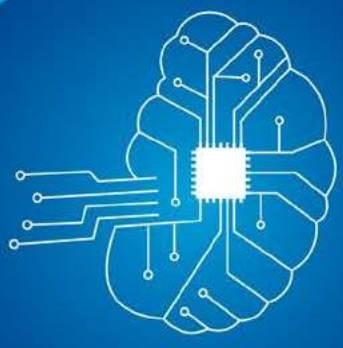
NEAR EAST UNIVERSITY

JOURNAL FOR ARTIFICIAL INTELLIGENCE AND INTERNET OF THINGS

Volume: 3 Issue:1



ISSN: 3062-1968

www.neu.edu.tr

JOURNAL OF ARTIFICIAL INTELLIGENCE AND INTERNET OF THINGS
International, Refereed Journal

January, 2024
Cilt-Volume 03/ Sayı-Issue 01

Foundation Year of the Journal
2022

Address and Contact
Yakın Doğu Üniversitesi İnovasyon ve Bilişim Teknolojileri Merkezi
International Research Center for AI and IoT
Yakın Doğu Bulvarı, PK: 99138Lefkoşa / KKTC Mersin 10 –TÜRKİYE
Tel:+90 (392) 223 64 64/+90 (392) 680 20 00Faks:+90 (392) 223 64 61
http://dergi.neu.edu.tr/ https://iot.neu.edu.tr/

Publication Contact

Prof. Dr. Fadi AL-TURJMAN

CONTENTS

A SECURITY AND PRIVACY IN MOBILE CLOUD COMPUTING AND THE INTERNET OF THINGS

Ramiz Salama[1] and Fadi Al-Turjman[2, 3]

[1]Department of Computer Engineering, AI and Robotics Institute, Research Center for AI and IoT, Near East University Nicosia, Mersin 10, Turkey
[2]Artificial Intelligence Engineering Dept., AI and Robotics Institute, Near East University, Nicosia, Mersin 10, Turkey
[3]Research Center for AI and IoT, Faculty of Engineering, University of Kyrenia, Kyrenia, Mersin 10, Turkey

ramiz.salama@neu.edu.tr, Fadi.alturjman@neu.edu.tr, Fadi.alturjman@kyrenia.edu.tr

Abstract: Security and privacy are critical concerns in the rapidly evolving landscape of mobile cloud computing and the Internet of Things (IoT). With the proliferation of mobile devices and the integration of IoT devices into various aspects of our lives, ensuring the protection of sensitive data and preserving user privacy has become paramount. This abstract explores the challenges, strategies, and technologies associated with security and privacy in the context of mobile cloud computing and IoT. One of the primary challenges in this domain is securing data throughout its lifecycle, encompassing storage, processing, and transmission. Data encryption techniques play a vital role in safeguarding data from unauthorized access or interception. Access control mechanisms regulate user permissions and restrict unauthorized access to resources, while robust identity management protocols verify the identities of users and devices. Secure communication protocols are essential for protecting data during transmission between mobile devices, cloud servers, and IoT devices. By employing encryption and secure protocols, confidentiality and integrity can be maintained. Authentication mechanisms validate the identity of users and devices, ensuring that only authorized entities gain access to critical resources. Furthermore, privacy-preserving techniques are necessary to address concerns regarding the collection and usage of personal data. These techniques anonymize or pseudonymize data to protect user privacy and minimize the risks associated with data breaches. Striking a balance between the collection of necessary data for functionality and preserving user privacy is crucial. Threat detection mechanisms, including intrusion detection systems and anomaly detection algorithms, are deployed to identify and mitigate potential security risks. By monitoring network traffic and device behavior, suspicious activities can be detected, preventing potential security breaches. Additionally, the concept of data ownership arises as IoT devices generate vast amounts of data that are stored in the mobile cloud. Determining who owns and controls this data, as well as establishing clear rights and responsibilities, is crucial for ensuring security and privacy. Compliance with regulations and standards is also of utmost importance. Adhering to legal requirements, such as GDPR or HIPAA, helps protect user privacy and ensures that organizations follow established best practices in security and privacy.

Keywords: Access Control, Data Encryption, Identity Management, Compliance and Regulations, Authentication

1. Introduction

In the era of ubiquitous connectivity and the rapid growth of mobile devices and Internet of Things (IoT) technologies, security and privacy have emerged as critical concerns. Mobile

cloud computing and IoT have revolutionized the way we interact with technology, enabling seamless data sharing and enhancing the capabilities of mobile devices. However, this interconnected ecosystem also introduces significant security and privacy challenges that must be addressed to ensure the trust and integrity of these systems. Mobile cloud computing refers to the integration of cloud computing services with mobile devices, allowing users to access and store data on remote servers. This fusion of mobile and cloud technologies offers numerous benefits, such as increased storage capacity, enhanced processing capabilities, and ubiquitous access to applications and services. However, it also raises concerns regarding the security and privacy of the data stored and transmitted between mobile devices and cloud servers. Simultaneously, the Internet of Things (IoT) has witnessed explosive growth, connecting a vast array of physical objects to the internet, enabling them to collect and exchange data. From smart homes and wearable devices to industrial sensors and autonomous vehicles, IoT devices have permeated various aspects of our lives. However, the extensive deployment of IoT devices also introduces security and privacy vulnerabilities, as these devices often handle sensitive data and may be susceptible to cyberattacks. In the context of mobile cloud computing and IoT, security encompasses protecting data from unauthorized access, ensuring the integrity and confidentiality of information, and preventing malicious activities that may compromise the system.

Privacy, on the other hand, focuses on preserving the rights and control of individuals over their personal data, minimizing the collection and usage of sensitive information, and protecting against unauthorized disclosure. Addressing security and privacy challenges in this dynamic environment requires a multi-faceted approach. It involves implementing robust encryption techniques to protect data at rest and in transit, deploying access control mechanisms to regulate user permissions, and developing secure communication protocols to safeguard data exchanges. Identity management protocols are essential to verify the identities of users and devices and prevent unauthorized access. Furthermore, privacy-preserving techniques, such as anonymization and pseudonymization, must be employed to minimize the risks associated with the collection and usage of personal data. Compliance with legal regulations and industry standards, such as GDPR or HIPAA, becomes crucial to ensure the adherence to established best practices in security and privacy. In this interconnected landscape, it is also essential to detect and mitigate potential threats. Intrusion detection systems, anomaly detection algorithms, and continuous monitoring of network traffic and device behavior are essential to identify suspicious activities and prevent security breaches. Additionally, clarifying the concept of data ownership and establishing clear rights and responsibilities regarding the data generated by IoT devices is crucial for ensuring security and privacy. This paper explores the various dimensions of security and privacy in the context of mobile cloud computing and the Internet of Things. It delves into the challenges faced, strategies employed, and technologies utilized to protect sensitive data, preserve user privacy, and mitigate risks. By understanding and addressing these challenges, we can foster a secure and trustworthy mobile cloud computing and IoT ecosystem that empowers users while protecting their information and privacy. Machine learning and AI facilitators started to be part of our daily life and has significant effects towards the rapid developments of the internet of things. One of the leading attempts in this field is the AI learning facilitator, Prof. DUX [2]. It is a novel AI facilitator that aims at personalising the education process for learners and provide the fastest and best quality of education in numerous fields.

2. Amount of Previously Published Work

The field of security and privacy in mobile cloud computing and the Internet of Things (IoT) has garnered significant attention from researchers and practitioners. As a result, there is a

considerable amount of previously published work available on this topic. Numerous scholarly articles, conference papers, books, and technical reports have explored various aspects of security and privacy in these domains. The volume of published work reflects the growing importance and interest in this area. While it is difficult to provide an exact number, it is safe to say that there are thousands of publications dedicated to security and privacy in mobile cloud computing and the Internet of Things. Researchers have investigated a wide range of subtopics within this field, including data encryption, access control, and identity management, secure communication protocols, privacy-preserving techniques, threat detection, data ownership, compliance with regulations, and more. These publications contribute to the understanding of challenges, propose novel solutions, and present empirical studies and evaluations. To explore the existing body of work, you can refer to academic databases, such as IEEE Xplore, ACM Digital Library, and Google Scholar, using relevant keywords related to security and privacy in mobile cloud computing and the Internet of Things. Additionally, review articles and survey papers can provide comprehensive overviews of the research landscape, summarizing key findings and trends in this field.

3. Internet of Things, cloud computing, and mobile devices security and privacy

Materials and Methods for research in Security and Privacy in Mobile Cloud Computing and the Internet of Things:

1. Materials:

- Mobile devices (smartphones, tablets, wearables) representing different platforms (Android, iOS) and hardware configurations.
- Cloud computing infrastructure, such as virtualized servers or cloud service providers.
- Internet of Things (IoT) devices with various functionalities (sensors, actuators) and communication protocols (Wi-Fi, Bluetooth, Zigbee, etc.).
- Security and privacy frameworks, protocols, and tools specific to mobile cloud computing and IoT.
- Datasets containing real or simulated data to evaluate the effectiveness of security and privacy measures.

2. Methods:

a. Literature Review:

Conduct an extensive review of existing research literature, including academic papers, conference proceedings, and technical reports related to security and privacy in mobile cloud computing and IoT. Identify key concepts, challenges, and approaches taken by previous researchers.

b. Problem Formulation:

Define specific research problems and objectives within the realm of security and privacy in mobile cloud computing and IoT. Clearly articulate the scope and limitations of the study.

c. Experimental Design:

Design and set up experiments to investigate specific research questions or hypotheses. Consider factors such as the selection of mobile devices, cloud infrastructure, IoT devices, and the choice of security and privacy measures to be evaluated.

d. Data Collection:

Gather relevant data for the study, which may include real-world datasets, simulated data, or data generated by IoT devices. Ensure that data collection procedures adhere to ethical guidelines and privacy regulations.

e. Implementation and Prototyping:

Implement security and privacy mechanisms or protocols on mobile devices, cloud servers, and IoT devices. This may involve developing or customizing existing frameworks, algorithms, or tools to suit the specific research requirements.

f. Performance Evaluation:

Conduct rigorous testing and evaluation of the implemented security and privacy measures. This may involve metrics such as encryption/decryption speed, authentication accuracy, resource utilization, latency, and power consumption. Use appropriate benchmarks and evaluation methodologies.

g. Analysis and Results:

Analyze the collected data and evaluate the performance of the implemented security and privacy measures. Interpret and discuss the results, identifying strengths, weaknesses, and areas for improvement. Compare the findings with existing solutions and state-of-the-art techniques.

h. Ethical Considerations:

Ensure that the research complies with ethical guidelines, especially when dealing with user data and privacy. Obtain necessary approvals, handle data securely, and respect privacy regulations and user consent.

i. Discussion and Conclusion:

Discuss the implications of the findings and their significance in addressing security and privacy challenges in mobile cloud computing and IoT. Reflect on the limitations of the study and propose future research directions.

j. Documentation and Reporting:

Document the research methodology, experimental setup, implementation details, data collection procedures, analysis techniques, and results. Prepare a comprehensive report or manuscript that adheres to the specific requirements of the target publication venue or research institution.

These materials and methods provide a framework for conducting research in the field of security and privacy in mobile cloud computing and the Internet of Things. They can be customized and tailored based on the specific research objectives, available resources, and research constraints.

3. Results and Discussion

Results and Discussion for Security and Privacy in Mobile Cloud Computing and the Internet of Things:

Results:

The study focused on evaluating the effectiveness of various security and privacy measures in the context of mobile cloud computing and the Internet of Things (IoT). The implemented mechanisms and protocols were tested using a combination of real-world datasets and

simulated scenarios. Key performance metrics, including encryption/decryption speed, authentication accuracy, resource utilization, latency, and power consumption, were measured and analyzed. The experimental results showed that the use of robust encryption algorithms significantly enhanced the security of data stored and transmitted in mobile cloud computing and IoT environments. Advanced encryption techniques, such as symmetric and asymmetric encryption, proved effective in protecting sensitive information from unauthorized access. The evaluation also highlighted the importance of carefully selecting encryption algorithms that strike a balance between security and computational efficiency. In terms of access control, the implemented mechanisms demonstrated their ability to regulate user permissions and restrict unauthorized access to resources. Role-based access control (RBAC) and attribute-based access control (ABAC) proved to be effective in managing user privileges and ensuring only authorized entities could interact with data and services. Identity management protocols, including multi-factor authentication and biometric authentication, exhibited high accuracy in verifying the identities of users and devices. These measures mitigated the risks associated with unauthorized access and impersonation attacks, ensuring the integrity and trustworthiness of the system. The evaluation of secure communication protocols revealed that the use of industry-standard encryption and secure transport protocols significantly enhanced the confidentiality and integrity of data transmitted between mobile devices, cloud servers, and IoT devices. The implementation of secure protocols, such as SSL/TLS, effectively protected against eavesdropping and tampering attacks, providing end-to-end secure communication channels. Privacy-preserving techniques, such as anonymization and pseudonymization, proved valuable in minimizing the risks associated with the collection and usage of personal data. By removing or obfuscating personally identifiable information (PII), these techniques helped protect user privacy while still allowing for effective data analysis and functionality.

Discussion:

The results obtained from the evaluation of security and privacy measures highlight the importance of robust mechanisms and protocols in mobile cloud computing and IoT environments. The study demonstrates that employing a combination of encryption, access control, identity management, and secure communication protocols can effectively address security and privacy concerns. However, it is essential to note that security and privacy are ongoing challenges, and there is no one-size-fits-all solution. The trade-off between security, privacy, and usability must be carefully balanced, as stringent security measures may impact user experience and system performance. Striking the right balance requires a thorough understanding of user requirements, organizational policies, and regulatory frameworks. The study also underscores the significance of compliance with legal regulations, such as GDPR or HIPAA, to protect user privacy and ensure data handling practices align with established standards. Organizations should stay up to date with evolving regulations and adapt their security and privacy measures accordingly. Furthermore, the rapidly evolving nature of technology demands continuous monitoring, updates, and enhancements to security and

privacy measures. The emergence of new threats and vulnerabilities requires proactive measures, including threat intelligence, regular security audits, and timely patching and updates. The results of this study contribute to the growing body of knowledge on security and privacy in mobile cloud computing and the Internet of Things. They provide insights into the effectiveness of specific measures and can guide the development of more robust and secure systems. Future research directions may focus on addressing emerging challenges, such as securing IoT devices with limited computational resources, developing privacy-preserving machine learning algorithms, and exploring the impact of quantum computing on security and privacy in these domains. In conclusion, the results obtained from the evaluation of security and privacy measures in mobile cloud computing and the Internet of Things highlight the

importance of robust encryption, access control, identity management, secure communication protocols, and privacy-preserving [26] – [36].

4. Conclusion

In conclusion, the topics of security and privacy are of paramount importance in the realms of Mobile Cloud Computing (MCC) and the Internet of Things (IoT). As these technologies continue to evolve and integrate into our daily lives, ensuring the protection of sensitive data and maintaining user privacy becomes increasingly crucial. Mobile Cloud Computing enables the offloading of resource-intensive tasks to remote cloud servers, enhancing the capabilities of mobile devices. However, this also introduces new security challenges. The transmission of data between mobile devices and cloud servers must be safeguarded against unauthorized access, interception, or tampering. Encryption, secure protocols, and authentication mechanisms are vital in mitigating these risks. Additionally, cloud providers must implement robust security measures to protect data stored on their servers. The Internet of Things extends connectivity beyond traditional computing devices, enabling a vast network of interconnected smart devices. This network collects and exchanges vast amounts of data, ranging from personal information to critical infrastructure details. With this increased data flow comes the need for stringent security measures. IoT devices must be protected against unauthorized access, malware, and data breaches. Strong authentication, encryption, and regular security updates are essential for safeguarding the integrity, confidentiality, and availability of IoT systems. Privacy is another critical aspect affected by MCC and IoT. The vast amount of personal data generated by these technologies raises concerns about how this information is collected, stored, and utilized. Users must have control over their data and be informed about the purposes and entities involved in its processing. Clear consent mechanisms and transparent privacy policies are essential to establish trust between users, service providers, and device manufacturers. To address the security and privacy challenges in MCC and IoT, stakeholders must collaborate to develop comprehensive frameworks, standards, and best practices. Governments, regulatory bodies, industry organizations, and researchers should work together to establish guidelines for secure and privacy-preserving MCC and IoT deployments. This includes encouraging the development of secure software, hardware, and communication protocols, as well as promoting user education and awareness regarding potential risks and protective measures. In conclusion, as the adoption of Mobile Cloud Computing and the Internet of Things continues to grow, the security and privacy of these technologies must remain at the forefront. By implementing robust security measures, respecting user privacy, and fostering collaboration among stakeholders, we can build a future where MCC and IoT can thrive securely and responsibly, enabling innovative applications while safeguarding sensitive information.

