal Assistant in the Public Space," International Journal of Human–Computer Interaction , vol. 31, no. 4, pp. 307–335, Apr. 2015, doi: 10.1080/10447318.2014.986642.

[12] K. Ateeq, M. R. Pradhan, B. Mago, and T. Ghazal, "Encryption as a Service for Multi-Cloud Environment," International Journal of Advanced Research in Engineering and Technology (IJARET) , vol. 11, no. 7, pp. 622–628, Jul. 2020, Accessed: Nov. 17, 2021. [Online]. Available: https://www.researchgate.net/publication/344308747_Encryption_as_a_Service_for_Multi-Cloud_Environment

[13] M. Nofer, P. Gomber, O. Hinz, and D. Schiereck, "Blockchain," Business & Information Systems Engineering, vol. 59, no. 3, Jun. 2017, Accessed: Nov. 17, 2021. [Online]. Available: https://aisel.aisnet.org/bise/vol59/iss3/7

[14] G. Lavrentyeva, S. Novoselov, E. Malykh, A. Kozlov, O. Kudashev, and V. Shchemelinin, "Audio-Replay Attack Detection Countermeasures," in International Conference on Speech and Computer, 2017, vol. 10458 LNAI, pp. 171–181. doi: 10.1007/978-3-319-66429-3_16.

[15] N. Fruchter and I. Liccardi, "Consumer attitudes towards privacy and security in home assistants," in Conference on Human Factors in Computing Systems - Proceedings, Apr. 2018, vol. 2018-April, pp. 1–6. doi: 10.1145/3170427.3188448.

[16] T. M. Ghazal, M. T. Alshurideh, and H. M. Alzoubi, "Blockchain-Enabled Internet of Things (IoT) Platforms for Pharmaceutical and Biomedical Research," in Proceedings of the International Conference on Artificial Intelligence and Computer Vision (AICV2021), Jun. 2021, pp. 589–600. doi: 10.1007/978-3-030-76346-6_52.

[17] D. Poddebniak, C. Dresen, J. Somorovsky, J. Schwenk, J. Müller, F. Ising, S. Schinzel, and S. Friedberger, "Skill Squatting Attacks on Amazon Alexa," in USENIX Security Symposium, 2018, pp. 33–47. Accessed: Nov. 17, 2021. [Online]. Available: https://www.usenix.org/conference/usenixsecurity18/presentation/poddebniak

[18] R. M. al Batayneh, N. Taleb, R. A. Said, M. T. Alshurideh, T. M. Ghazal, and H. M. Alzoubi, "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 Proceedings of the International Conference on Artificial Intelligence and Computer Vision (AICV2021), Jun. 2021, pp. 235–247. doi: 10.1007/978-3-030-76346-6_22.

[19] H. M. Alzoubi, M. Alshurideh, and T. M. Ghazal, "Integrating BLE Beacon Technology with Intelligent Information Systems IIS for Operations' Performance: A Managerial Perspective," in Proceedings of the International Conference on Artificial Intelligence and Computer Vision (AICV2021) , Jun. 2021, pp. 527–538. doi: 10.1007/978-3-030-76346-6_48.

[20] E. Zeng, S. Mare, F. Roesner, S. Clara, E. Zeng, S. Mare, and F. Roesner, "End User Security and Privacy Concerns with Smart Homes," Thirteenth Symposium on Usable Privacy and Security (SOUPS), no. Soups, 2017.

[21] X. Lei, G. H. Tu, A. X. Liu, C. Y. Li, and T. Xie, "The insecurity of home digital voice assistants - Vulnerabilities, attacks and countermeasures," Aug. 2018. doi: 10.1109/CNS.2018.8433167.

[22] E. Rehman, M. A. Khan, T. R. Soomro, N. Taleb, M. A. Afifi, and T. M. Ghazal, "Using blockchain to ensure trust between donor agencies and ngos in under-developed countries," Computers, vol. 10, no. 8, 2021, doi: 10.3390/computers10080098.

[23] F. Jelinek, Statistical methods for speech recognition. MIT Press, 1997. Accessed: Nov. 17, 2021. [Online]. Available: https://mitpress.mit.edu/books/statistical-methods-speech-recognition

[24] O. Novo, "Blockchain Meets IoT: An Architecture for Scalable Access Management in IoT," IEEE Internet of Things Journal, vol. 5, no. 2, 2018, doi: 10.1109/JIOT.2018.2812239.

[25] C. Stergiou, K. E. Psannis, B. G. Kim, and B. Gupta, "Secure integration of IoT and Cloud Computing," Future Generation Computer Systems, vol. 78, 2018, doi: 10.1016/j.future.2016.11.031.

