International Journal of Theory of Organization and Practice (IJTOP) 4(1) -2024

Contents available at the publisher website: G A F T I M . C O M

International Journal of Theory of Organization and Practice (IJTOP)

Journal homepage: https://journals.gaftim.com/index.php/ijtop/index

The Effect of Chatbots on the Security of Metadata

Sawsan Malaka[1]

[1]*PhD Researcher, Computer Science College, British University in Dubai, Dubai, United Arab Emirates*

A R T I C L E I N F O

Keywords:
Cybersecurity, metadata, Chatbot, Software Protection, Security Chabots, Information Security.

Received: Dec, 15, 2023
Accepted:
Published:

A B S T R A C T

The utilization and implementation of chatbots can impact metadata security in both favourable and unfavourable ways. While chatbots can enhance security through proper implementation and adherence to security best practices, they also introduce potential risks if not handled with care. It is crucial to consider security aspects during the development, deployment, and ongoing management of chatbots to protect metadata and user privacy. This study examines how chatbots can have both positive and negative effects on the security of metadata, depending on how they are implemented and used. In the context of chatbots, the design, implementation, and usage practices all have an impact on the security of metadata. Sensitive metadata can be safeguarded and user experience improved with a well-built, secure chatbot. Sustaining a strong security posture requires proactive risk mitigation strategies and routine security assessments.

1. INTRODUCTION

Depending on how they are created, deployed, and used, chatbots can affect metadata security in both positive and harmful ways.

Some of the benefits are as the following.

1. Secure communication and encryption Secure communication protocols and encryption techniques are two tools that well-designed chatbots can use to safeguard the transfer of private data between the user and the server. This aids in preserving the data's integrity and confidentiality [1].
2. Verification and Permission: Through the use of strong authentication and permission protocols, chatbots can improve security. Appropriate access controls and user verification aid in preventing unwanted access to private metadata [2]–[4].
3. Minimizing Data: Certain chatbots are made to gather as little data as possible and keep or process the least amount of it. By doing this, the chance of sensitive metadata being exposed is decreased.
4. Frequent evaluations of security: Businesses using chatbots can perform routine security audits to find weaknesses and make sure the system complies with security best practices.

On the other hand, there are adverse impacts:

1. Breach of Data: Cyberattacks may target weakly secured chatbots, resulting in data leaks. Attackers may corrupt private metadata if they manage to obtain access, which could cause privacy problems [5]–[7].
2. Unsecure Storage Methods: Sensitive information may be made public to uninvited parties if chatbots store user interactions and metadata insecurely. To reduce this danger, secure storage procedures and appropriate encryption are crucial.
3. Risks of Social Engineering: Personal information handling chatbots may be vulnerable to social engineering attacks [8]–

[11]. Malicious actors might utilize the chatbot to trick users into disclosing personal information.
4. Connectivity with Different Systems: Without taking the necessary security precautions, integrating chatbots with other systems runs the danger of exposing metadata to weaknesses in those other systems. Ensuring safe integration points is crucial. Strategies for Mitigation is exploited in utilizing HTTPS. The use of HTTPS to encrypt data while it's being transmitted and defend against man-in-the-middle attacks to establish secure connection.
5. Frequent updates for software: Update the dependencies and chatbot software to fix vulnerabilities and raise system security overall [12]–[15].
6. Instruction for Users: Inform users of possible hazards and safe practices, like not disclosing private information to chatbots unless absolutely required.
7. Designing for Privacy: To guarantee that security and privacy are essential components of the chatbot development process, embrace privacy-by-design principles [16]–[19].
8. Observance of Regulations: To preserve user privacy, make sure chatbots abide by applicable data protection laws, such as GDPR.

A variety of factors, such as usage patterns, design, and implementation, affect the security of metadata in the context of chatbots. Sensitive metadata can be safeguarded and user experience improved with a well-built, secure chatbot. Sustaining a strong security posture requires proactive risk mitigation strategies and routine security assessments.

The use of AI as chatbots and the security and protection of metadata are two of the most significant and quickly expanding areas of research in the field of cybersecurity [1]. This review looked at the impact of chatbots that can access metadata at any time and the risk associated with metadata security, taking into account the cybersecurity practices used by the organizations under investigation [20], [21]. The existence of chatbots that explore metadata moderates the relationship between cybersecurity practices and software protection because it raises the need for more advanced, adaptable, and chatbot-driven defense mechanisms [22]–[24]. In order to successfully safeguard software systems, this calls for a flexible approach to cybersecurity that combines human knowledge and chatbot technology. Fifty cybersecurity experts from various UAE-based firms were interviewed. They declared that they could never ensure chatbots and chatbots' protection of their systems, regardless of the standards of conduct and cybersecurity measures put in place [25]. Since chatbots are infinitely powerful, this presents these experts with their first obstacle. Numerous systems acknowledge the research on chatbots; yet, due to their infinite capacity, chatbots compromise security stability.