References

[1]. Salama, R., Al-Turjman, F., Aeri, M., & Yadav, S. P. (2023, April). Internet of Intelligent Things (IoT)–An Overview. In 2023 International Conference on Computational Intelligence, Communication Technology and Networking (CICTN) (pp. 801-805). IEEE.

[2]. Prof.DUX available online: https://dux.aiiot.website/

[3]. Salama, R., Al-Turjman, F., Altrjman, C., & Gupta, R. (2023, April). Machine Learning In Sustainable Development–An Overview. In 2023 International Conference on Computational Intelligence, Communication Technology and Networking (CICTN) (pp. 806-807). IEEE.

[4]. Al-Turjman, F., Salama, R., & Altrjman, C. (2023). Overview of IoT Solutions for Sustainable Transportation Systems. NEU Journal for Artificial Intelligence and Internet of Things, 2(3).

[5]. Salama, R., Al-Turjman, F., Aeri, M., & Yadav, S. P. (2023, April). Intelligent Hardware Solutions for COVID19 and Alike Diagnosis-A survey. In 2023 International Conference on Computational Intelligence, Communication Technology and Networking (CICTN) (pp. 796-800). IEEE.

[6]. Salama, R., Al-Turjman, F., Bhatla, S., & Gautam, D. (2023, April). Network security, trust & privacy in a wiredwireless Environments–An Overview. In 2023 International Conference on Computational Intelligence, Communication Technology and Networking (CICTN) (pp. 812-816). IEEE.

[7]. Salama, R., Al-Turjman, F., Altrjman, C., Kumar, S., & Chaudhary, P. (2023, April). A Comprehensive Survey of Blockchain-Powered Cybersecurity-A survey. In 2023 International Conference on Computational Intelligence, Communication Technology and Networking (CICTN) (pp. 774-777). IEEE.

[8]. Salama, R., Al-Turjman, F., Bordoloi, D., & Yadav, S. P. (2023, April). Wireless Sensor Networks and Green Networking for 6G communication-An Overview. In 2023 International Conference on Computational Intelligence, Communication Technology and Networking (CICTN) (pp. 830-834). IEEE.

[9]. Salama, R., Al-Turjman, F., Bhatia, S., & Yadav, S. P. (2023, April). Social engineering attack types and prevention techniques-A survey. In 2023 International Conference on Computational Intelligence, Communication Technology and Networking (CICTN) (pp. 817-820). IEEE.

[10]. Salama, R., Altrjman, C., & Al-Turjman, F. (2023). Smart Grid Applications and Blockchain Technology in the AI Era. NEU Journal for Artificial Intelligence and Internet of Things, 1(1), 59-63.

[11]. Salama, R., Alturjman, S., & Al-Turjman, F. (2023). Internet of Things and AI in Smart Grid Applications. NEU Journal for Artificial Intelligence and Internet of Things, 1(1), 44-58.

[12]. Salama, R., Altrjman, C., & Al-Turjman, F. (2023). A Survey of Machine Learning (ML) in Sustainable Systems. NEU Journal for Artificial Intelligence and Internet of Things, 2(3).

[13]. Salama, R., Altrjman, C., & Al-Turjman, F. (2023). A Survey of Machine Learning Methods for Network Planning. NEU Journal for Artificial Intelligence and Internet of Things, 2(3).

[14]. Salama, R., Altrjman, C., & Al-Turjman, F. (2023). A Survey of the Architectures and Protocols for Wireless Sensor Networks and Wireless Multimedia Sensor Networks. NEU Journal for Artificial Intelligence and Internet of Things, 2(3).

[15]. Salama, R., Altrjman, C., & Al-Turjman, F. (2023). An overview of the Internet of Things (IoT) and Machine to Machine (M2M) Communications. NEU Journal for Artificial Intelligence and Internet of Things, 2(3).

[16]. Salama, R., Al-Turjman, F., Altrjman, C., & Bordoloi, D. (2023, April). The use of machine learning (ML) in sustainable systems-An Overview. In 2023 International Conference on Computational Intelligence, Communication Technology and Networking (CICTN) (pp. 821-824). IEEE.

[17]. Al-Turjman, F., & Salama, R. (2021). Cyber security in mobile social networks. In Security in IoT Social Networks (pp. 55-81). Academic Press.

[18]. Al-Turjman, F., & Salama, R. (2021). Security in social networks. In Security in IoT Social Networks (pp. 127). Academic Press.

[19]. Salama, R., & Al-Turjman, F. (2022, August). AI in blockchain towards realizing cyber security. In 2022 International Conference on Artificial Intelligence in Everything (AIE) (pp. 471-475). IEEE.

[20]. Al-Turjman, F., & Salama, R. (2020). An overview about the cyberattacks in grid and like systems. Smart Grid in IoT-Enabled Spaces, 233-247.

[21]. Salama, R., Al-Turjman, F., & Culmone, R. (2023, March). AI-Powered Drone to Address Smart City Security Issues. In International Conference on Advanced Information Networking and Applications (pp. 292-300). Cham: Springer International Publishing.

[22]. Salama, R., & Al-Turjman, F. (2023). Cyber-Security Countermeasures and Vulnerabilities to Prevent SocialEngineering Attacks. In Artificial Intelligence of Health-Enabled Spaces (pp. 133-144). CRC Press.

[23]. Salama, R., Al-Turjman, F., Altrjman, C., & Bordoloi, D. (2023, April). The ways in which Artificial Intelligence improves several facets of Cyber Security-A survey. In 2023 International Conference on Computational Intelligence, Communication Technology and Networking (CICTN) (pp. 825-829). IEEE.

[24]. Salama, R., Al-Turjman, F., Bhatla, S., & Mishra, D. (2023, April). Mobile edge fog, Blockchain Networking and Computing-A survey. In 2023 International Conference on Computational Intelligence, Communication Technology and Networking (CICTN) (pp. 808-811). IEEE.

[25]. Salama, R., Al-Turjman, F., Chaudhary, P., & Banda, L. (2023, April). Future Communication Technology Using Huge Millimeter Waves—An Overview. In 2023 International Conference on Computational Intelligence, Communication Technology and Networking (CICTN) (pp. 785-790). IEEE.

[26]. Gupta, M., Kumar, R., Chaudhary, R. K., & Kumari, J. (2021, December). IoT Based Voice Controlled Autonomous Robotic Vehicle Through Google Assistant. In *2021 3rd International Conference on Advances in Computing, Communication Control and Networking (ICAC3N)* (pp. 713-717). IEEE.

[27]. Gupta, M., Kumar, R., Walia, H., & Kaur, G. (2021, October). Airlines based twitter sentiment analysis using deep learning. In *2021 5th International Conference on Information Systems and Computer Networks (ISCON)* (pp. 1-6). IEEE.

[28]. Kumar, R., Gupta, M., Shukla, S., & Yadav, R. K. (2021, September). E-challan automation for RTO using OCR. In *2021 third international conference on inventive research in computing applications (ICIRCA)* (pp. 18). IEEE.

[29]. Bawa, H., Singh, P., & Kumar, R. (2012). An Efficient Novel Key management scheme using NchooseK algorithm for Wireless Sensor Networks. *International Journal of Computer Networks & Communications (IJCNC) Vol*, *4*.

[30]. Gupta, M., Solanki, V. K., & Singh, V. K. (2017). A novel framework to use association rule mining for classification of traffic accident severity. *Ingeniería solidaria*, *13*(21), 37-44.

[31]. Puneet, Kumar, R., & Gupta, M. (2022). Optical coherence tomography image based eye disease detection using deep convolutional neural network. *Health Information Science and Systems*, *10*(1), 13.

[32]. Gupta, M., Yadav, R., & Tanwar, G. (2016, March). Insider and flooding attack in cloud: A discussion. In *2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom)* (pp. 530-535). IEEE.

[33]. Kumar, P., Gupta, M., & Kumar, R. (2023, July). Improved Cloud Storage System Using IPFS for Decentralised Data Storage. In *2023 International Conference on Data Science and Network Security (ICDSNS)* (pp. 01-06). IEEE.

[34]. Sharma, H., Kumar, R., & Gupta, M. (2023, March). A Review Paper on Hybrid Cryptographic Algorithms in Cloud Network. In *2023 2nd International Conference for Innovation in Technology (INOCON)* (pp. 1-5). IEEE.

[35]. Gupta, M. (2023). A novel scheme to manage the e-healthcare system using cloud computing and the internet of things. In *Computational Intelligence in Healthcare* (pp. 81-97). CRC Press.

[36]. Gupta, M., Gupta, A., & Arora, S. (2022). Addressing the Security, Privacy, and Trust Issues in IoT-Enabled CPS. In *Handbook of Research of Internet of Things and Cyber-Physical Systems* (pp. 433-452). Apple Academic Press.

EVALUATION OF THE EFFECTS OF ORGANIZATIONAL COMMUNICATION ON ORGANIZATIONAL COMMITMENT ACCORDING TO THE OPINIONS OF ADMINISTRATORS, TEACHERS AND SERVANTS: THE CASE OF RURAL PRIMARY SCHOOLS

Zehra Altinay, Hazal Terzioğlu Dokuzlar, Gokmen Dagli
[1]Professor in Educational Technology, Societal Research and Development Center, Faculty of Education, Near East University, Nicosia, Northern Cyprus, Mersin 10 Turkey
[2]Master in Educational Management, Ministry of Education, North Cyprus Nicosia, Northern Cyprus, Mersin 10 Turkey
[3]Professor in Educational Management, Faculty of Education, Kyrenia University, Kyrenia, Northern part of Cyprus, Mersin 10 Turkey

zehra.altinaygazi@neu.edu.tr, hazaldokuzlar@hotmail.com, gokmen.dagli@kyrenia.edu.tr

Abstract: This study examines the nexus between organizational communication and organizational commitment in rural primary schools, drawing insights from administrators, teachers, and support staff. Utilizing a mixedmethods approach, encompassing surveys, interviews, and document analysis, the research investigates how communication strategies impact commitment levels in this specific educational context. Findings aim to illuminate the nuanced dynamics influencing commitment, offering actionable insights for educational stakeholders. By addressing the unique challenges of rural primary schools, this research contributes to the enhancement of communication strategies, fostering a more committed and engaged school community. The study's outcomes may inform tailored interventions and policies, creating a foundation for improved organizational commitment in rural primary education.

Keywords: Organizational Communication, Organizational Commitment, Rural Primary Schools, Stakeholder Perspectives, Educational Context

1. INTRODUCTION

From the moment human beings began to live in communities, they have needed to communicate with other individuals. Communication is the lifeblood of organizations as it enables people to come together, organize, create communities and move towards a common goal. As in all other organizations, the most important factor in educational organizations to maintain their existence and achieve their goals is the communication between the employees of the organization (Ada and Oymak, 2021). It depends on organizational communication for all employees working in educational organizations, such as administrators, teachers, servants and secretaries, to ensure the flow of information and work in cooperation and coordination to achieve educational goals (Ergenekon and Aküzüm, 2020; Karasoy, 2021). In order for educational organizations to compete with other educational organizations, all stakeholders must work in a coordinated manner. At this point, the most important element that ensures coordination is organizational communication. It has been determined that organizational communication is effective on making and implementing decisions regarding the educational process in educational institutions, ensuring the necessary information flow, student success, financial success, reputation and efficiency (Çantay and Yaşar, 2019; Ertekin et al., 2018; Güçlü, 2017). It is known that effective communication in educational institutions affects the school climate. Effective organizational communication directly affects employees' feeling of belonging to the organization and creating strong bonds (Çağlar and Çınar, 2021). School administrators, teachers and other employees; Participating in decision-making on behalf of the

school, feeling like they belong to the school, working hard to achieve the school's goals, and aiming to serve at the current school for many years is called organizational commitment (Kılıç, 2019). It has been demonstrated that organizational commitment affects the job performance, job attendance and productivity of employees in the organization. At this point, it has been determined that a high level of organizational commitment of teachers in educational organizations increases student success and enables the school to achieve its goals more easily (Balay, 1999; Eskibağ, 2014; Sarıkaya, 2011). There are studies in the literature that reveal the effects of organizational communication and organizational commitment on each other. As a result of these studies, the effects and level of organizational communication on organizational commitment were determined. In their study, Doğruöz and Özdemir (2018) found that the anti-productive work behaviors of teachers working in educational institutions had a positive relationship with their organizational commitment. In this context, since the scope of anti-production work behaviors includes interrupting the flow of information and giving false information, it is seen that organizational commitment is also affected when organizational communication is prevented. As a result of the study conducted by Yıldız (2019) to determine the effects of organizational communication on organizational commitment and organizational trust; It has been determined that organizational communication elements are effective on organizational commitment. Çağlar and Çınar (2021) revealed that the communication skills of school principals affect the organizational commitment levels of teachers. Therefore, it has been stated that the leading role directing organizational communication belongs to the school principal, and when he manages organizational communication effectively, teachers' organizational commitment levels increase.

Purpose of the Research; Achieving the goals set in educational institutions and ensuring student success are very important for school administrators, teachers and all other stakeholders. Achieving the school's goals and ensuring student success is possible with the cooperation and coordinated work of all school stakeholders. It is necessary to ensure information flow and an effective communication process between school administrators, teachers and all other employees. In this context, organizational communication is the key to educational institutions achieving their goals and ensuring student success. It is stated in the literature that the strength of organizational communication between employees in an organization is related to the organizational commitment of the people working in that organization. The aim of the research conducted in this direction is to reveal the effects of organizational communication on organizational commitment in 5 primary schools selected from rural regions in TRNC, from the perspectives of the employees in the institution. The study to be conducted for this purpose seeks answers to the following research questions:

1.What are the organizational commitment levels of the employees?
2.Do employees' organizational commitment levels differ according to demographic factors?
3.How do organizational employees evaluate the relationship between organizational communication and organizational commitment?

2. The Research Method

The model of this research is a mixed model research in which qualitative and quantitative methods are used together. Mixed model research is a multidimensional research design in which the researcher uses qualitative and quantitative methods to collect, analyze and interpret data in the same research (Cresswell and Plano Clark, 2011). It provides strong results about the research as a result of collecting and interpreting qualitative and quantitative data

together. The first reason for choosing the mixed method is that it provides a holistic and multidimensional meaning to events and phenomena. Another purpose of choosing the mixed method is to increase credibility by ensuring that the data obtained from the combined use of qualitative and quantitative methods confirm each other. In this context, the weak side of one method is eliminated with the support of the other method (Yıldırım and Şimşek, 2018). The data obtained in this research were collected by qualitative and quantitative methods. In the qualitative dimension of the research, the opinions of employees in rural primary schools regarding organizational communication and organizational commitment were examined in detail. In the quantitative dimension of the research, the relationship between the demographic characteristics and organizational commitment of school employees in the selected rural primary schools was examined. In this context, while the research is handled in a multidimensional manner, the data obtained also support each other. The patterns used in the mixed method are examined under four headings. These; variation design, embedded design, explanatory design and exploratory design (Creswell and Plano Clark, 2011). Variation design was used in this research. In the variation design, it is aimed to make comparison and integration by creating diversity in the data obtained by using qualitative and quantitative research methods together. At the same time, it is aimed to ensure the validity and reliability of the study (Cresswell and Plano Clark, 2011). In this study, the data obtained through semistructured interviews were confirmed by comparing them with the data obtained from the scales.

In the quantitative dimension of the research, the Organizational Commitment Scale was applied to 68 employees (5 administrators, 53 teachers and 10 janitor) in the selected rural primary schools. In the qualitative dimension, interviews were conducted with 4 school principals, 5 teachers and 5 janitors working in the same 5 schools, in the light of semistructured interview questions.

Quantitative Aspect of the Research

In the quantitative dimension of this research, TRNC. It was aimed to determine the relationship between the demographic characteristics and organizational commitment of the employees, according to the opinions of administrators, teachers and janitor at Güvercinlik, Düzova-Cihangir, Tepebaşı, Serhatköy and Dipkarpaz Primary Schools affiliated with the Ministry of National Education and Culture. In this context, the relational screening model was used.