[26] S. Madakam, R. Ramaswamy, S. Tripathi, S. Madakam, R. Ramaswamy, and S. Tripathi, "Internet of Things (IoT): A Literature Review," Journal of Computer and Communications, vol. 3, no. 5, pp. 164–173, May 2015, doi: 10.4236/JCC.2015.35021.

[27] N. Zhang, X. Mi, X. Feng, X. Wang, Y. Tian, and F. Qian, "Dangerous skills: Understanding and mitigating security risks of voice-controlled third-party functions on virtual personal assistant systems," in Proceedings - IEEE Symposium on Security and Privacy, 2019, vol. 2019-May. doi: 10.1109/SP.2019.00016.

[28] M. Pilkington, "Blockchain technology: Principles and applications," in Research Handbooks on Digital Transformations, 2016. doi: 10.4337/9781784717766.00019.

[29] Z. Zheng, S. Xie, H. N. Dai, X. Chen, and H. Wang, "Blockchain challenges and opportunities: A survey," International Journal of Web and Grid Services, vol. 14, no. 4, 2018, doi: 10.1504/IJWGS.2018.095647.

[30] N. Ali, T. M. Ghazal, A. Ahmed, S. Abbas, M. A. Khan, H. M. Alzoubi, U. Farooq, M. Ahmad, and M. Adnan Khan, "Fusion-Based Supply Chain Collaboration Using Machine Learning Techniques," Intelligent Automation & Soft Computing, vol. 31, no. 3, 2022, doi: 10.32604/iasc.2022.019892.

[31] V. Martin, Q. Cao, and T. Benson, "Fending off IoT-hunting attacks at home networks," in Cloud-Assisted Networking Workshop, Dec. 2017, pp. 67–72. doi: 10.1145/3155921.3160640.

[32] M. K. H. R. H. , S. I. S. N. H. S. A. , M. A. M. A. , D. K. Taher M. Ghazal, "Security Vulnerabilities, Attacks, Threats and the Proposed Countermeasures for the Internet of Things Applications," Solid State Technology, vol. 63, no. 1s, pp. 2513–2521, Oct.

2020, Accessed: Nov. 16, 2021. [Online]. Available: https://solidstatetechnology.us/index.php/JSST/article/view/3096

[33] K. al Shebli, R. A. Said, N. Taleb, T. M. Ghazal, M. T. Alshurideh, and H. M. Alzoubi, "RTA's Employees' Perceptions Toward the Efficiency of Artificial Intelligence and Big Data Utilization in Providing Smart Services to the Residents of Dubai," in Proceedings of the International Conference on Artificial Intelligence and Computer Vision (AICV2021), Jun. 2021, pp. 573–585. doi: 10.1007/978-3-030-76346-6_51.

[34] M. Suleman, T. R. Soomro, T. M. Ghazal, and M. Alshurideh, "Combating Against Potentially Harmful Mobile Apps," in Proceedings of the International Conference on Artificial Intelligence and Computer Vision (AICV2021), Jun. 2021, pp. 154–173. doi: 10.1007/978-3-030-76346-6_15.

[35] A. K. Carter and C. G. Clopper, "Prosodic effects on word reduction," Language and Speech, vol. 45, no. 4, pp. 321–353, Aug. 2002, doi: 10.1177/00238309020450040201.

[36] T. M. Ghazal, R. A. Said, and N. Taleb, "Internet of vehicles and autonomous systems with AI for medical things," Soft Computing, pp. 1–13, Jul. 2021, doi: 10.1007/S00500-021-06035-2/TABLES/5.

[37] T. M. Ghazal, "Internet of Things with Artificial Intelligence for Health Care Security," Arabian Journal for Science and Engineering 2021, pp. 1–12, Aug. 2021, doi: 10.1007/S13369-021-06083-8.

[38] T. M. Ghazal, T. R. Soomro, and K. Shaalan, "Integration of Project Management Maturity (PMM) Based on Capability Maturity Model Integration (CMMI)," European journal of scientific research, vol. 99, no. 3, pp. 418–428, Apr. 2013.

[39] P. Svoboda, T. M. Ghazal, M. A. M. Afifi, D. Kalra, M. T. Alshurideh, and H. M. Alzoubi, "Information Systems Integration to Enhance Operational Customer Relationship Management in the Pharmaceutical Industry," in Proceedings of the International Conference on Artificial Intelligence and Computer Vision (AICV2021), Jun. 2021, pp. 553–572. doi: 10.1007/978-3-030-76346-6_50.