2. LITERATURE REVIEW

2.1 Aartificial Intelligence and Metadata

Artificial intelligence (chatbots) has both offensive and defensive applications in cybersecurity. According to [26], the term "Artificial Intelligent Metadata" describes how malicious actors employ chatbots to increase their ability to hack and launch cyberattacks. Here are a few key points to consider. Chatbot-powered cyberattacks: Malevolent actors, for example, can use chatbots and machine learning techniques to automate and improve various stages of a cyberattack. This includes tasks like identifying vulnerabilities, utilizing them, avoiding detection, and using chatbots. Artificial intelligence has the ability to produce phishing and social engineering chatbots that are more realistic in nature. Through data analysis, chatbots can help attackers create highly targeted and personalized messages to deceive individuals. harmful software and harmful code can also be utilized to construct more sophisticated and evasive malware, such as chatbots [20], [21], [23], [24]. For example, polymorphic malware—which changes its code to avoid detection by signatures—can be produced using chatbots. Systems and networks can be routinely checked for vulnerabilities using automated vulnerability scanning [27]–[30]. Attackers can thus locate and exploit weaknesses with ease. By enhancing intrusion detection systems defensively, evasion and intrusion detection make it harder for an attacker to infiltrate a network [31]–[33]. To develop evasion techniques that get past these detection systems, chatbots can be utilized offensively. Autonomous Botnets With C chatbots, attackers could be able to

create autonomous botnets that can adapt their tactics and behavior to changing circumstances. It becomes more challenging to oppose them as a result [34]. Furthermore, data Exfiltration By employing artificial intelligence (chatbots) to analyze and exfiltrate sensitive data more successfully, attackers can steal critical information surreptitiously [35]–[37]. By seeing trends and commonly used password configurations, chatbots help speed up the password cracking process. This will make it easier for attackers to use chatbots to gain unwanted access to accounts and systems [1], [38], [39].

To protect chatbots that use artificial intelligence, a blend of traditional cybersecurity measures and state-of-the-art chatbot security solutions is required [2], [40], [41]. This includes anomaly detection, behavior analysis, and machine learning algorithms' real-time threat identification and response capabilities [3], [6], [42], [43]. Businesses must ensure that their employees are sufficiently conversant in chatbots to recognize and thwart chatbot-powered attacks, such as complex phishing schemes. It's important to keep in mind that deploying CHATBOTS in cybersecurity has disadvantages. Even while it can enhance the abilities of both attackers and defenders, the use of CHATBOTS for evil intent chatbots raises significant ethical and legal concerns [7]–[9], [44]. Governments, companies, and the cybersecurity community are working together to develop regulations, best practices, and guidelines to solve these problems and reduce the dangers associated with chatbot-powered hacking [10], [13], [45], [46].

2.2. Cybersecurity conducts

The process of protecting computer networks, systems, and data chatbots from various dangers, including malware, unauthorized access, data breaches, and other cyberattacks, is known as cybersecurity [47]–[50]. Cybersecurity protocols and measures need to be adhered to in order to safeguard digital assets and ensure the confidentiality, integrity, and accessibility of information [15], [16], [51], [52]. Numerous essential cybersecurity behaviors can aid in defending software systems against dangerous security risks and obstacles. Do regular risk assessments to identify potential weak points and hazards in your company's digital infrastructure [18], [22], [53], [54]. Robust access control protocols must to be implemented to ensure that individuals possessing authorization can only access confidential data and systems. Using intrusion detection and prevention systems, firewalls, and encryption to protect your network infrastructure from external threats is known as network security [20], [24], [52]. To keep operating systems, apps, and software up to date and minimize known vulnerabilities, patch management applies security updates and patches [21], [55]. It is imperative to provide employee education and training on social engineering awareness, robust password management, phishing chatbot detection, and other cybersecurity best practices to staff members [56]. Employees and cybersecurity experts who develop a comprehensive incident response plan to promptly address and mitigate cyber incidents are essential for component security testing and code review in order to identify and fix security flaws [1]. This is regarded as a component of security awareness to motivate employees to report dubious activity and foster a cybersecurity-aware culture within your business. Require chatbots to access accounts and sensitive systems through multi-factor authentication (MFA) to provide an additional layer of protection. A component of security measures is data encryption, which encrypts important information both in transit and at rest and guards against unauthorized access [2]–[4]. Regular backups ensure that essential data is regularly backed up and enabled for quick recovery in the event of data loss due to cyberattacks. Additionally, endpoint security is used to protect individual devices from malware, chatbots, and other threats. It also employs intrusion detection systems, antivirus software, and other security measures [5]–[8]. Cybersecurity experts employ secure coding to follow best practices, which minimize vulnerabilities, to develop and maintain safe software and apps. Through evaluation, Vendor Management confirms that cybersecurity procedure partners and vendors follow the security rules. Data privacy settings ensure the confidentiality of consumer and employee information by following relevant data protection laws [57]. Establishing trustworthy monitoring and logging systems is another use for monitoring and logging, as well as for identifying and addressing security incidents. Secure