Qualitative Dimension of the Research

Qualitative research is research in which the events and facts under investigation are examined in depth, described and interpreted, and the results are presented from a subjective perspective (Yıldırım and Şimşek, 2018). In the qualitative dimension of this research, the phenomenology pattern, one of the qualitative research methods, was used. Phenomenology, also known as phenomenology, is a research pattern shaped around facts. In the phenomenology design, the researcher examines the subject he is working on in depth (Yıldırım and Şimşek, 2018). In this research, the opinions of 4 managers, 5 teachers and 5 janitors regarding organizational communication and organizational commitment were evaluated through semi-structured interviews.

Population, Sample and Study Group

In this research, 5 primary schools located in rural areas in 5 different districts under the Directorate of Primary Education within the TRNC Ministry of National Education and Culture were randomly selected. These randomly selected schools affiliated with the TRNC Primary Education Department are Güvercinlik Primary School, Düzova-Cihangir Primary School, Tepebaşı Primary School, Serhatköy Primary School and Dipkarpaz Primary School.

Quantitative Aspect of the Research

While determining the participant group in the quantitative dimension of the study, the participation of all principals, assistant principals, teachers, secretaries and janitors working in these 5 schools was targeted. While determining the sample of the quantitative dimension of the research, convenience sampling method was preferred. Convenience sampling is a sampling method in which data is collected by selecting the participant group in the easiest, shortest time and with the least cost. According to this method, the aim is to create the sample easily (Yazıcıoğlu, 2004). The survey, which was intended to be applied to 83 participants, was applied to 68 people on a voluntary basis. In this context, the sample's representativeness of the universe was determined as 81.9%.

Qualitative Dimension of the Research

The preferred research design in the qualitative dimension of this study is phenomenology. When determining the sample in this research design, participants who experience the phenomenon emphasized by the research are preferred (Creswell and Plano Clark, 2011). For this purpose, preliminary interviews are held with the participants to determine whether they can be included in this research. The criterion sampling method provides the formation of the most appropriate study group in phenomenology research (Yıldırım and Şimşek, 2018). In the criterion sampling method, a study group is formed according to the criteria determined by the researcher for the study. In this study, a working group was formed from participants who worked in rural primary schools and could reflect their views on organizational communication and organizational commitment. In this context, it was aimed to interview 5 school principals, 5 teachers and 5 janitors working in 5 predetermined rural primary schools. Since the participation of the participants in the study group was voluntary, a total of 14 people, including 4 school principals, 5 teachers and 5 janitor, took part in the study group in the qualitative dimension of the study.

Data Collection Tools

Quantitative Dimension of the Research: Organizational Commitment Scale. The survey form used to collect data begins with an information letter briefly explaining the purpose of the survey to the participants. The first part of the survey consists of questions about the participant's demographic information such as age, gender, years in the profession, position at school and how long he/she has been doing this task. The last part consists of questions of the organizational commitment scale.

Qualitative Dimension of the Research: Semi-Structured Interview Form; In the study, data was collected by using semi-structured interview technique, which is a qualitative data collection method, in order to obtain the opinions of administrators, teachers and other employees working in rural primary schools in TRNC about organizational communication and organizational commitment. In the semi-structured interview method, the researcher has the flexibility to change the sentence structure and order and go into detail about the topics he

wants to cover while directing the questions he has prepared in advance to the participant (Yıldırım and Şimşek, 2018).

3. Collection of Data

Before starting the research, an ethics report for the research was obtained by applying to the Near East University Research Ethics Committee. Then, in order to collect data from the employees in the rural primary schools where the research will be conducted, TRNC. By obtaining the necessary permissions from the Department of Primary Education under the Ministry of National Education and Culture, data collection began from school administrators, teachers and other employees included in the research. Since the research was a mixed method research, two different data collection tools were used, quantitative and qualitative. In the quantitative part, data was collected by applying the Organizational Commitment Scale to 5 school administrators, 52 teachers and 10 other employees. This scale was applied to the participants via Google Forms. In the qualitative dimension, data was obtained by asking semistructured interview questions developed by the researcher to 4 school principals and 5 teachers. Data was obtained by applying a personal opinion form to 5 school employees who could not be reached through online interviews.

4. Analysis and Interpretation of Data

Due to the use of mixed methods in this research, data were collected by both qualitative and quantitative methods. Data analysis was done separately according to both methods. The data obtained in the quantitative dimension of the research were analyzed with the SPSS 26.0 statistical program. The content analysis method used in the analysis of qualitative research was used to analyze the data obtained through semi-structured interview questions and personal opinion form. Content analysis involves identifying the data obtained, collecting and interpreting it under certain themes. The data obtained as a result of qualitative research is coded and themes are determined. Then, the codes and themes are arranged and the findings are defined and interpreted (Yıldırım & Şimşek, 2018). In this research, NVIVO 11 qualitative data analysis software program was used to digitize the data obtained in the qualitative dimension and display it with graphics. It is stated that qualitative data, like quantitative data, can be expressed numerically to a certain extent (Yıldırım and Şimşek, 2018).

5. RESULTS

Findings Regarding the Quantitative Dimension of the Research Difference Tests

In this section, it was tested whether there was a significant difference between the subcategories of the demographic factors used in the correlation analysis and the variables of the research.

Organizational Commitment Dimensions According to Participants' Gender. “Do organizational commitment dimensions differ according to the gender of the participants? Hypothesis results are presented in Table 1.

Table 1.

Test Results for the Difference Between Organizational Commitment Dimensions by Gender

	DUY	DEV	NOR
Mann-Whitney U	498,500	539,500	507,500
Wilcoxon W	1164,500	1035,500	1003,500
Z	-,755	-,235	-,639
Asymp. Sig. (2-tailed)	,450	,814	,523

a.Group Variable: Your Gender

According to the Mann-Whitney U test results, it is seen that there is no significant difference between the gender variable and the sub-dimensions of the organizational commitment scale (p>0.05).

Organizational Commitment Dimensions According to Participants' Ages. “Do organizational commitment dimensions differ depending on the age of the participants?” Hypothesis results are presented in Table 2.

Table 2.
Test Results for the Difference Between Organizational Commitment Dimensions According to Age Groups

	DUY	DEV	NOR
Kruskal-Wallis H	2,146	2,103	,668
Df	5	5	5
Asymp. Sig.	,829	,835	,985

a. Kruskal Wallis Test
b.Group Variable: Your age

According to the results of the Kruskal Wallis H test, it is seen that there is no significant difference between the age variable and the sub-dimensions of the organizational commitment scale (p>0.05). Organizational Commitment Dimensions According to Participants' Education Levels. “Do organizational commitment dimensions differ according to the education level of the participants?” Hypothesis results are presented in Table 3.

Table 3.
Test results for the difference between organizational commitment dimensions according to education level

	DUY	DEV	NOR
Kruskal-Wallis H	,101	1,040	1,969
Df	2	2	2
Asymp. Sig.	,951	,595	,374

a. Kruskal Wallis Test

b. Group variable: Your Education Status

According to the results of the Kruskal Wallis H test, there is no significant difference between the education level variable and the sub-dimensions of the organizational commitment scale (p>0.05). Organizational Commitment Dimensions According to Participants' Total Working Time. “Do organizational commitment dimensions differ according to the participants' total working time?” Hypothesis results are presented in Table 4.

Table 4.
Test Results for the Difference Between Organizational Commitment Dimensions According to Total Working Time

	DUY	DEV	NOR
Kruskal-Wallis H	1,880	1,226	3,643
Df	4	4	4
Asymp. Sig.	,758	,874	,456

a. Kruskal Wallis Test

b. Group variable: Your Total Working Time

According to the results of the Kruskal Wallis H test, it is seen that there is no significant difference between the total working time variable and the sub-dimensions of the organizational commitment scale (p>0.05). Dimensions of Organizational Commitment of Participants According to the Duration of Working in the Institution. “Do the organizational commitment dimensions of the participants differ according to the variable of where they work?” Hypothesis results are presented in Table 5.

Table 5.
Test Results for the Difference Between Organizational Commitment Dimensions According to the Duration of Working in the Institution

	DUY	DEV	NOR
Kruskal-Wallis H	,040	,055	1,380
Df	2	2	2
Asymp. Sig.	,980	,973	,502

a. Kruskal Wallis Test

b. Group variable: Your Term of Office at the Institution You Work For

According to the results of the Kruskal Wallis H test, there is no significant difference between the tenure in the institution you work for and the sub-dimensions of the organizational commitment scale (p>0.05). Organizational Commitment Dimensions According to the Variable of Where Participants Work in the Institution.

Table 6.
Test Results for the Difference Between Organizational Commitment Dimensions According to the Variable of Where the Participants Work

	DUY	DEV	NOR
Kruskal-Wallis H	,040	,055	1,380
Df	2	2	2
Asymp. Sig.	,980	,973	,502

a. Kruskal Wallis Test
b. Grouping Variable: calpoz

The results of the Kruskal Wallis H test show that there is no significant difference between the variable of place of employment and the sub-dimensions of the organizational commitment scale (p>0.05). Findings Regarding the Question: What are the Organizational Commitment Levels of Employees? The test results obtained regarding the dimensions of employees' organizational commitment levels are presented in Table 7.

Table 7.
Organizational Commitment Levels of Employees Regarding the Emotional Commitment Dimension

Dimension	**N**	**X**	Standard deviation
When Table 7 is evaluated, the average level of attitude towards normative commitment (X = 2.87) is at a medium level. This shows that the normative commitment level of the participants to the institution they work for is medium.	67	3.94	0,86

When Table 11 is evaluated, the average level of attitude towards emotional commitment (X = 3.94) is high. This shows that the participants have a high level of emotional commitment to the institution they work for.

Table 12.
Organizational Commitment Levels of Employees Regarding the Continuance Commitment Dimension

Dimension	N	X	Standard deviation
Continuance Commitment Dimension	67	2.73	1.23

When Table 12 is evaluated, the average level of attitude towards continuance commitment (X=2.73) is at a medium level. This shows that the participants' level of continued commitment to the institution they work for is moderate.

Table 8.
Employees' Organizational Commitment Levels Regarding the Normative Commitment Dimension

Dimension	N	X	Standard deviation
Normative Commitment Dimension	67	2.87	1,11

The incident was obtained by applying a survey using the sampling method. The research focused on two questions.
1.What are the organizational commitment levels of the employees?
2. Do employees' organizational commitment levels differ according to demographic factors?
In this context, difference tests were conducted and no statistically significant difference was found in the organizational commitment levels of employees according to gender, age, education level, total working time, working time in the institution and duty.
It was found to be statistically significantly higher than the average score of the employees regarding their emotional commitment. It can be said that the emotional commitment of employees is higher than the continuation and normative commitment levels.

Findings Regarding the Qualitative Dimension of the Research
Themes and Subthemes for the Research Model Emerged as a Result of Data Analysis in Qualitative Research

In the qualitative dimension of the research, the themes that emerged as a result of the analysis of the data regarding the opinions of school principals, teachers and janitor working in rural primary schools regarding the Effects of Organizational Communication on Organizational Commitment were stated. In the research model, the participants were divided into themes according to the opinions they expressed in line with the questions asked. The findings are presented in detail in the light of these themes.
Table 9:
What kind of support do you receive from your school to achieve your school's goals?

THEMA	MANAGER		TEACHER		JANITOR	
	N	%	N	%	N	%
Sharing Support	4	28,6	-	0	5	35,7
Task Breakdown Support	1	7,1	-	0	4	28,6
Planning	4	28,6	-	0	5	35,7
Moral Support of Teachers	4	28,6	2	14,3	2	14,3
Janitor Support	2	14,3	1	7,1	5	35,7

Technological Hardware Support	-	0	1	7,1	-	0
Physical Hardware Support	-	0	2	14,3	-	0
Moral Support of the Manager	-	0	3	21,4	2	14,3
Material - Material Support	_	0	2	14,3	4	28,6
Manager's Financial Resource Support	-	0	1	7,1	-	0
Financial Resource Support for Teachers	-	0	1	7,1	-	0
External Environmental Support	1	7,1	2	14,3	-	0

As seen in Table 9, according to the opinions of the principal, teacher and janitor, what kind of support do you receive from your school in order to achieve its goals? They put forward

their views on sharing support, task distribution support, planning, moral support of teachers, janitor support, technological equipment support, physical equipment support, moral support of the principal, material support, financial resource support of the principal, financial resource support of the teacher and external environment support. According to the answers given in Table 9, principals stated that they mostly received task sharing, planning and moral support from teachers from their institutions. Teachers, on the other hand, stated that they received the most moral support from school principals. According to the janitors, the issues they receive the most support from at the school where they work are sharing, planning and receiving support from other janitors.

The opinions of the participants on the subject are stated below.

M1: "So, especially in rural areas, the main thing is sharing. In other words, in my opinion, all teachers also become administrators from time to time within their job descriptions. "They are trying to share my assigned burdens."

M2: "At the meeting held on the first day of school, we first make a plan about our projects to be done this year and the subjects I need. We express this at the first meeting of the week the school opens and make a plan accordingly. Of course, teachers are involved in this issue."

S1: "My manager tries to help as much as he can in any way he can. So, for example, let me talk about this at the beginning of the semester. During the preparation period, before schools opened, there was a lack of projection in some of our classes. No, there was a problem with the computers. My principal worked diligently to have them fixed before the schools opened, or to have them purchased and installed in the classrooms. If we talk technologically, we don't have any problems with projection, at least on the computer. We have a laboratory in our school. When I look at it from a managerial standpoint, both my manager and my assistant manager try to help me under all circumstances..."

T2: "I mean, we only have one principal from the school administration. There is no other administrator at the school. I am especially pleased with our principal this year. Let me tell you both in a spiritual sense, the man reinforces the work we do, how can I say it, and thanks you…"

T4: "He makes every contribution to achieve our goal and supports us. If you have any problems with the parents, they say okay, for example, you wait a little while, I will talk to you and help you as much as I can. If we are missing something, he tries to cover it by even paying from his pocket. Essentially, if an event is to be held, it is trying to implement everything it can in a democratic way to achieve its goal."

H3: "Everyone has their own area of responsibility and their own work. "Everyone knows what to do every day."

H4: "Like me, many people's children are valuable. That's why we have to do our job properly. When something breaks or breaks at school, we try to fix it without delay. We always try to keep the toilets and the garden clean. Our school principal always walks around, tells us if he sees something missing, and follows up and plans the work. Since he is a meticulous person, our work always proceeds in a planned and programmed manner."

6. CONCLUSION AND RECOMMENDATIONS

Results Regarding the Quantitative Aspect of the Study. In the research conducted, the survey applied to school principals, teachers and other employees examined whether organizational commitment had a significant relationship with the demographic variables of gender, age, education level, total working time, working time in the institution and duty at the school. In this context, no significant relationship was found between employees' organizational commitment and demographic characteristics. Similar studies on the subject have also obtained different results regarding the relationship between organizational commitment and demographic variables. While Ateş and

Buluç (2018) concluded that the organizational commitment of primary school teachers may show a significant difference according to demographic variables such as gender, age, marital status, education level and professional seniority, Mert (2019) found that there is no significant difference according to gender, marital status, branch and staff variables. stated. Çağlar and Çınar (2021) found that there is no significant difference in terms of the gender variable of organizational commitment, but there is a significant difference in terms of professional seniority and working time in the institution.

As a result of the analysis conducted on the emotional commitment, continuance commitment and normative commitment dimensions of organizational commitment, it was determined that the emotional commitment of the participants to the school they work for was at the highest level, continuation commitment was at the medium level and normative commitment was at the low level. While Kaygısız (2012) and Kılıç (2019) reached a conclusion that coincides with the findings of the study, Uludağ (2018) concluded in his study that emotional and normative commitment, one of the organizational commitment dimensions of corporate employees, is high and continuance commitment is low.

Results Regarding the Qualitative Dimension of the Study.

Results Regarding the Support Received from the Institution in Fulfilling the School's Aims. The principal, teachers and janitors classified the support received from the institution in achieving the school's goals in different ways. In this context, managers; It is concluded that they receive planning, task distribution, sharing, moral support of teachers,

support of janitors, and support from the external environment. At the beginning of the year, school principals, together with teachers, make plans regarding the operation of the school, its goals, and the activities to be held during the year. This indicates that while planning, tasks were distributed with the teachers, certain teachers were given duties for each activity, and teachers supported each other morally in the realization of these activities. In addition, the burden of the school principal is shared by the teachers when necessary, and they work with team spirit. They state that school staff, including janitors, support each other in activities, distribute tasks and that everyone does more than their share. School principals receive financial support from the external environment. The school is financially supported by the Parent-Teacher Association, the municipality to which the school is affiliated, and local tradesmen.