[40] M. McCARTHY, D. A. JAMES, J. B. LEE, T. WADA, and D. ROWLANDS, "Effect of Machine Learning Techniques Upon Wearable Devices," in The Proceedings of the Symposium on sports and human dynamics, Nov. 2016, vol. 2016, no. 0, p. A-30. doi: 10.1299/JSMESHD.2016.A-30.

[41] A. H. Ngu, M. Gutierrez, V. Metsis, S. Nepal, and Q. Z. Sheng, "IoT Middleware: A Survey on Issues and Enabling Technologies," IEEE Internet of Things Journal, vol. 4, no. 1, pp. 1–20, Feb. 2017, doi: 10.1109/JIOT.2016.2615180.

[42] D. Yaga, P. Mell, N. Roby, and K. Scarfone, "Blockchain Technology Overview - National Institute of Standards and Technology Internal Report 8202," NIST Interagency/Internal Report, 2018.

[43] R. Naqvi, T. R. Soomro, H. M. Alzoubi, T. M. Ghazal, and M. T. Alshurideh, "The Nexus Between Big Data and Decision-Making: A Study of Big Data Techniques and Technologies," in Proceedings of the International Conference on Artificial Intelligence and Computer Vision (AICV2021), Jun. 2021, pp. 838–853. doi: 10.1007/978-3-030-76346-6_73.

[44]. Alzoubi, H. (2018). The Role of Intelligent Information System in e-Supply Chain Management Performance. International Journal of Multidisciplinary Thought, 7(2), 363–370.

[45]. Alzoubi, A., Al-Gasaymeh, A., & Alzoubi, H. (2018). The Impact of Changes in the Qualitative Characteristics of Accounting Information on the Quality of Investment Decisions: A Field Study in the Brokerage Offices. The Journal of Economic and Management Perspectives (JEMP), 12(4), 67-82.

[46]. Alnazer, N., Alnuaimi, M. & Alzoubi, H. (2017). Analyzing the Appropriate Cognitive Styles and its effect on Strategic Innovation in Jordanian Universities. International journal of business excellence, 13(1), 127-140, doi.org/10.1504/IJBEX.2017.085799

[47]. Khafajy, N., Alzoubi, H. & Aljanabee, A. (2016). Analyzing the effect of knowledge management processes in the services' quality in Iraqi commercial banks. International Review of Management and Business Research, 5(1), 302-314.

[48]. Alzoubi, H., Alnazer, N. & Alzoubi, A. (2016). Exploring the Impact of the use of Business Information systems BIS on the organizational performance effectiveness. International Journal of Business and Management Invention, 5(4), 48-55.

[49]. Alnuaimi, M., Alzoubi, H., Alzubi, A. & AL-Shinewi, M. (2015). The Impact of Managers Efficiency on Quality of Strategic Decision-making under Crisis Management. European Journal of Business and Management, 7(26), 156-166.

[50]. Alrubaiee, L., Alzubi, H., Hanandeh, R. & Ali, R. (2015). Investigating the Relationship between Knowledge Management Processes and Organizational Performance: The Mediating Effect of Organizational Innovation. International Review of Management and Business Research, 4(4), 977-997

[51]. Alzoubi, H. & Khafajy, N. (2015). The Impact of Business Process Management on Business Performance Superiority. International Journal of Business and Management Review, 3(2), 17-34

[52]. Alzubi, H., Mohammad, S. & Abu-salma, A. (2015). Evaluating Strategic Quality Management Dimensions Using Analytic Hierarchy Process (AHP) and its Impact on Organizational Success. International Journal of Research in Management, 5(1), 137-150.

[53]. Mohammad, S., Abu-salma, A. & Alzoubi, H. (2015). American Muslims' Perceptions Toward Transforming Islamic Banking System. International Journal of Economics, Commerce and Management, 5(1), 1-16.

[54]. Alrubaiee, L., Al zuobi, H. & Abu-Alwafa, R. (2013). Exploring the Relationship between Quality Orientation, New Services Development and Organizational Performance. American Academic & Scholarly Research Journal, 5(3), 315-329.

[55]. Alzoubi, H. & Khafajy, N. (2010). Analyze the Impact of Managers Awareness of Environmental Uncertainty on Exploiting Strategic Competencies. Egyptian Journal for Commercial Studies, 34(2), 611-625.

[56]. Al-zu'bi, H. (2010). Applying Electronic Supply Chain Management Using Multi-Agent System: A Managerial Perspective. International Arab Journal of e-Technology, 1(3), 106-113.