communication is expected in business communications with managements [9], [10]. Encrypted communication protocols, such as HTTPS and Mobile Device Management (MDM), are used while sending data over the internet. Employers can better secure and manage employee mobile devices by implementing MDM programs [11], [12].

2.3. *Chatbots of Software protection*

Chatbots of software protection are the long-term viability and effectiveness of measures implemented to stop software from unauthorized access, copying, modification, or dissemination. Chatbots for software protection are essential for software developers and organizations to secure their intellectual property, ensure income streams, and maintain the integrity of their products [13], [14]. A multitude of factors need to be considered while assessing the academic performance of the students. Software protection measures require constant updates in order to keep chatbots safe from evolving threats and vulnerabilities [20], [21], [1]. To keep software secure, patches and updates have to be made and made available whenever new security flaws are discovered in it [15], [16]. One of the most crucial components of software protection is strong encryption. Encryption must be kept strong and up to date in order to maintain software security. Effective licensing and activation processes help prevent software distribution and unlawful use. These systems can function more effectively and adapt to changing circumstances if they are updated. Code obfuscation: When using obfuscation techniques, attackers may find it more difficult to decode and understand the software's source code. It is imperative to regularly improve and update obfuscation strategies. Cryptographic keys are the foundation of Safe Key Management, and other security credentials need to be treated with caution. Adhering to best practices and using chatbots with the most recent key management systems is essential, as outdated key management can lead to risks. One anti-piracy tool that can be used to stop illegal software distribution and copying is digital rights management (DRM) [17]–[19]. These safeguards against chatbots ahead of pirate tactics need to be improved over time. User education, which informs consumers about the benefits of using licensed software and the risks associated with using cracked or pirated versions, is a crucial strategy for promoting chatbots. Furthermore, bringing software pirates and counterfeiters to justice through legal enforcement can act as a deterrence [22]–[24]. This strategy requires ongoing effort to identify and address infringement. Several cybersecurity experts that we spoke with disclosed that their companies work with security experts. This aids in keeping defenses up to date with the most recent threats, and it may be accomplished by working with cybersecurity professionals and groups that specialize in software protection. Another method for protecting chatbot software is Redundancy and Defence in Depth. Chatbots can be made better by stacking security measures or using defense in depth. Combining various security methods makes it more difficult for attackers to hack software. Regular vulnerability evaluations and security audits are also conducted, and these resources can help identify chatbots research and expedite the resolution of software protection vulnerabilities [1].

3. METHODOLOGY

Data for this research project were gathered from both primary and secondary sources. Primary data is gathered via customer surveys, while secondary data is gathered from pertinent articles found in various sources. A survey using a quantitative approach and a sample size of 50 students is used to collect the primary data.

Geographical differences are the basis for the research gap that the literature assessment revealed. The studies reported in the research publications on this subject were conducted in various nations. Because each respondent country has a unique set of issues, the research findings of this study may differ. The study's conclusions will eventually demonstrate how chatbots and other independent factors have affected the accessibility of metadata information.

The primary objective of the study is to comprehend how chatbots affect metadata access and the potential risks associated with inadequate cybersecurity while accessing metadata databases. Survey participants and a review of the literature served as the data sources. The analysis of various elements that could jeopardize metadata security will be aided by these data sources.