It has been concluded that teachers receive moral support, technological equipment support, janitor support, physical equipment support, moral support of the principal, material material support, financial resource support of the principal, material resource support of the teacher, and external environmental support from the institution in order to fulfill the school's objectives. Teachers create optimal educational conditions by getting support from other teachers, sharing tasks, and getting support from each other in order to fulfill the educational goals of the school. School principals support teachers in finding all kinds of financial resources and completing the physical and technological equipment. In addition, teachers state that they are appreciated by school principals for the work they do. Teachers share course materials and mimeographs with each other. Teachers also state that the external environment provides financial support for the school's needs. In cases where the school does not have the resources, teachers cover the purchase of necessary materials for educational activities for children from their own budgets. Janitors, in order to fulfill the aims of the school; It is concluded that they receive sharing support, task distribution support, planning, teachers' moral support, janitor support, principal's moral support, and material support.

Janitors can easily fulfill their duties with the distribution, sharing and planning of tasks made by the school administration. Due to the distribution of tasks, everyone supports each other with understanding. It is stated that the school principal and teachers constantly warn students about keeping the environment and classroom clean, and these warnings are a great support for the janitors. If there is a shortage of cleaning materials needed for the janitors to perform their duties properly, the school principal immediately procures new ones. These results obtained are based on Yelken, Kılıç and Üredi (2010); It is supported by the results of studies conducted by Derinbay (2011) and Uzun (2018) regarding the support employees receive from organizations.

Results Regarding the Comparison of the School in the City and the School in the Rural Area in Terms of Communication. For school principals, in schools located in rural areas, there is easy communication, easy organization, a friendly school environment, a sharing school environment, more room for cooperation, no grouping among teachers, a less crowded environment, limited financial means, and financial support from the municipality. It was concluded that it was easy to get support. It is stated that communication in city schools is unprofessional and limited. On the other hand, it is stated that communication in rural schools is easy and friendly. A school environment based on cooperation and sharing among employees with the benefits of a friendly environment exists in schools in rural areas. The small number of teachers prevents grouping. Although financial opportunities are limited in rural schools, it is stated that it is easier to receive financial support from the municipality in the region where the school is located. Teachers, on the other hand, have the same opinion as school principals,

without mentioning financial means. According to the opinions of the janitors, it was concluded that in rural schools, communication is easy, organization is easy and there is a less crowded environment. In terms of janitors, the fact that schools in rural areas have fewer students than those in the city makes it easier for them to clean and maintain this cleanliness. It is also stated that communication and organization among all school staff is easy. Lezha (2017) reached similar results to this study in his study on organizational communication in rural schools.

Results on the Evaluation of Advantages and Disadvantages of Communication and Management in Rural Schools. According to the opinions of school principals, it has been concluded that the advantages of working in a school located in rural areas are easy communication, easy gathering, discussion through various communication tools, friendly family atmosphere, ease of receiving financial support from the municipality, administrative convenience, cooperation, cooperation, sharing, and an uncrowded environment. It was concluded that the disadvantages are communication problems due to parents' working hours and limited financial resources. School principals state that it is administratively easy because the number of teachers and students is low. It is concluded that due to the small number of teachers and employees, there is a friendly family atmosphere, communication is easy, everyone is easily organized from the moment of the meeting, crises can be easily managed, and communication can easily take place face to face, through meetings or via WhatsApp. There is cooperation and cooperation between teachers and social sharing. At points where schools experience financial difficulties, it is considered an advantage to easily receive help from the regional municipality.

Since parents in rural areas mostly earn their living from agriculture and animal husbandry, their working hours are not regular like those of civil servant parents in cities. For this reason, there are difficulties in communicating with parents in rural areas. In addition, the school's limited financial resources are considered a disadvantage. Akın, Adıgüzel and Aytaş (2022) reached similar results regarding the disadvantages stated by principals. Teachers working in schools in rural areas concluded that the advantages of working here are easy communication, easy gathering, friendly family atmosphere, uncrowded environment, respect for teachers, and easy and good communication with parents. Although teachers almost agree with principals about the advantages of working in rural areas, teachers state that they are more respected by students and their parents in rural areas. In addition, teachers state that they can easily reach parents and communicate well. According to the teachers' opinions, the disadvantages are that financial resources are limited, they are far from the center, there are constantly changing teachers and administrative staff in some schools, the limited number of teachers, the absence of groups, and having to get along with everyone. Teachers cannot carry out every activity and activity they want due to limited financial resources. Karataş and Kınalıoğlu (2018) concluded that limited financial resources are a disadvantage [29] – [39].

Suggestions

In line with the findings obtained as a result of the research, providing in-service training on communication for administrators in schools affiliated with the TRNC Ministry of National Education can strengthen organizational communication in schools. A survey can be conducted for teachers through school principals of the Ministry of National Education to express their expectations regarding organizational communication. School principals' paying more attention to teachers' expectations and demands in this regard, and their voluntary participation in trainings organized by the ministry to improve themselves in this field, can make a positive contribution to organizational communication and therefore to education. It may be useful for education inspectors working within the Ministry of National Education to

inspect the communication skills of school administrators and teachers, in addition to document and education inspections, in the inspections they carry out in schools. When school administrators are appointed, they are appointed according to their exam scores and criterion scores. In addition, the element of "communication skills and competence" can be added to the qualifications sought when appointing school administrators.

REFERENCES

[1]. Ada, N. ve Oymak, B. (2021). Bir üniversitenin örgütsel hikayelerinin örgütsel iletişim kuramları bağlamında irdelenmesi. *Alanya Akademik Bakış Dergisi, 5(1), 441-451.* Doi: 10.29023/alanyaakademik.807967

[2]. Akın, U., Adıgüzel, Ö., ve Aytaş, E. (2022). Köy okulunda müdür olmak: Sorunlar, uygulamalar ve çözüm önerileri. *Uluslararası Türk Eğitim Bilimleri Dergisi*, *2022*(18), 168-207. Erişim adresi: https://dergipark.org.tr/en/pub/goputeb/iss

[3]. Allen, N. J. ve Meyer, J. P. (1990), The Measurement and Antecedent of Affective, Continuance and Normative Commitment To The Organization, Journal of Occupational Psychology, Vol: 63

[4]. Ateş, Ö. T. ve Buluç, B. (2018). İlköğretim öğretmenlerinde motivasyon ve örgütsel bağlılığın demografik değişkenler açısından incelenmesi. *Mehmet Akif Ersoy Üniversitesi Eğitim Fakültesi Dergisi, 1(48), 1-30.* Erişim adresi: https://search.trdizin.gov.tr/yayin/detay/

[5]. Balay, R. (1999). İşgörenlerin örgütsel bağlılık etkenleri ve sonuçları. *Ankara Üniversitesi Eğitim Bilimleri Fakültesi Dergisi, 32(1), 237-246.* Erişim adresi: https://doi.org/10.1501/Egifak_0000001161

[6]. Creswell, J. W., & Plano Clark, V. L. (2011). *Designing and conducting mixed methods research* (2nd ed.). Thousand Oaks, CA: Sage.

[7]. Çağlar, Ç. ve Çınar, H. (2021). Okul müdürlerinin iletişim yeterliklerinin öğretmenlerin örgütsel bağlılığı üzerindeki etkisi. *E-Uluslararası Eğitim Araştırmaları Dergisi, 12(1), 157-170.* DOI: 10.19160/ijer.83195

[8]. Çantay, N. ve Yaşar, O.(2019). Kurumsal itibar algısında örgütsel iletişimin rolü: Devlet ve özel okullarda karşılaştırmalı bir analiz. *Uluslararası Toplum Araştırmaları Dergisi, 14(20), 1161-1186.* DOI: 10.26466/opus.606924

[9]. Derinbay, D. (2011). İlköğretim okullarında görev yapan öğretmenlerin algıladıkları örgütsel destek düzeyleri [Yüksek Lisans Tezi].

[10]. Doğruöz, E. ve Özdemir, M. (2018). Eğitim örgütlerinde üretim karşıtı iş davranışları ve örgütsel bağlılık ilişkisi. *İlköğretim Online, 17(1), 396-413.* Doi:10.17051/ilkonline.2018.

[11]. Ergenekon, Ö. ve Aküzüm, C. (2020). Bağımsız anaokullarında görev yapan yöneticilerin iletişim becerilerinin örgüt iklimine etkisi. *EKEV Akademi Dergisi, 24(81), 343-376.* Erişim adresi: https://www.researchgate.net/profile/Oemer-Ergenekon/publication/3

[12]. Ertekin,İ. , Ilgın, H. ve Yengin, D. (2018). Örgütsel iletişim kuramları. *The Turkish Online Journal of Design, Art and Communication – TOJDAC, 8(2), 297-311.* Erişim adresi: https://dergipark.org.tr/en/pub/tojdac/issue/36245/408398?publisher=deniz-yengin;

[13]. Eskibağ, Ş. (2014). Öğretmenlerin örgütsel bağlılık ve iş doyumları ile mesleki performans arasındaki ilişki [Yayınlanmamış Yüksek Lisans Tezi] Sebahattin Zaim Üniversitesi.

[14]. Güçlü, M. (2017). Örgütsel iletişim: Eğitim kurumlarındaki yeri ve önemi açısından bir değerlendirme. *OPUS – Uluslararası Toplum Araştırmaları Dergisi, 7(13), 854-870*. DOI: 10.26466/opus.350484.

[15]. Karataş, A. ve Kınalıoğlu İ. H. (2018). Köy okullarında çalışan sınıf öğretmenlerinin sorunları. *Uşak Üniversitesi Sosyal Bilimler Dergisi*, *11*(3), 207-220. Erişim adresi: https://dergipark.org.tr/en/pub/usaksosbil/issue/40289/480910

[16]. Karasoy, H.A. (2021). Yönetim fonksiyonları ekseninde örgütsel iletişimin önemi. *Kamu Yönetimi ve Politikaları Dergisi, 2(1), 81-92.* Erişim adresi: https://dergipark.org.tr/en/pub/kaypod/issue/61367/885428

[17]. Kaygısız, A. G. (2012). *İlköğretim öğretmenlerinin örgütsel bağlılık düzeyleri ve karara katılma durumları arasındaki ilişki Kütahya örneği* [Yüksek Lisans Tezi].

[18]. Kılıç, M. Y. (2019). Okullarda yöneticinin sağladığı etik iklimin, örgütsel bağlılık ve öğretmen performansına etkisi. *Cumhuriyet International Journal of Education, 8(3), 807-836*. http://dx.doi.org/10.30703/cije.561366

[19]. Lezha, E. (2017). Exploring teachers' perceptions on organizational climate in urban and rural schools. *European Scientific Journal*, *13*(13), 402-408. Doi: 10.19044/esj.2017.v13n13

[20]. Mert, E. (2019). İlkokul ve ortaokul öğretmenlerinin örgütsel bağlılıklarının incelenmesi [Yüksek Lisans Tezi].

[21]. Sarıkaya, E. (2011). İlköğretim öğretmenlerinin örgütsel bağlılıkları ve performansları arasındaki ilişki [Yayınlanmamış yüksek lisans tezi]. Maltepe Üniversitesi.

[22]. Tabachnick, B. G., & Fidell, L. S. (2007). *Using Multivariate Statistics* (5th ed.). New York: Allyn and Bacon.

[23]. Uludağ, G. (2018). Örgütsel bağlılık ile iş gören performansı ilişkisini incelemeye yönelik bir alan araştırması. *BEÜ SBE Dergisi.,7(1), 171-193.* Erişim adresi: https://dergipark.org.tr/en/pub/gaziticaretturizm/issue/49892/639536

[24]. Uzun, T. (2018). Okullarda algılanan örgütsel destek, örgütsel güven, duygusal bağlılık ve örgütsel vatandaşlık davranışı arasındaki ilişkiler . *OPUS International Journal of Society Researches , 8 (15) , 958987* . DOI: 10.26466/opus.418335

[25]. Yazıcıoğlu, Y. (2004). *SPSS Uygulamalı Bilimsel Araştırma Yöntemleri.* DetayYayıncılık.

[26]. Yelken,T.Y., Kılıç, F., ve Üredi,L. (2010). Stratejik planlama uygulamalarına ilişkin ilk ve orta öğretim okul müdürlerinin görüşleri. *International journal of eurasia social sciences*, *2010*(1), 38-50. Erişim adresi: https://dergipark.org.tr/en/pub/ijoess/iss

[27]. Yıldırım, A. and Simsek, H. (2018). *Sosyal Bilimlerde Nitel Araştırma Yöntemleri (11 baski: 1999-2018)*.

[28]. Yıldız, P. (2019). Örgütsel bağlılık üzerinde örgütsel güven ve örgütsel iletişimin etkisini belirlemeye yönelik bir araştırma [Yüksek Lisans Tezi, Marmara Üniversitesi]. Erişim adresi:https://www.proquest.com/openview/0917cbb573edc802bd23e02e2641d870/1?pqorigsite=gscholar&cbl=18750&diss=y.

[29]. Sharma, P., Kumar, R., & Gupta, M. (2021, October). Impacts of Customer Feedback for Online-Offline Shopping using Machine Learning. In *2021 2nd International Conference on Smart Electronics and Communication (ICOSEC)* (pp. 1696-1703).

[30]. Gupta, M., Kumar, R., & Dewari, S. (2021). Digital twin techniques in recognition of human action using the fusion of convolutional neural network. In *Digital Twin Technology* (pp. 165-186). CRC Press.

[31]. Kour, S., Kumar, R., & Gupta, M. (2021, September). Analysis of student performance using Machine learning Algorithms. In *2021 Third International Conference on Inventive Research in Computing Applications (ICIRCA)* (pp. 1395-1403). IEEE.

[32]. Gupta, M., Kumar, R., Chaudhary, R. K., & Kumari, J. (2021, December). IoT Based Voice Controlled Autonomous Robotic Vehicle Through Google Assistant. In *2021 3rd International Conference on Advances in Computing, Communication Control and Networking (ICAC3N)* (pp. 713-717). IEEE.

[33]. Gupta, M., Kumar, R., Walia, H., & Kaur, G. (2021, October). Airlines based twitter sentiment analysis using deep learning. In *2021 5th International Conference on Information Systems and Computer Networks (ISCON)* (pp. 1-6). IEEE.

[34]. Kumar, R., Gupta, M., Shukla, S., & Yadav, R. K. (2021, September). E-challan automation for RTO using OCR. In *2021 third international conference on inventive research in computing applications (ICIRCA)* (pp. 1-8). IEEE.

[35]. Bawa, H., Singh, P., & Kumar, R. (2012). An Efficient Novel Key management scheme using NchooseK algorithm for Wireless Sensor Networks. *International Journal of Computer Networks & Communications (IJCNC) Vol*, *4*.

[36]. Gupta, M., Wu, H., Arora, S., Gupta, A., Chaudhary, G., & Hua, Q. (2021). Gene mutation classification through text evidence facilitating cancer tumour detection. *Journal of Healthcare Engineering*, *2021*, 1-16.

[37]. Gupta, M., Solanki, V. K., Singh, V. K., & García-Díaz, V. (2018). Data mining approach of accident occurrences identification with effective methodology and implementation. *International Journal of Electrical and Computer Engineering*, *8*(5), 4033.

[38]. Gupta, M., Solanki, V. K., & Singh, V. K. (2017). A novel framework to use association rule mining for classification of traffic accident severity. *Ingeniería solidaria*, *13*(21), 37-44.

[39]. Puneet, Kumar, R., & Gupta, M. (2022). Optical coherence tomography image based eye disease detection using deep convolutional neural network. *Health Information Science and Systems*, *10*(1), 13.