[57]. Alnuaimi, M., Alzoubi, A. & Alzoubi, H. (2010). Propose a model for Performance Criteria and measuring its impact for Achieving Excellence. Association of Arab Universities Journal, 56(4), 920-941.

[58]. Mehmood, T., Alzoubi, H, Alshurideh, M., Al-Gasaymeh, A., &Ahmed, G. (2019). Schumpeterian Entrepreneurship Theory: Evolution and Relevance. Academy of Entrepreneurship Journal, 25(4). 1-10, doi.org/10.1080/13662716.2016.1216397

[59]. Alzoubi, H., Ahmed, G., Al-Gasaymeh, A., & Alkurdi, B. (2019). Empirical study on Sustainable Supply Chain Strategies and its impact on Competitive Priorities: The mediating role of Supply Chain Collaboration. Management Science Letters, 10(3), 703-708, doi.org/10.5267/j.msl.2019.9.008

[60]. Alzoubi, H. & Ahmed, G. (2019). Do Total Quality Management (TQM) Practices Improve Organisational Success? A case study of electronics industry in the UAE. International Journal of Economics and Business Research, 17(4), 459-472, doi.org/10.1504/IJEBR.2019.099975

[61]. Al-Gasaymeh, A., Ahmed, G., Mehmood, T. & Alzoubi, H. (2019). Co-Integration Tests and the Long-Run Purchasing Power Parity: A Case Study of India and Pakistan Currencies. Theoretical Economics Letters, 9(4), 570-583.

[62]. Alzoubi, H., Abdo M., Al-Gasaymeh, A. & Alzoubi, A. (2019). An empirical study of e-Service quality and its impact on achieving a value added. Journal of Business and Retail Management Research (JBRMR), 13(4), 138-145.

[63]. Aziz, N., & Aftab, S. (2021). Data Mining Framework for Nutrition Ranking: Methodology: SPSS Modeller. International Journal of Technology, Innovation and Management (IJTIM), 1(1), 85-95.

[64]. Radwan, N., & Farouk, M. (2021). The Growth of Internet of Things (IoT) In The Management of Healthcare Issues and Healthcare Policy Development. International Journal of Technology, Innovation and Management (IJTIM), 1(1), 69-84.

[65]. Cruz, A. (2021). Convergence between Blockchain and the Internet of Things. International Journal of Technology, Innovation and Management (IJTIM), 1(1), 34-53.

[66]. Lee, C., & Ahmed, G. (2021). Improving IoT Privacy, Data Protection and Security Concerns. International Journal of Technology, Innovation and Management (IJTIM), 1(1), 18-33.

[67]. Alzoubi, A. (2021) The impact of Process Quality and Quality Control on Organizational Competitiveness at 5-star hotels in Dubai. International Journal of Technology, Innovation and Management (IJTIM). 1(1), 54-68

[68]. Al Ali, A. (2021). The Impact of Information Sharing and Quality Assurance on Customer Service at UAE Banking Sector. International Journal of Technology, Innovation and Management (IJTIM), 1(1), 01-17.

[69]. Kashif, A. A., Bakhtawar, B., Akhtar, A., Akhtar, S., Aziz, N., & Javeid, M. S. (2021). Treatment Response Prediction in Hepatitis C Patients using Machine Learning Techniques. International Journal of Technology, Innovation and Management (IJTIM), 1(2), 79-89.

[70]. Akhtar, A., Akhtar, S., Bakhtawar, B., Kashif, A. A., Aziz, N., & Javeid, M. S. (2021). COVID-19 Detection from CBC using Machine Learning Techniques. International Journal of Technology, Innovation and Management (IJTIM), 1(2), 65-78.

[71]. Eli, T. (2021). StudentsPerspectives on the Use of Innovative and Interactive Teaching Methods at the University of Nouakchott Al Aasriya, Mauritania: English Department as a Case Study. International Journal of Technology, Innovation and Management (IJTIM), 1(2), 90-104.

[72]. Alsharari, N. (2021). Integrating Blockchain Technology with Internet of things to Efficiency. International Journal of Technology, Innovation and Management (IJTIM), 1(2), 01-13.

[73]. Mehmood, T. (2021). Does Information Technology Competencies and Fleet Management Practices lead to Effective Service Delivery? Empirical Evidence from E-Commerce Industry. International Journal of Technology, Innovation and Management (IJTIM), 1(2), 14-41.

[74]. Miller, D. (2021). The Best Practice of Teach Computer Science Students to Use Paper Prototyping. International Journal of Technology, Innovation and Management (IJTIM), 1(2), 42-63.