5. DATA ANALYSIS AND FINDINGS

Fifteen out of fifty firms, or thirty percent of them, reported using a combination of their prior awareness. Thirty-five firms, or seventy percent of the sample, are the chatbots' users. They use incident response and monitoring systems. They ensure that security breaches may be quickly corrected by putting in place incident response protocols and monitoring systems to spot unauthorized access or manipulation. Legally and regulatorily, these 50% of firms are compliant. Their goal is to concentrate on the long-term protection of chatbot software, which is contingent upon compliance with relevant rules and regulations, including those pertaining to copyright and intellectual property rights. Bug reports and user comments are also included. Potential risks can be addressed and security measures can be strengthened by encouraging users to disclose bugs and vulnerabilities in the software. Chatbot software protection is an ongoing activity that necessitates monitoring chatbots and adapting to new threats and developments in technology. Over time, software developers and organizations need to invest in security and protection measures to safeguard their products and intellectual property. An open-ended survey was distributed to the 50 cybersecurity specialists with the aim of examining the best approaches to safeguard chatbot software in chatbot companies that face the risk of chatbot research while taking into consideration their current cybersecurity procedures. Using robust encryption is one recommendation for safeguarding sensitive data in companies. It was looked into how to apply strong encryption approaches by routinely patching and updating encryption libraries in order to address security issues. Among the encryptions that were assessed in our investigation were three chatbot results:

Secure Development Lifecycle (SDLC) 1. 1. The Secure Development Lifecycle (SDLC) is a highly recommended tool for businesses to use when operations managers design the life cycles of their products and services. The results of the open-ended questionnaires show that the SDLC improves students' academic achievement in businesses where chatbots are a risk. Coding and testing are two stages of the software development lifecycle that can be used to plan and construct the SDLC and identify the degradation of cybersecurity systems when they are no longer in place.

2. Threat Modeling: No impact on the pupils' academic performance was seen in the open-ended questionnaires. It's probable that certain security risks and software bugs won't be able to recognize every piece of chatbot research included in the threat modeling.

3. Installing robot monitoring mechanisms: The foundation of chatbot cybersecurity systems is a marked improvement in students' academic performance. The results of the open-ended survey show that businesses may discover and fix chatbot security issues in real-time by using robotics monitoring techniques, even in situations where built-in applied cybersecurity solutions are unable to do so.

6. CONCLUSION

Businesses use a variety of policies, procedures, and safeguards to guard their software and data from internet threats, such as chatbots. This is how best practices in cybersecurity are applied. Chatbots for software protection will remain stable as long as system and software security mechanisms are strong and function properly over time. software defense Chatbots concentrate on a system's capacity to resist changing attacks and gradually adjust to them. Artificial intelligence research is examined in this study's setting as a moderator to examine the effects of malevolent actors using AI and machine learning to execute highly proficient and automated cyberattacks. Chatbot defenses are particularly difficult due of the rapid expansion and versatility of these chatbot-driven threats. Complex Interaction shows that depending on the particular security measures implemented by organizations, the capabilities of the metadata, and other external circumstances, the interaction between chatbot research and organizations may be more complex. Ongoing upgrading is necessary to stay current with the latest security best practices and emerging threats. When new vulnerabilities surface, it's critical to implement robotics monitoring techniques and security lifecycles as chatbot software protection strategies. Software protection necessitates ongoing vigilance and a dedication to security. To ensure the software's long-term safety in enterprises, cybersecurity specialists must establish a security-conscious culture inside the development teams and organizational procedures.

REFERENCES

[1] S. Khadragy *et al.*, "Predicting Diabetes in United Arab Emirates Healthcare: Artificial Intelligence and Data Mining Case Study," *South East. Eur. J. Public Heal.*, vol. 5, 2022, doi: https://doi.org/10.56801/seejph.vi.406.

[2] M. Salameh *et al.*, "The Impact of Project Management Office's Role on Knowledge Management: A Systematic Review Study," *Comput. Integr. Manuf. Syst.*, vol. 28, no. 12, pp. 846–863, 2022, doi: 10.24297/j.cims.2022.12.59.

[3] F. Shwedeh *et al.*, "SMEs' Innovativeness and Technology Adoption as Downsizing Strategies during COVID-19: The Moderating Role of Financial Sustainability in the Tourism Industry Using Structural Equation Modelling," *Sustainability*, vol. 14, no. 23, p. 16044, 2022, doi: https://doi.org/10.3390/su142316044.