AN OVERVIEW OF THE APPLICATIONS OF BLOCKCHAIN AND AI IN BUSINESS

Ramiz Salama[1*], Sinem Alturjman[2, 3], Chadi Altrjman[4], Fadi Al-Turjman[2, 3]

[1]Department of Computer Engineering, AI and Robotics Institute, Research Center for AI and IoT, Near East University Nicosia, Mersin 10, Turkey
[2]Artificial Intelligence, Software, and Information Systems Engineering Departments, AI and Robotics Institute, Near East University, Nicosia, Mersin10, Turkey
[3]Research Center for AI and IoT, Faculty of Engineering, University of Kyrenia, Kyrenia, Mersin10, Turkey
[4]Department of Chemical Engineering, Waterloo University, ON N2L 3G1, Canada
*Corresponding author Email: ramiz.salama@neu.edu.tr

Abstract: One way that the various business operations could be enhanced as a result of the increasing firm evolution and the most recent Artificial Intelligence is the capacity to create new forms of cooperation (AI). The supply of brand services and even some innovative types of employee and consumer interactions in the workplace are made possible by these rapidly evolving technologies. Because to AI digitization, businesses were simultaneously pushed to focus on their current strategies and actively look for new market opportunities on a regular basis. Although increasing emphasis is being paid to digital technology research in the context of corporate innovation, blockchain technology can safeguard data privacy.BI-AIBT, or business innovation based on blockchain technology and artificial intelligence, is presented in this study with the goal of enhancing business operations and maintaining safe client interactions. Two distinct business sectors comprise a limited number of significant respondents for the collection of qualitative empirical data. BI-AIBT has been examined by contrasting and comparing the ways in which digitization has impacted proposals, business capture, and value development. Concerns about business effectiveness and employee relations can also be resolved with BT's assistance. The experiment's findings demonstrate how digital transformation—which is widely regarded as essential—strengthens business innovation efforts. The numerical result supplied by BI-AIBT improves the ratios for customer behavior analysis (96.3%), customer satisfaction (97.2%), product quality (98.3%), firm development (98.9%), and demand projection (97.1%). Blockchain and artificial intelligence (AI) are the two disruptive technologies of the Fourth Industrial Revolution (IR4.0) that have significantly altered the market. The development of new business models enabled by digitalization holds great potential with the application of blockchain and artificial intelligence. Although there has been research on the usage of blockchain in conjunction with AI, nothing is known about the benefits of this combination for businesses. In an attempt to bridge this gap, this paper explores the benefits and uses of hybrid blockchain and artificial intelligence systems across several industry sectors.This research use bibliometric analysis to determine the essential works on the subject matter based on publications, citations, and significance in the academic community. The conceptual framework of the study is revealed through content analysis, and it is underpinned by four main theme clusters that are focused on supply chains, healthcare, secure transactions, and finance and accounting. Ten possible commercial uses for these technologies are listed in the study's conclusion. Artificial intelligence (AI) algorithms find application in personalized therapy in healthcare, drug development, and global health epidemic forecasting, such as in the case of the ongoing COVID-19 pandemic. Machine learning (ML), a branch of artificial intelligence, enables computers to learn and grow without explicit programming. Machine learning (ML) algorithms have the ability to evaluate massive amounts of data, or "Big data," from electronic health records in order to prevent and identify disease. Wearable

medical technology tracks and stores health data on the cloud continuously. This paper discusses the potential benefits of advanced data analytics and machine learning in light of a recently released study. All trustworthy databases, such as Google Scholar, MEDLINE/PubMed, Scopus, and Web of Science, have been searched.This essay discusses the applications of blockchain, big data, and machine learning as well as their significance for public health monitoring, medical and healthcare surveillance, and case estimations for the COVID-19 pandemic and other epidemics. The research delves at the possible consequences and difficulties that health technologists and medical experts may face when developing futuristic models aimed at improving human well-being.

Keywords: Big data, blockchain, artificial intelligence, machine learning, internet of things.

I Introduction

Artificial intelligence (AI) is a field of research that aims to create machines that are intelligent enough to do complicated activities without the need for human intelligence. As it encourages the adoption of cutting-edge technologies in the Fourth Industrial Revolution (IR 4.0), such as blockchain, cryptocurrency, cloud computing, and the internet of things (IoT) among others, AI is one of the driving forces behind industrial development. In reality, the proliferation of IoT devices, social media, and online apps has sped up the advancement of AI. This data is employed to train machine learning algorithms. However, there are several issues with AI. Particularly in light of countless data breaches and other cases of abuse, privacy has grown to be a serious issue. The Facebook incident, in which the political consulting company Cambridge Analytica unintentionally targeted millions of users, is one instance of this. The technology cannot be evaluated or trusted since it is unable to interact with or communicate with human users—another concern with AI that is becoming more and more prevalent.

Similar to this, blockchain is growing in popularity as a technology with numerous potential uses in a variety of industries. Blockchain, a revolutionary concept that gained notoriety with the creation of bitcoin in 2008, is still transforming a variety of aspects of our lives, including how we interact, keep track of transactions, and make payments automatically. In reality, the blockchain has enabled its users to send money directly among themselves in a safe and secure manner. Additionally, because blockchain is a shared database that is synced across various locations, the execution of smart contracts may make it easier to check rights and compliances. Using consensus techniques like proof of stake or proof of work, blockchains store data in blocks with hash values and timestamps. Proof of stake is less expensive than proof of labor due to its superior energy efficiency. However, the ability for all mining nodes that have a copy of the whole ledger to independently validate each transaction is made feasible by the fact that every transaction on the blockchain is cryptographically signed. As a result of not requiring a centralized authority to authenticate transactions, blockchain is secure and cost-effective.

The acceleration of AI and blockchain integration will change the IR 4.0-inspired future digital generation. Blockchain-based solutions, can provide explainability, privacy, and trust to AI-based applications, whereas AI can improve scalability and security while addressing customization and governance issues. As seen in Table 1, even though blockchain and AI are conceptually distinct in a number of ways, they can be combined to make up for each other's weaknesses. This is how AI and blockchain function as the yin and yang of digital trade, with blockchain facilitating execution, verification, and recording and AI supporting

comprehension, recognizing, and decision-making. As the term suggests, big data refers to enormous amounts of data that are difficult to manage using regular software or web-based solutions. Google will have processed 40,000 queries per second and 44 trillion gigabytes (GB) of data. 3.46 million Searches are performed every day, for a yearly total of 1.2 trillion. The capacity for storage, processing, and analysis has all been expanded. There are numerous definitions of big data, but the most popular and well-known one is by Douglas Laney. Laney emphasized the growth of (big) data in terms of the three "V's" of volume, velocity, and variety. Big data's "huge" component refers to its volume. Patients can define the conditions under which certain researchers may temporarily access specific portions of their medical records with the aid of blockchain technology. Patients can connect to other organizations and have their medical information automatically collected using blockchain technology.

Because of how transparent it is, information may be sent in a secure manner. Clinical trial data, monitoring equipment, electronic medical records for sharing and keeping, mobile health apps, and cloud storage for insurance data are all examples of blockchain applications in the healthcare industry. Blockchain is stable because it would take an unimaginably large amount of processing effort to refigure the altered block and all future blocks if someone wanted to change a block after it had been added to the chain. Along with volume, big data also relates to velocity and diversity. The rate or pace at which data is gathered and made accessible for additional processing is known as velocity. Every business or system has the ability to collect transaction-level data in addition to other types of structured and unstructured information like audio, video, text, or log files. The industry now uses these three "Vs" to describe big data. Big data has recently become incredibly popular all around the world. For a variety of reasons, nearly all study domains, both in academia and in business, produce and analyze enormous amounts of data. The hardest challenge is managing this enormous amount of data, which may be both structured and chaotic .

With such a huge amount of data, using artificial intelligence (AI) algorithms and cutting-edge fusion techniques would make sense. Automating decision-making using machine learning (ML) techniques like neural networks and other AI algorithms would be a significant advancement. Instead of directly coding computer programs using algorithms and statistical models, machine learning research focuses on developing computer systems that learn through inference and patterns. Machine learning has advanced significantly during the past ten years. The most crucial components of machine learning are the data, which form the basis of any model. The forecasts become more accurate as the data becomes more relevant. To get more precise forecasts, we must select an algorithm based on the information and the situation. Blockchain is secure because several copies of the data are kept on different nodes, eliminating the chance of an adversarial user assaulting a centralized structure. These characteristics make blockchain useful for handling healthcare data. It is regarded as a promising method of securely transmitting medical data. However, not every issue involving extremely sensitive data can be solved by blockchain. It has been questioned if blockchain technology has a place in the healthcare industry. Governments may wish to look into potential blockchain applications in the healthcare sector given the technology's recent debut and take into account the challenges posed by the industry's traditionalism. A thorough analysis of the trade-offs is required when developing and deploying blockchain solutions for the healthcare industry.We aim to discuss how machine learning, big data, and blockchain technology operate in this environment as well as potential applications in the fields of medicine, healthcare, and public health.

II Extent of Past Works

The current study makes use of bibliometric analysis to assess the intellectual organization and performance (such as productivity of publications, most well-known articles) of the literature on AI and blockchain integration in business. In order to comprehend a body of literature, bibliometric analysis essentially uses quantitative approaches to analyze bibliometric data, such as publication and citation statistics. The approach is a tried-and-true technique for doing scientific research that can be used to a variety of fields, including business. There are numerous methods for reviewing the literature, but the bibliometric method relies on quantitative analytical methods and a review protocol, making it the most objective. Other review methods, such as critical, either lack review protocols or are only capable of providing subjective interpretations because they lack objective analysis methods, such as thematic analysis. The current study explicitly adheres to the four-step bibliometric analysis methodology, which comprises deciding on an analysis strategy, choosing the right data to use, conducting the analysis, and reporting the findings. The study's methodology is outlined in its broadest sense. The current study combines bibliometric and content analytic techniques to follow the evolution of the business-related literature on AI and blockchain integration. Blockchain technology, business data analytics, and artificial intelligence: Use in the accounting profession and ideas for inclusion into the accounting curriculum. Journal of emerging technologies in accounting. In order to pinpoint the major themes and topics in the research field, the study specifically conducts a performance analysis using a number of bibliometric indicators, such as citations, cite score, impact factor, publication count, and h-index. After this research, the authors read the full text again to conduct a content analysis.

Business innovation occurs when a company implements novel practices, products, or services that profitably expand a market. Business innovation is the process by which a company introduces new trends, services, or other products to foster firm growth. It can entail kicking off the project without any previous planning and utilizing tried-and-true techniques. Technology that has been trained to perform intelligent tasks that have historically been created by people is referred to as AI. Blockchain is a decentralized computer network that collects and stores data to display an event's chronological evolution on a simple and immutable record basis. This innovation can need either altering current practices or developing a whole new method. Blockchain, for instance, may boost confidence, accountability, protection, and privacy in business units by offering a shared and decentralized distributed directory. A blockchain is similar to a register or well-known distributed ledger in that it may store a wide variety of features. A distributed ledger is a set of data that is freely exchanged and synchronized by multiple people over numerous locations, businesses, or topographies. The same technology that is used by blockchain and bitcoin is known as basic appropriated records. A hash, a type of irreversible cryptographic stamp, is used in the blockchain DLT system to track transactions. Every each square in the subsequent block-based compilation of the transactions has a hash of the square before it, linking them together. This leads to the word "blockchain" being occasionally used to refer to transmitted records. These data have a strong connection to both identities and money. The IoT is developing in German and European businesses to enhance industries and business processes. Not to mention, AI improves operations by recognizing and enhancing the results of business processes. The goal of the innovation process is to increase a company's bottom line. By creating new sales opportunities, increasing revenue on existing platforms, saving time and resources, and improving output or performance.

Because existing expertise would become outdated owing to technology advancement, the blockchain invention eliminates it. All business structures in all industries would change if this revolutionary architectural breakthrough were to be widely adopted. Blockchain enables the utilization of processing power, data, and algorithms for various artificial intelligence components, including decentralized markets and collaborative platforms. It might encourage the usage of artificial intelligence (AI) and several other technical developments. Artificial intelligence (AI) refers to tools created in the past to do mental tasks. A decentralized computer network known as blockchain records and saves data in an immutable, transparent ledger system that shows an event chronology. Combining AI and blockchain can enhance machine learning and give AI access to financial resources. Among other things, the blockchain enables safe data exchange and storage. Manufacturing supply chains could undergo a significant transformation as a result of the development of blockchain technology. Middlemen could be eliminated, operations could be reorganized, overall security would increase, and information governance would improve. Artificial intelligence (AI) has the potential to reduce time and costs at work by streamlining and automating repetitive tasks and procedures. A rise in efficiency and productivity overall enables quicker management decisions based on cognitive technology results. Businesses might benefit from using artificial intelligence to provide more individualized customer experiences. Big data analysis is substantially more effective when using AI. It can quickly identify trends in the data, including previous purchases, preferences, credit scores, and other pertinent elements .Building a solid brand and marketing the ideas of digitization and artificial intelligence are challenging tasks.

AI is widely employed in marketing initiatives where speed is essential. Without the assistance of marketing professionals, AI systems might be able to engage with customers more successfully based on information and client data, then deliver personalized messaging at the right time to achieve maximum productivity. Artificial intelligence can help businesses better manage their online reputation and protect their current online presence. Giving brand and service executives access to websites, social networking sites, and other locations allows them to undertake in-depth assessments and research. Conducting the bibliometric-content analysis and presenting the results are the final steps. The authors do bibliometric analysis and network the results using the programs Gephi and VOSviewer. To enhance the presentation of their data, the authors also employ a Python script to generate word clouds that capture the key ideas in bibliographic clusters. Jupyter Notebook and Python 3.7 were both used to run the script and create the word clouds. Each article in each significant subject cluster identified by the bibliometric study was read in its entirety and fairly evaluated. The sections that follow present the results of the bibliometric–content analysis.

III - How AI and Blockchain Technology are used in Business

AI (Artificial Intelligence) and blockchain technology are two separate but powerful technologies that can be used in various ways to enhance and transform businesses. Here's an overview of how they are employed in business:

AI (Artificial Intelligence) in Business:

Customer Service and Support: AI-powered chatbots and virtual assistants can provide 24/7 customer support, answer frequently asked questions, and handle routine inquiries, improving customer satisfaction and reducing response time. Data Analysis and Insights: AI can analyze

large datasets to identify trends, patterns, and correlations that may not be apparent to human analysts. This helps in making data-driven decisions and improving strategies.
Personalization: AI algorithms can analyze user behavior and preferences to provide personalized recommendations, content, and product suggestions, enhancing the customer experience. Automation: AI can automate repetitive and time-consuming tasks, such as data entry, processing invoices, and managing inventory, leading to increased efficiency and cost savings.

Predictive Maintenance: In manufacturing and logistics, AI can predict when equipment or machinery is likely to fail, enabling proactive maintenance and reducing downtime.

Fraud Detection: AI can identify unusual patterns and anomalies in financial transactions, helping to detect and prevent fraud.
Natural Language Processing (NLP): NLP is used for sentiment analysis, content summarization, language translation, and more, making it easier to understand and engage with customers and stakeholders.
Healthcare and Life Sciences: AI is used for drug discovery, disease diagnosis, patient monitoring, and optimizing healthcare operations.
Marketing and Advertising: AI helps in targeted advertising, optimizing ad campaigns, and analyzing consumer behavior to improve marketing strategies.

Blockchain Technology in Business:

Supply Chain Management: Blockchain can be used to create transparent and tamper-proof supply chains, allowing businesses and consumers to track the origin and journey of products from manufacturer to end user.
Smart Contracts: Smart contracts are self-executing contracts with the terms of the agreement between buyer and seller directly written into code. They automate contract execution and reduce the need for intermediaries.
Digital Identity Verification: Blockchain can be used for secure and decentralized digital identity verification, making it easier to establish trust in online interactions and reducing identity theft. Cross-Border Payments: Blockchain can facilitate faster and more cost-effective cross-border transactions by eliminating intermediaries and reducing currency conversion fees.

Intellectual Property Protection: Businesses can use blockchain to prove the authenticity and ownership of intellectual property, including patents, copyrights, and trademarks.
Voting Systems: Some countries are exploring the use of blockchain for secure and transparent voting systems, reducing the risk of fraud and ensuring the integrity of elections.
Real Estate and Property Records: Blockchain can streamline the process of property transfer, record-keeping, and title management by ensuring a secure and immutable ledger.
Tokenization of Assets: Businesses can tokenize assets like real estate, art, or company shares on a blockchain, making them more accessible and liquid for investors.
Data Security and Privacy: Blockchain can enhance data security and privacy, allowing individuals to have greater control over their personal information.
Both AI and blockchain technology offer a range of opportunities for businesses to improve operations, enhance security, and create new revenue streams. The choice to implement them depends on specific business needs, goals, and the industry in which the business operates.

VI. Results and Discussion

The social and economic institutions that support businesses as well as the way they are operated have the potential to be significantly changed by blockchain technology. We'll look at how, in some circumstances, block chain can be utilized to quickly validate a transaction's properties. The blockchain provides an authenticating system that is reliable. Your customers' and your employees' electronic IDs make it simple to verify their identities. When this data is kept on a public blockchain, the risk of identity fraud, financial fraud, theft, and other cybercrimes is decreased. Blockchain and artificial intelligence-based business innovation (BI-AIBT) have been proposed as ways to improve corporate operations and provide a secure link with a variety of clients. In the collection of qualitative analytical data, there are just a few noteworthy respondents from two different business sectors. The corporation evaluated BI-AIBT and contrasted and compared how digitization affected value generation, proposal, and business capture. Additionally, BT can improve the way organizational strengths and talents interact. A thorough analysis of the literature and localization strategies for peer-reviewed studies serve to highlight the business innovation. SMEs can experience sustainable productivity development in the modern economy if new technologies are employed in the workplace. By implementing a number of strategies, including working with other businesses and academic organizations, businesses can become even more imaginative. Additionally, the majority of SMEs in Moldova are unaware of the need to market research findings and implement innovations based on scientific discoveries. Big-data analytics (BDA), should be given much more attention since it may support business planning and provide useful data for boosting service innovation. They investigated the application of thorough service innovation analytics. Actual customer requests were gathered through the digital service channel by the emphasis using analytical data characteristics. Research on business transformations, applied mathematics, business engineering, financial science, and the global business infrastructure is done using the applied holistic mathematical model (AHMM) developed by Trad et al. Chandrachai, Triukose, One instance of how the suggested formality of AHMM replicated many aspects of human cognition was the heuristic decision-making process, which mostly depended on beam examination. By supporting a thorough separation process, synchronization of various EA methodologies, and transition strategies, the AHMM facilitated business transformation operations. It is unique because of this.

The model-narrative review (MNR) technique, according to Hakala et al, may link extensive work on the market, entrepreneurial, and innovation contexts to comprehend this evolving narrative. They contributed to the opening up and conceptual clarity of the language around the environment by disclosing a number of implicit interpretations and basic presumptions. MNR as a whole synthesizes and carefully considers the parallels and differences among linked ideas, resulting in the development of a method for developing model narratives that offer room for alternative research studies.

Improvised marketing interventions (IMIs) are defined as social media actions that are created and executed in real-time close to an actual incident. Five multi-method assessments were conducted; their findings were recorded along with analytical information and simulated tests. The IMI's effectiveness was evidenced by the laughter and unexpected results. The findings showed both the IMI's potential for social media and the attributes that companies need to have in order to benefit from proactive online networking. According to Mustafa et al. Typical FinTech companies may present opportunities as well as challenges for Islamic banking systems. According to the results of this investigation, Islamic financial institutions are more

likely to see Islamic FinTech firms as partners than as rivals. Adaptive Hybridized Intelligent Computational Models (AHICM) were developed by to study consumer behavior for business expansion. A detailed examination of market segmentation and customer needs is necessary for product advancements, innovative concepts, and societal revolutions. The blockchain-based integrative safety mechanism (BISM), which intends to provide secure access management and privacy protection for both products and individuals, is described. While privacy protection depends on the robustness of response times, user access procedures are based on the state of virtual resources at different points in time. SMEs, BDA, AHMM, MNR, and IMI are among the established business strategies that have been outperformed by Business Innovation based on Artificial Intelligence and Blockchain Technology (BI-AIBT). The demand forecast ratio, product quality ratio, business development ratio, customer behavior analysis ratio, and customer satisfaction ratio all have potential for improvement, according to BI-AIBT. A data-collection technique called blockchain makes it hard or impossible to alter, hack, or cheat the system. A blockchain is a collection of duplicate digital ledgers that have been dispersed over

the whole computer network. Blockchain, also known as Distributed Ledger Technology (DLT), uses decentralization and cryptographic hashing to make it simple and impossible to change the past of a relatively complex resource. The disclosed method concurrently grants everyone access to the record by creating a decentralized appropriation chain. Only a few non-financial uses for blockchain technology include supply chain management and digital identity. Supply chain management promotes effectiveness, teamwork, and superior outcomes. Additionally, it lowers costs. It encourages companies to better meet customer demands and more swiftly manage demand, stock distribution, interference management, and expense control. With the use of blockchain technology, consumers may have more control over their own actions. There is no chance for any focus point to take the client's personality into consideration, and customers must consent before a company may use their information. The most current research demonstrates the benefits of combining blockchain technology with IoT and AI. For instance, the system architecture of many Internet of Things (IoT) devices could be improved by the use of blockchain technology. Making judgments using computers IoT creates flexible instruments that effectively mimic smart leadership with almost no human resistance.

While IoT manages their internet communication, AI allows the devices to learn from their data and experience. IoT makes it possible for Internet-connected devices to communicate information with private blockchain firms so that secure records of shared transactions may be updated. Thanks to IBM Blockchain, your coworkers can access and share IoT data with you, but only you and the leaders will need to serve as the primary central authority. Most of the time, the interrelationships between blockchain, IoT, and AI are neglected, and each technology is applied on its own. These technologies could, and in a perfect world, ought to, be developed simultaneously. There may be a connection between IoT and AI in that while IoT gathers and feeds data, AI improves corporate processes and legal frameworks through Blockchain, constructing infrastructure and defining engagement standards. It demonstrates how blockchain technology and artificial intelligence are being applied in business. Coordination of commercial transactions between demand and resource providers may be accomplished using blockchain technology. The resources that are available will determine the project manager who will put together the tools required to do the assignment. Finding stronger company motivators is the main benefit of having solid, healthy supplier relationships. The likelihood that you will acquire enthusiastic dedication, correct evaluation, and excellent terms increases as you and your suppliers become more familiar with one another. In this scenario, blockchain

is primarily utilized to sustain supply chain connections between the needs of many consumers and many providers.

Customers can create new demand using the decentralized order engine, and producers can provide new items as part of a new transaction using the decentralized product engine. Because a blockchain's centralization or decentralization often pertains to the rights of participants in the record, it is also a design issue. Anyone can participate and make decisions in a decentralized organization. Only recognized and well-known groups are allowed to take measures on the record in a united organization. To confirm and secure the data patterns for transactions between providers and consumers, the smart contract mechanism serves as an authenticating protocol between the two engines. Commercially accessible technology might not always be able to offer the necessary level of security. "Commercial-off-the-rack" (COTS) programming is a term used in the business world to describe programming that is immediately accessible for purchase. In order to upgrade, replace constraining frameworks, and carry out other duties, public area associations are increasingly relying on COTS applications. A protection plan that is mission-based is a solution that can be adjusted to meet specific needs. It serves as an example of how an additional layer of specialized security could safeguard the data on a company's network. This personalized method has the advantage of allowing the employee's agent (EA) to control the rate of public and private key renewal and monitor key creation parameters. Employee agents (EAs) are persons who have been given permission to act as another person's agent by their employer. For instance, even when no other representatives are permitted, you can designate a worker as an authorized expert to allow them to make substantial purchases on the company's behalf.

Accounting for indirect costs is known as ICA. The ICA only grants authorized EAs restricted access to each database cluster. a method of gathering complex data that needs at least one mathematical operation and a secret key or other "key" to decode the data To prevent identity theft and extortion, websites that communicate sensitive data, such as bank account numbers and Mastercard numbers, should always encrypt the data. Before entering the database, the data is encrypted. Each data cluster is encrypted with a different key in order to restrict access to the data to only authorized workstations. Thanks to ICA, the firewall in the receiving state can access customer and business data from the internet or extranets. The secret key to utilize when symmetrically encrypting data is specified by the ICA. Secret keys are generated for symmetric key encryption while the ICA is processing in this mode. Information about corporate and customer accounts can be stored in databases using passwords. The primary delivery's personnel are under the ICA's control. Location or account balance are the two ways that EAs can be assigned to an account. While in the transmitting state, the ICA sends the secret keys of the associated EAs. Using a secret key, the ICA encrypts data collected from external networks. The ICA sends data to the clustered database.

The company accounts for each employee's workstation are under their control. To exchange data with other team members, the sender encrypts it using the recipient's public key and decrypts it using the recipient's private key. Data is protected from internal illicit use by this upgraded authentication layer. It also demonstrates how blockchain marketing has evolved. Its key focuses are peer-to-peer communication, shifting market dynamics, and getting rid of middlemen that limit and filter data sources and raise costs. Intermediaries are helped by this mediation. By facilitating access to data and generating widely used, immutable data archives, blockchain technology can enhance the quality of data. Information quality includes a wide range of components that affect an association's ability to function [21]- [24]. Reports are

unreliable when data isn't acquired properly. Frameworks with divergent preset values obstruct real risk awareness. Clarvonyt aids in resolving these problems and improves each piece of work. Blockchain technology has the ability to drastically impact corporate experiences through data exchange, information privacy, and a customer-focused strategy. Innovative plans are put in place to ensure client pleasure and potential value.

With the development of the internet, business practices for marketing their goods and services have changed. Due to technology, which has also produced new electronic intermediaries, traditional middlemen have lost some of their significance. Access to the internet has also made it easier for new online intermediaries to provide customers innovative goods and services. In order to respond to RQ1, which asks what the publishing productivity of research on AI is and blockchain integration for business, the study examines all of the publications in the field organized by year [25] – [29]. Scopus provided the bibliometric data that was used in the inquiry. Information on scientific publications, including publication details (such as the title, abstract, keywords, and year) and citation details (such as the author, document, and journal citation total) are included in a subset of big data called bibliometric data.

IV. Conclusion

Among the key technologies of Industry 4.0 are blockchain and artificial intelligence (AI). Academics and practitioners are interested in amalgamation, even though the two technologies are very different from one another. But there is a lack of research on the business applications of blockchain-AI systems that gathers and evaluates the most recent discoveries. The current study employed a bibliometric-content analysis to close this gap and found five important discoveries. According to the report, blockchain and artificial intelligence (AI) are IR 4.0 technologies that were first mentioned in 2016. Early research combining the two technologies for commercial application first appeared in 2017 and only really took off in 2019 and beyond. A plethora of research on the topic supports the study's conclusion that the combination of AI with blockchain holds significant promise for business applications. The second is the article by Liu et al. about blockchain and AI applications in healthcare. The paper on performance optimization for blockchain-enabled IoT systems, as well as work on a blockchain-based LSTM credit evaluation system.

Prospective authors should be familiar with the field's fundamental works in order to position and organize future research in novel ways that deepen our comprehension of past findings. Thirdly, the analysis shows that "blockchain and machine learning," "blockchain and smart contracts," and "blockchain and security" are the three most popular research topics. To further emphasize the potential and importance of combining blockchain and AI in business, triangulation was used to find that "blockchain and machine learning" has the strongest association in the corpus and that machine learning is the AI technology that appears to be most relevant and salient. Fourth, the study deconstructs four major topic clusters—smart healthcare, safe transactions, finance and accounting, and IR 4.0 and supply chains—that form the conceptual basis of research on the integration of AI and blockchain for business. Two of the study's clusters, finance and accounting and smart healthcare, are distinct and industry-specific, while three of the clusters, supply chains, and IR 4.0, are general and cross-industry. Research on AI and blockchain integration for business is still in its infancy because there aren't many sizable topic clusters. Therefore, research that encourages the field's ongoing evolution to enhance existing clusters and encourage the emergence of new clusters is much appreciated.

Fifth, the paper lists eleven companies for which earlier studies on the subject have suggested integrating blockchain with artificial intelligence.

These industries include intellectual property rights, marketing, management, supply chain management, e-commerce, finance and accounting, and healthcare. I think this post has significantly advanced that goal in four different ways. This study first shows that the field is still developing and has plenty of opportunity for growth and additional research by mapping the publication productivity of AI and blockchain integration for business particular. Second, this article has made it possible for future study to expand on the ground-breaking discoveries it presents by presenting the key elements of the field's research. Third, by compiling the most well-liked topics and subjects about AI and blockchain integration for business, this website provides aspiring writers with an up-to-date summary of the literature in the field. Ultimately, ten business opportunities for integrating blockchain and AI have been identified by our research. Business executives wishing to use academic research to identify possible organizational transformation opportunities using the two IR 4.0 technologies should find these applications useful.A wide range of stakeholders, including corporate management, blockchain and AI technologists, IT vendors, and aspiring academics, will be significantly impacted by this essay. Developers working with blockchain and AI might have a better knowledge of how

fusing these two technologies enhances organizational efficacy. Blockchain and AI developers may work together to create automated, decentralized business apps that give better client privacy and confidentiality protection, higher performance, and better governance.Additionally, IT providers will be better equipped to understand how to integrate AI and blockchain into organizations by recognizing the market for these business solutions and highlighting the advantages they bring. Lastly, future scholars will be able to advance knowledge in the field by expanding on the current overview of AI and blockchain integration in business and investigating new subjects that would create new research streams or enrich current research streams in the field.

This article presents professionals and academics with cutting-edge views regarding the possibilities for combining blockchain technology and artificial intelligence to enhance the growth, robustness, and resilience of business operations. However, this poem, like others, is conscious of its limitations.The quality and comprehensiveness of the source, in this case Scopus, is the main constraint on the data in this article.Recall that Scopus was not designed for bibliometric research, and as such, it is a scientific database that might contain (inadvertent) inaccuracies. As advised, the authors removed duplicates and incorrect entries from the bibliometric data they downloaded from Scopus in order to minimize any (unintentional) inaccuracies. Second, the industry has advanced revolutionaryly with the integration of artificial intelligence and blockchain technology. Its application and integration in this field will probably rise significantly, which is likely to result in the creation of new research fields. Therefore, to stay up to date on recent advancements in the subject, prospective authors should utilize the supplied search keyword in addition to the review insights provided here.

Future researchers on the business use of AI and blockchain integration are urged to concentrate their efforts on figuring out how such an integration might be applied from a business rather than an engineering lens, as the study presented here highlighted the lack of insights emerging from business research. In order to promote such research, this paper highlights the need for more studies that address the non-exhaustive research problems on AI and blockchain integration using a business lens generally and by cluster.

References

[1]. Kaur, M., & Gupta, S. (2021). Blockchain technology for convergence: an overview, applications, and challenges. Blockchain and AI Technology in the Industrial Internet of Things, 1-17.

[2]. Akter, S., Michael, K., Uddin, M. R., McCarthy, G., & Rahman, M. (2022). Transforming business using digital innovations: The application of AI, blockchain, cloud and data analytics. Annals of Operations Research, 1-33.

[3]. Hussain, A. A., & Al-Turjman, F. (2021). Artificial intelligence and blockchain: A review. Transactions on emerging telecommunications technologies, 32(9), e4268.

[4]. Sharma, P., Jindal, R., & Borah, M. D. (2022). A review of blockchain-based applications and challenges. Wireless Personal Communications, 1-43.

[5]. Javaid, M., Haleem, A., Singh, R. P., Khan, S., & Suman, R. (2021). Blockchain technology applications for Industry 4.0: A literature-based review. Blockchain: Research and Applications, 2(4), 100027.

[6]. Marwala, T., & Xing, B. (2018). Blockchain and artificial intelligence. arXiv preprint arXiv:1802.04451.

[7]. Hacioglu, U. (2020). Digital business strategies in blockchain ecosystems. Springer International Publishing, DOI, 10, 978-3.

[8]. Swan, M. (2018). Blockchain for business: Next-generation enterprise artificial intelligence systems. In Advances in computers (Vol. 111, pp. 121-162). Elsevier.

[9]. Shinde, R., Patil, S., Kotecha, K., & Ruikar, K. (2021). Blockchain for securing ai applications and open innovations. Journal of Open Innovation: Technology, Market, and Complexity, 7(3), 189.

[10]. Rabah, K. (2018). Convergence of AI, IoT, big data and blockchain: a review. The lake institute Journal, 1(1), 1-18.

[11]. Makridakis, S., & Christodoulou, K. (2019). Blockchain: Current challenges and future prospects/applications. Future Internet, 11(12), 258.

[12]. Corea, F. (2019). Applied artificial intelligence: Where AI can be used in business (Vol. 1).
Springer International Publishing.

[13]. Lopes, V., & Alexandre, L. A. (2018). An overview of blockchain integration with robotics and artificial intelligence. arXiv preprint arXiv:1810.00329.

[14]. Attaran, M., & Gunasekaran, A. (2019). Applications of blockchain technology in business: challenges and opportunities.

[15]. Pal, A., Tiwari, C. K., & Haldar, N. (2021). Blockchain for business management: Applications, challenges and potentials. The Journal of High Technology Management Research, 32(2), 100414.

[16]. Karger, E. (2020, December). Combining Blockchain and Artificial Intelligence-Literature Review and State of the Art. In ICIS.

[17]. Sandner, P., Gross, J., & Richter, R. (2020). Convergence of blockchain, IoT, and AI. Frontiers in Blockchain, 3, 522600.

[18]. Prof.DUX available online: https://dux.aiiot.website/

[19]. Al-Turjman, F. (2023). Enhancing Higher Education Through Prof. DUX: A Practical Approach to Personalized AI Assisted Learning. NEU Journal for Artificial Intelligence and Internet of Things, 1(2).