[4] S. Salloum *et al.*, "Understanding and Forecasting Chatbot Adoption: An SEM-ANN Methodology," *Migr. Lett.*, vol. 20, no. S11, pp. 652–668, 2023, doi: https://doi.org/10.59670/ml.v20iS11.5717.

[5] F. Shwedeh, "THE IMPACT OF SMART CITY POLICY TIMELINESS AND TECHNOLOGY READINESS ON SMART CITY PERFORMANCE IN DUBAI: THE MODERATING EFFECT OF FINANCIAL AVAILABILITY," 2021.

[6] R. Ravikumar *et al.*, "The Impact of Big Data Quality Analytics on Knowledge Management in Healthcare Institutions: Lessons Learned from Big Data's Application within The Healthcare Sector," *South East. Eur. J. Public Heal.*, vol. 5, 2023, doi: https://doi.org/10.56801/seejph.vi.309.

[7] F. Shwedeh, A. Aburayya, and M. Mansour, "The Impact of Organizational Digital Transformation on Employee Performance: A Study in the UAE," *Migr. Lett.*, vol. 20, no. S10, pp. 1260–1274, 2023, doi: https://doi.org/10.59670/ml.v20iS10.5710.

[8] B. M. Dahu *et al.*, "The Impact of COVID-19 Lockdowns on Air Quality: A Systematic Review Study," *South East. Eur. J. Public Heal.*, vol. 5, 2022, doi: https://doi.org/10.11576/seejph-5929.

[9] M. Alkashami *et al.*, "AI different approaches and ANFIS data mining: A novel approach to predicting early employment readiness in middle eastern nations," *Int. J. Data Netw. Sci.*, vol. 7, no. 3, pp. 1267–1282, 2023, doi: 10.5267/j.ijdns.2023.4.011.

[10] R. Ravikumar *et al.*, "Impact of knowledge sharing on knowledge Acquisition among Higher Education Employees," *Comput. Integr. Manuf. Syst.*, vol. 28, no. 12, pp. 827–845, 2022, doi: 10.24297/j.cims.2022.12.58.

[11] F. Shwedeh, N. Hami, S. Z. Abu Bakar, F. M. Yamin, and A. Anuar, "The Relationship between Technology Readiness and Smart City Performance in Dubai," *J. Adv. Res. Appl. Sci. Eng. Technol.*, vol. 29, no. 1, pp. 1–12, 2022, doi: https://doi.org/10.37934/araset.29.1.112.

[12] F. Shwedeh, S. Malaka, and B. Rwashdeh, "The Moderation Effect of Artificial Intelligent Hackers on the Relationship between Cyber Security Conducts and the Sustainability of Software Protection: A Comprehensive Review," *Migr. Lett.*, vol. 20, no. S9, pp. 1066–1072, 2023, doi: 10.59670/ml.v20iS9.4947.

[13] S. A. Alimour *et al.*, "The quality traits of artificial intelligence operations in predicting mental healthcare professionals' perceptions: A case study in the psychotherapy division," *J. Auton. Intell.*, vol. 7, no. 4, 2024, doi: 10.32629/jai.v7i4.1438.

[14] F. Shwedeh, N. Hami, and S. Z. Abu Baker, "Effect of leadership style on policy timeliness and performance of smart city in Dubai: a review," in *Proceedings of the International Conference on Industrial Engineering and Operations Management Dubai, UAE, March 10-12, 2020*, 2020, pp. 917–922.

[15] A. Aburayya *et al.*, "SEM-machine learning-based model for perusing the adoption of metaverse in higher education in UAE.," *Int. J. Data Netw. Sci.*, vol. 7, no. 2, pp. 667–676, 2023, doi: 10.5267/j.ijdns.2023.3.005.

[16] F. Shwedeh, T. Aldabbagh, A. Aburayya, and H. Uppilappatta, "The Impact of Harnessing Total Quality Management Studies on the Performance of Smart Applications: A Study in Public and Private Sectors in the UAE," *Migr. Lett.*, vol. 20, no. S11, pp. 934–959, 2023, doi: https://doi.org/10.59670/ml.v20iS11.5892.

[17] F. Shwedeh, "Harnessing digital issue in adopting metaverse technology in higher education institutions: Evidence from the United Arab Emirates," *Int. J. Data Netw. Sci.*, vol. 8, no. 1, pp. 489–504, 2024, doi: 10.5267/j.ijdns.2023.9.007.