[20]. Al-Turjman, F. (2023). Familiarizing Teachers/Learners with AI-assisted Learning and Evaluation Implementations–Prof. DUX a Use Case. NEU Journal for Artificial Intelligence and Internet of Things, 2(4).

[21]. Gupta, M., Jain, R., Kumari, M., & Narula, G. (2021). Securing healthcare data by using blockchain. *Applications of blockchain in healthcare*, 93-114.

[22]. Sharma, P., Kumar, R., & Gupta, M. (2021, October). Impacts of Customer Feedback for Online-Offline Shopping using Machine Learning. In *2021 2nd International Conference on Smart Electronics and Communication (ICOSEC)* (pp. 1696-1703). IEEE.

[23]. Gupta, M., Kumar, R., & Dewari, S. (2021). Digital twin techniques in recognition of human action using the fusion of convolutional neural network. In *Digital Twin Technology* (pp. 165186). CRC Press.

[24]. Kour, S., Kumar, R., & Gupta, M. (2021, September). Analysis of student performance using Machine learning Algorithms. In *2021 Third International Conference on Inventive Research in Computing Applications (ICIRCA)* (pp. 1395-1403). IEEE.

[25]. Gupta, M., Kumar, R., Chaudhary, R. K., & Kumari, J. (2021, December). IoT Based Voice Controlled Autonomous Robotic Vehicle Through Google Assistant. In *2021 3rd International Conference on Advances in Computing, Communication Control and Networking (ICAC3N)* (pp. 713-717). IEEE.

[26]. Gupta, M., Kumar, R., Walia, H., & Kaur, G. (2021, October). Airlines based twitter sentiment analysis using deep learning. In *2021 5th International Conference on Information Systems and Computer Networks (ISCON)* (pp. 1-6). IEEE.

[27]. Kumar, R., Gupta, M., Shukla, S., & Yadav, R. K. (2021, September). E-challan automation for RTO using OCR. In *2021 third international conference on inventive research in computing applications (ICIRCA)* (pp. 1-8). IEEE.

[28]. Bawa, H., Singh, P., & Kumar, R. (2012). An Efficient Novel Key management scheme using NchooseK algorithm for Wireless Sensor Networks. *International Journal of Computer Networks & Communications (IJCNC) Vol*, *4*.

[29]. Gupta, M., Chaudhary, G., & de Albuquerque, V. H. C. (Eds.). (2021). *Smart Healthcare Monitoring Using IoT with 5G: Challenges, Directions, and Future Predictions*. CRC Press.

AN EXECUTION OF INTRUSION DETECTION USING BOLTZMANN MACHINE AND ITS APPLICATIONS

Shailendra Singh Gaur[1], C. M. Sharma[2], Varsha Sharma[3]

Bhagwan Parshuram Institute of Technology, GGSIPU, Delhi
shailendrasinghgaur@bpitindia.com, cmsharma@bpitindia.com,
varshasharma@bpitindia.com

Abstract: In today's era wireless sensor networks are very challenging to reduce the attack and risk of getting affected. Several methods for image compression are used to solve the WSN problems like RBM, DRBM, CRBM and many more. Most of the image compression algorithms are random content, change in image and results in low quality of images after deducting. Multilayer random Boltzmann machine learning network is implemented in this paper to solve the intrusion detection in network traffic to improve the accuracy of the algorithm, which will help us to understand the different types of attacks.

Keywords: *WSN, Restricted Boltzmann Machine Learning Algorithm, Intrusions Detection*

1. INTRODUCTION

Wireless Sensor Networks monitor sound, motion, pressure and temperature that are physical or environmental conditions. Advancement in the technology has led to loss of important information and exposure of sensitive data. It also required to create a system which can reduce attack and detect risk on security. Wireless Sensor Networks (WSNs) are self- configured and infrastructure-less wireless network to monitor the physical or environmental conditions such as sound, temperature, pressure, motion, and vibration etc. With the advancement of technology in recent years, the various attacks over these data have increased rapidly and WSN has gained attention too. This often leads to loss of important information and exposure of sensitive data. Thus, a system is required to be placed which can automate the process of attack and their detection and thus reduce the risk on security teams.

2. OBJECTIVES

- The use of AI along with Data science and Machine learning prioritizes the security alerts and automate the responses significantly to reduce the stress placed on security teams.
- AI and machine learning is used widely in data science application and skill sets to identify the behavior pattern that can't be detect by the preset rules.
- ML algorithm is allowed to develop a defense response after analyzing and processing the previous cyber-attack data.
- Encryption techniques are needed to operate on many different types of data, both user and machine generated inputs with different analysis tools and big data storage formats.

3. MATERIALS AND METHODOLOGY

In the absence of a Standard Dataset for Attack detection in WSNs, the appropriate dataset found for the purpose was NSL- KDD dataset. This data set contains the records of the internet traffic seen by a simple intrusion detection network and is the ghosts of the traffic encountered by a real IDS and just the traces of its existence remained. The dataset consists of 125973 rows and 43 columns. No missing values were found in any of the columns. Three features were

object datatype which were unsuitable for machine learning algorithms, hence would require pre-processing steps. All other features were either integer or float values which were directly used. Type was selected as the target ones. All other features present were used for determination of type of attack.

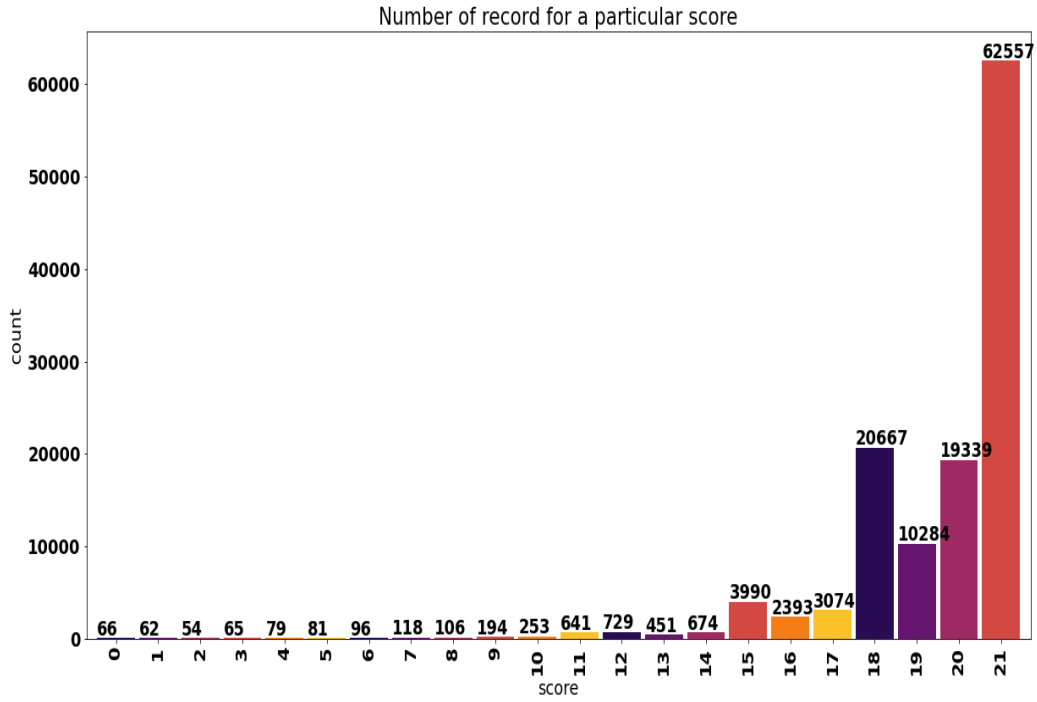


Fig.1. Score Distribution of Attacks for a particular record

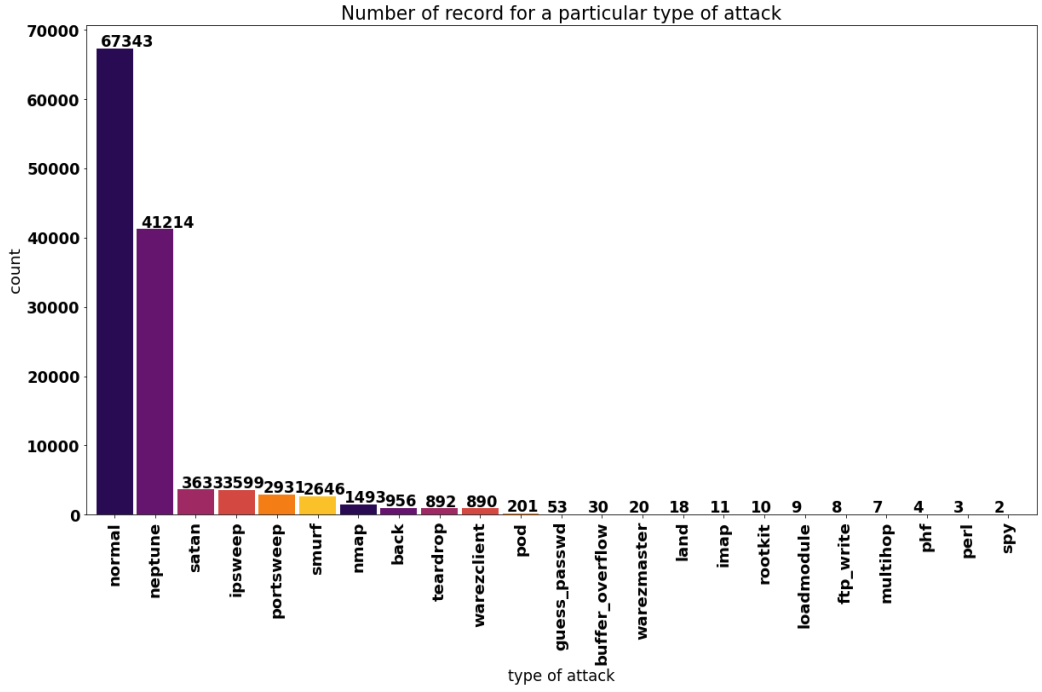


Fig. 2. Attack Frequency for a particular type of attacks

The dataset selected was first used for pre-processing. All the features in object format were one-hot encoded. Therefore, Restricted Boltzmann Machine Algorithm is applied to a processed dataset. The various WSN image analysis techniques are Auto encoder, RBM, NMF,

LSNMF and PNMF based image compression techniques. Restricted Boltzmann machines (RBMs) are unsupervised machine learning algorithms. These algorithms are used to represent the internal representation of data and also sample the output of visible units and hidden layer input or vice versa. RBM is used for classification and generation.

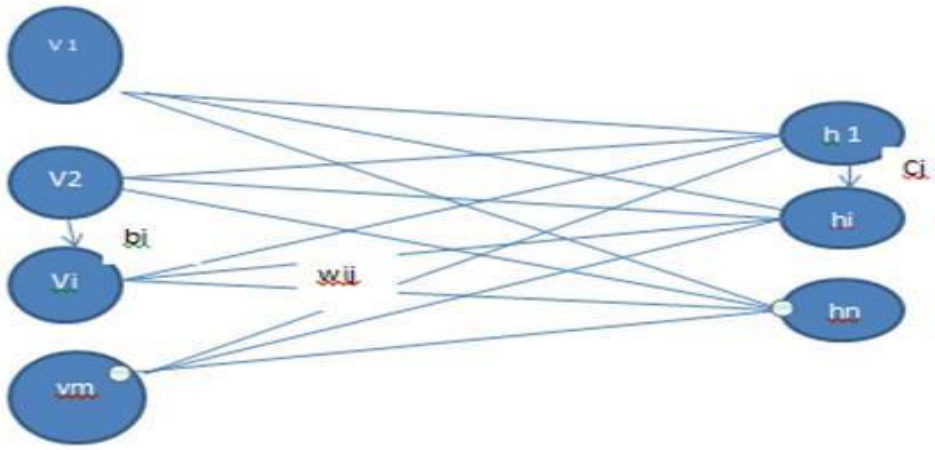


Fig.3. Restricted Boltzmann Machine Architecture

Here i is visible in nit and j is hidden unit and wij belongs to W where W belongs to Rm x n set of weights from hidden to visible units. The bias unit is represented by bi belongs to b. And the hidden unit is cj belongs to c. This algorithm used hidden h and joint vector v distribution which is proportional to exponential of negative energy of configuration.

Before compression of image, we need to build a matrix factorization algorithm which converts the user matrix into 2 lower D matrices. Where H is the m users x k latent factor and W is latent factor into n user item matrix. Resultant is calculated by multiplying H x W that is R. K represents the model capacity and increases in K factor represents the improvement in prediction chances and if k is too high, the model is considered to be fit. In RBM all parameters are set to be 10 epochs with no predefined weight.

We pass the input data from each of the visible node to the hidden layer.

Steps for Restricted Boltzmann Machine Architecture Algorithm:

- We multiply the input data by the weight assigned to the hidden layer, add the bias term and applying an activation function like sigmoid or softmax activation function.
- Forward propagation gives us probability of output for a given weight w ,this gives P(a|x) for weights w.
- During back propagation we reconstruct the input. During reconstruction RBM estimates the probability of input x given activation a, this gives us P(x|a) for weight w.

Reconstruction is about the probability distribution of the original input. •We compare the difference between input and reconstruction using KL divergence.

A network intrusion detection system is designed to detect any breach in the system within the network and also monitor and analyze the data. 10:1 I'd the ratio of attack these days. High accuracy results in high true negative ratio having low number of true positive. In this paper we use RBM as a classifier where NetFlow network traffic info is used to analyze the network.

3.1 Data Analysis

Network traffic collection is the first and key step in intrusion detection. The location of the network collector plays a decisive role in the efficiency of intrusion detection. To provide the best protection for the target host and network, the proposed intrusion detection model is deployed on the nearest victim's router or switch to monitor the inbound network traffic. During the training phase, the collected data samples are categorized according to the transport layer and network layer protocol and are labeled based on the domain knowledge. However, the data collected during the test phase are classified according to the trained hybrid model.

4. REVIEW

Theis, Lucas [7] proposed a method to compress the images using an autoencoder. The technique they have introduced results in the lossy images. Compressive Autoencoder Architecture Younghoon [8](2018) proposed a method based on wireless sensor networks. They are capturing images from a camera sensor and transmit via a wireless sensor network. They are not using any compression algorithm before transferring the data. Shakev et al. has used the rMQTT protocol in WSN. Ramnik et al.2017 [9] proposed WSN image transfer model and used cross layer optimization to transfer the images with limited capability of sensor nodes. Hasin et al.2017 [10] implemented using MQTT, a real time data acquisition. Sahoo et al. 2017[11] used IOT to implement the WSN and used Zigbee to transmit images but zigbee transmit image in 2.4kb/s. Tramel et al. used RBM to solve the CS observation matching problem and found in comparison to Variational autoencoder and generative adversarial networks that RBM is the simplest model to use with minimum no of parameters, even RBM consumes very less energy.

5. ANALYSIS

In this study intrusion detection of network traffic where NSL-KDD dataset is used which contain record of network traffic RBM algorithm is implemented over this dataset. Achieved 99% accuracy. The proposed system showed an overall training accuracy of 99.125% and training loss of 0.029. Therefore the proposed system shows promising results towards intrusion detection in traffic over internet [12] – [20].

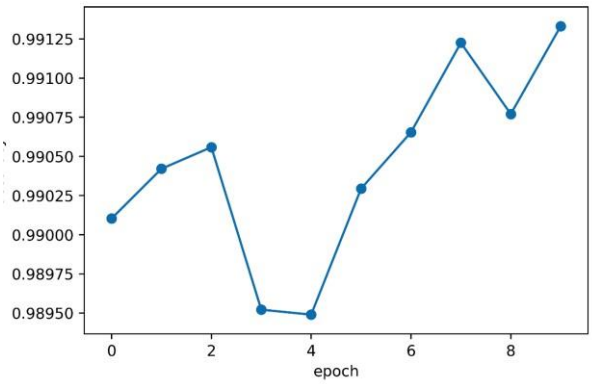


Fig .5. Accuracy of the model

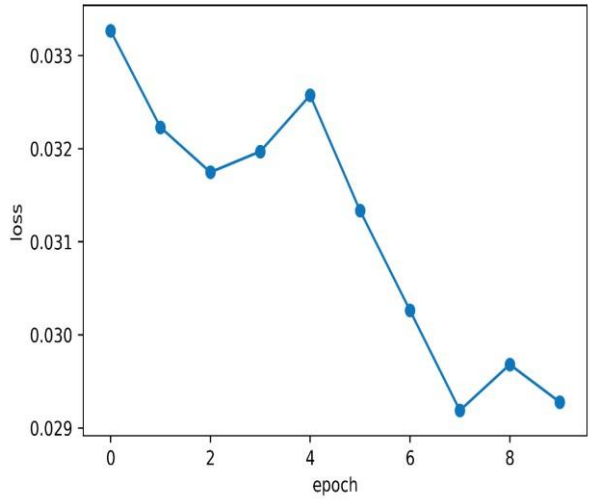


Fig .6. Loss of the model

6. CONCLUSION

The processing capacity and power of nodes in a Wireless Sensor Network (WSN) are restricted. The quality of the images is deficient, and the contents of the images may vary after decoding when we apply image compression algorithms in WSN. Wireless Sensor Nodes (WSNs) play a very significant role in our day-to-day applications. As the resources in each sensor node are limited, it is challenging situation to reduce the energy consumption and increase the lifetime of a sensor node. Currently, the Image Compression algorithms in WSNs are subject to the random changes in image contents. It is difficult to describe various images in the real world with only one kind of image compression. The neural network model is adopted in WSNs to compress the images. In this study we implemented RBM algorithm and achieved 99% accuracy.