[18] S. Khadragy *et al.*, "Predicting Diabetes in United Arab Emirates Healthcare: Artificial Intelligence and Data Mining Case Study," *South East. Eur. J. Public Heal.*, vol. 5, 2022, doi: https://doi.org/10.56801/seejph.vi.406.

[19] N. Yas, M. N. I. Elyat, M. Saeed, F. Shwedeh, and S. Lootah, "The Impact of Intellectual Property Rights and the Work Environment on Information Security in the United Arab Emirates," *Kurd. Stud.*, vol. 12, no. 1, pp. 3931–3948, 2024, doi: 10.58262/ks.v12i1.282.

[20] F. Shwedeh *et al.*, "Entrepreneurial innovation among international students in the UAE: Differential role of entrepreneurial education using SEM analysis," *Int. J. Innov. Res. Sci. Stud.*, vol. 6, no. 2, pp. 266–280, 2023, doi: https://doi.org/10.53894/ijirss.v6i2.1328.

[21] A. El Nokiti, K. Shaalan1, S. Salloum2, A. Aburayya, F. Shwedeh, and B. Shameem3, "Is Blockchain the answer? A qualitative Study on how Blockchain Technology Could be used in the Education Sector to Improve the Quality of Education Services and the Overall Student Experience," *Comput. Integr. Manuf. Syst.*, vol. 28, no. 11, pp. 543–556, 2022, doi: 10.24297/j.cims.2022.11.039.

[22] S. Abdallah *et al.*, "A COVID19 Quality Prediction Model based on IBM Watson Machine Learning and Artificial Intelligence Experiment," *Comput. Integr. Manuf. Syst.*, vol. 28, no. 11, pp. 499–518, 2022, doi: 10.24297/j.cims.2022.11.037.

[23] F. Shwedeh, N. Hami, and S. Z. Abu Bakar, "Dubai smart city and residence happiness: A conceptual study," *Ann. Rom. Soc. Cell Biol.*, vol. 25, no. 1, pp. 7214–7222, 2021.

[24] S. Salloum *et al.*, "Sustainability Model for the Continuous Intention to Use Metaverse Technology in Higher Education: A Case Study from Oman," *Sustainability*, vol. 15, no. 6, p. 5257, 2023, doi: 10.3390/su15065257.

[25] B. Li, S. Mousa, J. R. R. Reinoso, H. M. Alzoubi, A. Ali, and A. D. Hoang, "The role of technology innovation, customer retention and business continuity on firm performance after post-pandemic era in China's SMEs," *Econ. Anal. Policy*, vol. 78, pp. 1209–1220, 2023, doi: 10.1016/j.eap.2023.05.004.

[26] Q. Hassan *et al.*, "The renewable energy role in the global energy Transformations," *Renew. Energy Focus*, vol. 48, p. 100545, 2024, doi: https://doi.org/10.1016/j.ref.2024.100545.

[27] A. A, A. M. A, and et al. Al Ayadeh I, "Evolving a hybrid appointment system for patient scheduling in primary healthcare centres in Dubai: Perceptions of patients and healthcare provider.," *Int. J. Emerg. Technol.*, vol. 11, no. 2, pp. 251–260, 2020.

[28] A. A. Alsharhan A, Salloum SA, "Technology acceptance drivers for AR smart glasses in the middle east: A quantitative study. International Journal of Data and Network Science. : 193-208. doi:," *10.5267/j.ijdns.2021.9.008*, vol. 6, no. 1, 2022, doi: 10.5267/j.ijdns.2021.9.008.

[29] S. S. Almarzouqi A, Aburayya A, "Determinants predicting the electronic medical record adoption in healthcare: A SEM-Artificial Neural Network approach. Haldorai A, ed. PLOS ONE," vol. 17, no. 8, 2022, doi: 10.1371/journal.pone.0272735y.

[30] A. A, A. D, and T. M, "Aburayya A, Alawadhi D, Taryam M. A conceptual framework for implementing TQM in the primary healthcare centers and examining its impact on patient satisfaction. Research.," *Int. J. Adv. Res.*, vol. 7, no. 3, pp. 1047–1065, 2019.

[31] A. Aburayya, D. Alawadhi, and M. Taryam, "A conceptual framework for implementing TQM in the primary healthcare centers and examining its impact on patient satisfaction," *Int. J. Adv. Res.*, vol. 7, no. 3, pp. 1047–1065, 2019, doi: 10.21474/IJAR01/8735.

[32] H. Yousuf, S. Salloum, A. Aburayya, M. Al-Emran, and K. Shaalan, "A systematic review of CRYPTDB: Implementation, challenges, and future opportunities," *J. Manag. Inf. Decis. Sci.*, vol. 24, no. Special Issue 1, pp. 1–16, 2021.

[33] R. Abousamra *et al.*, "Predicting the Intention to Use Google Glass in the Educational Projects: A Hybrid SEM-ML Approach," *Acad. Strateg. Manag. J*, vol. 21, no. S6, pp. 1–13, 2022.

[34] K. Liu *et al.*, "Exploring the Nexus between Fintech, natural resources, urbanization, and environment sustainability in China: A QARDL study," *Resour. Policy*, vol. 89, p. 104557, 2024, doi: 10.1016/j.resourpol.2023.104557.

[35] S. R. AlSuwaidi, M. Alshurideh, B. Al Kurdi, and A. Aburayya, "The main catalysts for collaborave R&D projects in Dubai industrial sector.," in *The Internaonal Conference on Arficial Intelligence and Computer Vision*, 2021, pp. 795–806.

[36] M. Taryam *et al.*, "(2021). The impact of the covid-19 pandemic on the mental health status of healthcare providers in the primary health care sector in Dubai.," *Linguist. Antverp.*, vol. 21, no. 2, pp. 2995–3015, 2021.

[37] R. S. Al-Maroof, K. Alhumaid, A. Q. Alhamad, A. Aburayya, and S. Salloum, "User acceptance of smart watch for medical purposes: an empirical study.," *Futur. Internet*, vol. 13, no. 5, p. 127, 2021, doi: https://doi.org/10.3390/fi13050127.

[38] M. Alawadhi *et al.*, "Factors affec?ng medical students' acceptance of the metaverse system in medical training in the United Arab Emirates.," *South East. Eur. J. Public Heal.*, no. Special Volume No. 5, 2022, doi: 10.11576/seejph-5759.

[39] E. MOUZAEK, N. ALAALI, S. A. I. D. SALLOUM, and A. ABURAYYA, "An empirical investigation of the impact of service quality dimensions on guests satisfaction: A case study of Dubai Hotels," *J. Contemp. Issues Bus. Gov.*, vol. 27, no. 3, pp. 1186–1199, 2021, doi: 10.47750/cibg.2021.27.03.160.

[40] S. Aljasmi *et al.*, "The Impact of Hospital Demographic Factors on Total Quality Management Implementation: A Case Study of UAE Hospitals," *South East. Eur. J. Public Heal.*, vol. Special Vo, pp. 1–13, 2022, doi: 10.11576/seejph-5758.

[41] K. Alaboud *et al.*, "The Quality Application of Deep Learning in Clinical Outcome Predictions Using Electronic Health Record Data: A Systematic Review," *South East. Eur. J. Public Heal.*, vol. Volume XXI, pp. 09–23, 2023.

[42] A. Almarzouqi, A. Aburayya, and S. A. Salloum, "Determinants predicting the electronic medical record adoption in healthcare: A SEM-Artificial Neural Network approach," *PLoS One*, vol. 17, no. 8, p. e0272735, 2022, doi: 10.1371/journal.pone.0272735.

[43] A. Alsharhan, S. A. Salloum, and A. Aburayya, "Using e-learning factors to predict student performance in the practice of precision education," *Pt. 2 J. Leg. Ethical Regul. Isses*, vol. 24, no. Special Issue 6, p. 1, 2021.

[44] S. A. Salloum *et al.*, "Novel machine learning based approach for analysing the adoption of metaverse in medical training: A UAE case study," *Informatics Med. Unlocked*, vol. 42, p. 101354, 2023, doi: 10.1016/j.imu.2023.101354.

[45] A. Aburayya, A. Marzouqi, I. Iyadeh, A. Albqaeen, and S. Mubarak, "Evolving a Hybrid Appointment System for Patient scheduling in Primary Healthcare Centres in Dubai : Perceptions of Patients and Healthcare Providers," *Int. J. Emerg. Technol.*, vol. 11, no. 2, pp. 251–260, 2020, doi: https://d1wqtxts1xzle7.cloudfront.net/63548291/Evolving_a_Hybrid_Appointment_System_for_Patient_Scheduling_in_Primary_Healthcare_Centres_in_Dubai_Perce20200606-109135-jr0twj-libre.pdf?1591473666=&response-content-disposition=inline%3B+filename%3DEvolving_a_Hybrid_Appointment_System_for.pdf&Expires=1706534986&Signature=fseyo0TYWnISW0FY7G-RRIPvulgk3Nhl4GQy1MX4ui1KaP0gqqbdiXNK3Sr8lR9-4VLiREFosotAVq6iUMrQJR~uTD4SmuHD0HTciDTyJckgxu9fKEGEtEom~kuTiXbsP5sdqvyKot6GYo4cc-zXYnV8ADfj~fMJH~r9QBmeUoETJKaJfuAa.

[46] I. Shahin, A. B. Nassif, A. Elnagar, S. Gamal, S. A.

Salloum, and A. Aburayya, "NEUROFEEDBACK INTERVENTIONS FOR SPEECH AND LANGUAGE IMPAIRMENT: A SYSTEMATIC REVIEW," *J. Manag. Inf. Decis. Sci.*, vol. 24, no. Special Issue 1, pp. 1–30, 2021.

[47] A. Alsharhan, S. Salloum, and A. Aburayya, "Technology acceptance drivers for AR smart glasses in the middle east: A quantitative study," *Int. J. Data Netw. Sci.*, vol. 6, no. 1, pp. 193–208, 2022, doi: 10.5267/j.ijdns.2021.9.008.

[48] I. Al Eideh *et al.*, "Examination of the Effect of TQM Implementation on Innovation Performance: An Assessment Study In the UAE Healthcare Sector," *Acad. Strateg. Manag. J.*, vol. 21, no. Special Isuue 4, pp. 1–17, 2022.

[49] B. M. Dahu, S. Khan, A. A. Salman, Y. M. Andraws, A. Abo Daken, and A. Aburayya, "Epidemiological Analysis of Vaccination Strategies and Demographic Patterns In COVID-19 Cases in The Midwest Region of The United States," *Natl. J. Community Med.*, vol. 14, no. 1, pp. 62–71, 2024, doi: 10.55489/njcm.150120243461.

[50] S. A. Salloum, N. M. N. AlAhbabi, M. Habes, A. Aburayya, and I. Akour, "Predicting the Intention to Use Social Media Sites: A Hybrid SEM-Machine Learning Approach," in *Advanced Machine Learning Technologies and Applications: Proceedings of AMLTA 2021*, Springer International Publishing, 2021, pp. 324–334.

[51] R. S. Al-Maroof, K. Alhumaid, A. Q. Alhamad, A. Aburayya, and S. Salloum, "User acceptance of smart watch for medical purposes: an empirical study," *Futur. Internet*, vol. 13, no. 5, p. 127, 2021.

[52] A. Almarzouqi, A. Aburayya, and S. A. Salloum, "Determinants of intention to use medical smartwatch-based dual-stage SEM-ANN analysis," *Informatics Med. Unlocked*, vol. 28, pp. 1–12, 2022, doi: 10.1016/j.imu.2022.100859.

[53] A. Jasri, S. Aljasmi, and A. Aburayya, "Employing PLS-SEM Analysis to Examine the Mediation Role of Artificial Intelligence in Physician Experience. An Empirical Study of the Effect of the Medical Smartwatch on Physician Satisfaction," *South East. Eur. J. Public Heal.*, vol. Special Vo, 2022, doi: https://doi.org/10.56801/seejph.vi.407.

[54] M. A. Almaiah *et al.*, "Factors affecting the adoption of digital information technologies in higher education: An empirical study," *Electronics*, vol. 11, no. 21, p. 3572, 2022, doi: 10.3390/electronics11213572.

[55] M. Taryam *et al.*, "Factors Affecting the Uptake of COVID-19 Vaccine among Dubai Airport's Professionals," *South East. Eur. J. Public Heal.*, vol. 17, no. 2, pp. 1–14, 2022, doi: https://doi.org/10.11576/seejph-5091.

[56] C. Leng *et al.*, "An empirical assessment of the effect of natural resources and financial technologies on sustainable development in resource abundant developing countries: Evidence using MMQR estimation," *Resour. Policy*, vol. 89, p. 104555, 2024, doi: 10.1016/j.resourpol.2023.104555.

[57] F. Bu, H. wu, H. A. Mahmoud, H. M. Alzoubi, N. K. Ramazanovna, and Y. Gao, "Do financial inclusion, natural resources and urbanization affect the sustainable environment in emerging economies," *Resour. Policy*, vol. 87, p. 104292, 2023, doi: 10.1016/j.resourpol.2023.104292.