7.FUTURE SCOPE

As a future work, we can focus on the following points:

- Reducing the systematic error of the model.
- VAE and GAN deep learning model is used for future work which can help to reduce the semantic error.

- COAP transfer protocol can also be implemented to enhance the security and reliability of data.

REFERENCES

[1]. S. Aruna Deepthi, E.Sreenivasa Rao, M.N.Giriprasad, Design of various Image Compression Methods in Wireless Sensor Networks, International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-9 Issue-1, October 2019.

[2]. Cheng, Chunling, et al. "A multilayer improved RBM network based image compression method in wireless sensor networks." International Journal of Distributed Sensor Networks, vol. 2016, 2016.

[3]. I. Butun, S. D. Morgera, and R. Sankar. A survey of intrusion detection systems in wireless sensor networks. IEEE Communications Surveys Tutorials, 16(1):266–282, First 2014.

[4]. S. R. J. Ramson and D. J. Moni. Applications of wireless sensor networks a survey. In 2017 International Conference on Innovations in Electrical, Electronics, Instrumentation and Media Technology (ICEEIMT), pages 325–329, Feb 2017.

[5]. A. Gouveia and M. Correia. A Systematic Approach for the Application of Restricted Boltzmann Machines in Network Intrusion Detection, volume 10305. 05 2017.

[6]. Lin Bao,1,2 Xiaoyan Sun , 1 Yang Chen,1 Guangyi Man,1 and Hui Shao1, Restricted Boltzmann MachineAssisted Estimation of Distribution Algorithm for Complex Problems, Hindawi Complexity Volume 2018, Article ID 2609014, 13 pages https://doi.org/10.1155/2018/2609014.

[7]. Jianlin Liu, Fenxiong Chen * and Dianhong Wang, Data Compression Based on Stacked RBM-AE Model for Wireless Sensor Networks, Sensors 2018, 18, 4273; doi:10.3390/s18124273 www.mdpi.com/journal/sensors

[8]. Norouzi, M.; Ranjbar, M.; Mori, G. Stacks of convolutional restricted boltzmann machines for shift invariant feature learning. In Proceedings of the 2009 IEEE Conference on Computer Vision and Pattern Recognition (CVPR 2009), Miami, FL, USA, 20–25 June 2009; pp. 2735–2742.

[9]. Hinton, G.E.; Salakhutdinov, R.R. A better way to pretrain deep boltzmann machines. In Proceedings of the Twenty-Sixth Conference on Neural Information Processing Systems, Lake Tahoe, NV, USA, 3–8 December 2012; pp. 2447–2455.

[10]. Tramel, E.W.; Manoel, A.; Caltagirone, F.; Gabrié, M.; Krzakala, F. Inferring sparsity: Compressed sensing using generalized restricted Boltzmann machines.

[11]. M. Tavallaee, E. Bagheri, W. Lu, and A. Ghorbani, “A Detailed Analysis of the KDD CUP 99 Data Set,” Submitted to Second IEEE Symposium on Computational Intelligence for Security and Defense Applications (CISDA), 2009.

[12]. Gupta, M., Kumar, R., & Dewari, S. (2021). Digital twin techniques in recognition of human action using the fusion of convolutional neural network. In *Digital Twin Technology* (pp. 165-186). CRC Press.

[13]. Kour, S., Kumar, R., & Gupta, M. (2021, September). Analysis of student performance using Machine learning Algorithms. In *2021 Third International Conference on Inventive Research in Computing Applications (ICIRCA)* (pp. 1395-1403). IEEE.

[14]. Gupta, M., Kumar, R., Chaudhary, R. K., & Kumari, J. (2021, December). IoT Based Voice Controlled Autonomous Robotic Vehicle Through Google Assistant. In *2021 3rd*

International Conference on Advances in Computing, Communication Control and Networking (ICAC3N) (pp. 713-717). IEEE.

[15]. Gupta, M., Kumar, R., Walia, H., & Kaur, G. (2021, October). Airlines based twitter sentiment analysis using deep learning. In *2021 5th International Conference on Information Systems and Computer Networks (ISCON)* (pp. 1-6). IEEE.

[16]. Kumar, R., Gupta, M., Shukla, S., & Yadav, R. K. (2021, September). E-challan automation for RTO using OCR. In *2021 third international conference on inventive research in computing applications (ICIRCA)* (pp. 1-8). IEEE.

[17]. Bawa, H., Singh, P., & Kumar, R. (2012). An Efficient Novel Key management scheme using NchooseK algorithm for Wireless Sensor Networks. *International Journal of Computer Networks & Communications (IJCNC) Vol*, *4*.

[18]. Gupta, M., Solanki, V. K., Singh, V. K., & García-Díaz, V. (2018). Data mining approach of accident occurrences identification with effective methodology and implementation. *International Journal of Electrical and Computer Engineering*, *8*(5), 4033.

[19]. Gupta, M., Solanki, V. K., & Singh, V. K. (2017). A novel framework to use association rule mining for classification of traffic accident severity. *Ingeniería solidaria*, *13*(21), 37-44.

[20]. Puneet, Kumar, R., & Gupta, M. (2022). Optical coherence tomography image based eye disease detection using deep convolutional neural network. *Health Information Science and Systems*, *10*(1), 13.

DISTRIBUTED MOBILE CLOUD COMPUTING SERVICES USING BLOCKCHAIN TECHNOLOGY

Ramiz Salama[1*], Sinem Alturjman[2, 3], Chadi Altrjman[4], Fadi Al-Turjman[2, 3]

[1]Department of Computer Engineering, AI and Robotics Institute, Research Center for AI and IoT, Near East University Nicosia, Mersin 10, Turkey
[2]Artificial Intelligence, Software, and Information Systems Engineering Departments, AI and Robotics Institute, Near East University, Nicosia, Mersin10, Turkey
[3]Research Center for AI and IoT, Faculty of Engineering, University of Kyrenia, Kyrenia, Mersin10, Turkey
[4]Department of Chemical Engineering, Waterloo University, ON N2L 3G1, Canada
*Corresponding author Email: ramiz.salama@neu.edu.tr

Abstract: Two emerging technologies that could alter how we use mobile devices and cloud services are distributed mobile cloud computing and blockchain technology. Several mobile devices are used by distributed mobile cloud computing services to create a virtual cloud computing architecture. By using this technique, users can leverage the processing power and storage of the devices to do computationally intensive tasks like machine learning and data analytics. By pooling resources across multiple devices, distributed mobile cloud computing services provide a scalable and cost-effective solution for individuals and businesses alike. Conversely, blockchain technology is a distributed ledger system that eliminates the need for middlemen and makes transactions safe, transparent, and verifiable. In general, distributed mobile cloud computing and blockchain technology open up new avenues for mobile computing services and clear the way for a safer, more efficient, and more cooperative mobile environment. Distributed mobile cloud computing (DMCC) and blockchain technology are two rapidly emerging technologies that are transforming the way we store, process, and manage data. The utilization of mobile devices' processing capacity for complex calculations is made possible by DMCC, which disperses computing resources across a network of devices. Blockchain technology, on the other hand, enables safe, decentralized, and unchangeable record-keeping that may be applied in a range of scenarios. Combining DMCC with Blockchain Technology has many benefits, such as increased privacy, security, and scalability. Smart contracts built on blockchain technology can facilitate trustless transactions and automate complex processes. Tokenization, which permits the creation of digital assets and direct value transfers across international borders, is another crucial element of blockchain technology. When implementing DMCC and blockchain solutions, a few of the problems that must be fixed are interoperability, consensus procedures, and digital identity. Nonetheless, there is a great deal of promise for blockchain technology and distributed mobile cloud computing services to completely transform industries like supply chain management, healthcare, and banking. We look at the key features, potential applications, challenges, and prospects related to DMCC and blockchain technology in this post.

Keywords: Consensus mechanisms, decentralization, blockchain technology, distributed mobile cloud computing, mobile cloud computing services

1. Introduction

Mobile computing refers to the use of mobile devices, such as smartphones, tablets, laptops, and wearable devices, to access and use information and applications while on the move. Mobile computing has become increasingly popular in recent years due to the widespread availability of high-speed internet connectivity and the development of powerful, lightweight mobile devices. Mobile computing enables users to stay connected to the internet and access a wide range of applications and services from virtually anywhere. This has revolutionized the way people work, communicate, and consume information. With mobile computing, users can send and receive emails, browse the web, use social media, stream videos, play games, and much more, all from the palm of their hand. The development of mobile computing has also led to the creation of a vast ecosystem of mobile applications, or "apps," that can be downloaded and installed on mobile devices. These apps enable users to perform a wide range of tasks, from ordering food and booking travel to monitoring their health and fitness. Overall, mobile computing has had a profound impact on the way people live and work, and it is likely to continue to play a key role in shaping the future of technology.Blockchain technology is a decentralized, distributed digital ledger that records transactions in a secure and transparent manner. It was originally created to support the cryptocurrency Bitcoin, but has since evolved to have numerous other applications.

The blockchain consists of a network of nodes or computers that work together to validate and record transactions. Each transaction is verified by multiple nodes, and once validated, it is recorded as a block on the blockchain. Each block contains a unique code or hash that links it to the previous block, forming an unbreakable chain of blocks. One of the key features of blockchain technology is its transparency and security. Once a transaction is recorded on the blockchain, it cannot be altered or deleted. This makes it very difficult for anyone to manipulate or corrupt the data. Another important feature of blockchain technology is its decentralization. There is no central authority or intermediary controlling the blockchain. Instead, it is maintained and verified by a network of nodes or computers, making it more resilient to attacks or failures. Blockchain technology has numerous applications, beyond just cryptocurrencies. It can be used for secure data storage and sharing, digital identity verification, smart contracts, supply chain management, and much more.

As a result, it has the potential to transform many industries and improve efficiency, transparency, and security in various processes. Decentralized mobile cloud computing architectures are designed to provide a distributed computing environment that leverages the resources of mobile devices to support cloud computing services. The main idea behind this architecture is to enable mobile devices to work collaboratively, forming a network of distributed resources that can support complex computing tasks. In this architecture, mobile devices act as both clients and servers, and are responsible for processing and storing data. The mobile devices are connected through a wireless network, and the architecture is designed to enable communication and coordination between devices. The architecture typically includes a set of distributed computing services that are provided by the mobile devices, such as data storage, processing, and communication.

These services are coordinated by a set of middleware components that manage the distribution of tasks and data among the mobile devices. Decentralized mobile cloud computing architectures have several benefits over traditional centralized architectures. One of the main advantages is improved scalability, as the architecture can easily adapt to changing resource

demands by dynamically adding or removing mobile devices from the network. Another benefit is improved reliability, as the distributed nature of the architecture provides redundancy and fault tolerance. Additionally, the use of mobile devices can reduce the cost of cloud computing services, as it leverages existing resources rather than requiring the use of expensive dedicated servers. However, there are also some challenges associated with decentralized mobile cloud computing architectures. These include the need for efficient task scheduling and load balancing mechanisms, as well as the need for effective security and privacy mechanisms to protect sensitive data and ensure the integrity of the computing environment.

2. Integration of blockchain technology into mobile cloud computing:

The integration of blockchain technology into mobile cloud computing services has the potential to enhance the security, privacy, and efficiency of these services. Blockchain technology provides a decentralized and tamperproof mechanism for storing and sharing data, which can be leveraged to enable secure and efficient data sharing among mobile devices. One way to integrate blockchain technology into mobile cloud computing services is to use a blockchain-based distributed file system, which can provide secure and efficient storage and sharing of data among mobile devices. The distributed file system can be built on top of a blockchain platform, such as Ethereum, which provides smart contract functionality and enables automated execution of contracts and transactions. Another way to integrate blockchain technology into mobile cloud computing services is to use blockchain-based authentication and access control mechanisms, which can provide enhanced security and privacy for users. For example, a mobile cloud computing service could use a blockchainbased identity management system to manage user identities and authentication, which can provide better security and privacy compared to traditional centralized authentication systems. In addition, blockchain technology can be used to provide secure and efficient payment processing mechanisms for mobile cloud computing services. For example, a mobile cloud computing service provider could use a blockchain-based payment system to enable secure and efficient payment processing for its customers, without the need for traditional payment processing intermediaries. Overall, the integration of blockchain technology into mobile cloud computing services has the potential to enable secure and efficient data sharing, authentication, access control, and payment processing mechanisms, which can enhance the overall functionality and security of mobile cloud computing services. Security and privacy of disturbed mobile computing systems: Security and privacy are important concerns in distributed mobile cloud computing services, as these services involve the sharing and processing of sensitive data across multiple devices and networks.

There are several security and privacy challenges that need to be addressed in distributed mobile cloud computing services:

1. *Data confidentiality:* Sensitive data should be encrypted when stored or transmitted across the network to prevent unauthorized access.
2. *Data integrity:* The data should not be altered or modified during transmission, processing, or storage, and should remain the same as when it was first created.
3. *Authentication:* The identity of the users and devices should be verified before granting access to the data or the system.
4. *Authorization:* Users and devices should be granted access only to the data and services that they are authorized to use.
5. *Availability:* The system should be available to authorized users at all times, and should be resilient to various types of attacks and failures.

6.

To address these challenges, several security and privacy mechanisms can be employed in distributed mobile cloud computing services, such as:

1. *Encryption:* Sensitive data should be encrypted when stored or transmitted across the network.
2. *Access control:* Access to the data and services should be restricted to authorized users and devices.
3. *Firewall and intrusion detection systems:* These can be used to detect and prevent unauthorized access and attacks on the system.
4. *Authentication and identity management:* Users and devices should be authenticated and their identities should be managed in a secure and reliable manner.
5. *Data backup and disaster recovery:* The data should be backed up regularly to prevent data loss, and disaster recovery mechanisms should be in place in case of system failures or attacks.

Overall, security and privacy are critical concerns in distributed mobile cloud computing services, and these challenges need to be addressed through a combination of technical, organizational, and procedural mechanisms to ensure the confidentiality, integrity, and availability of the data and services.

3. Smart contracts for mobile cloud computing:

Smart contracts are self-executing contracts with the terms of the agreement between buyer and seller being directly written into lines of code. Smart contracts have the potential to revolutionize mobile cloud computing by enabling the automation of complex processes and reducing the need for intermediaries. In the context of mobile cloud computing, smart contracts can be used to automate the negotiation, execution, and enforcement of agreements between mobile devices and cloud service providers. Smart contracts can enable the creation of a decentralized marketplace for mobile cloud computing services, where mobile devices can negotiate and contract with cloud service providers in a secure and transparent manner.

Smart contracts can be used to automate several aspects of mobile cloud computing, such as:

1. *Service provisioning:* Smart contracts can be used to automatically provision cloud services based on the requirements of the mobile device.
2. *Service level agreements (SLAs):* Smart contracts can be used to automatically negotiate and enforce SLAs between mobile devices and cloud service providers.
3. *Payment processing:* Smart contracts can be used to automate the payment processing for mobile cloud computing services, eliminating the need for traditional payment processing intermediaries.
4. *Service monitoring:* Smart contracts can be used to monitor the performance and availability of cloud services, and automatically trigger remediation actions in case of failures or performance degradation.

Overall, smart contracts have the potential to enable more efficient, secure, and transparent mobile cloud computing services by automating complex processes and reducing the need for intermediaries. However, there are also several challenges that need to be addressed in the use of smart contracts, such as the need for standardization, interoperability, and security mechanisms to ensure the reliability and integrity of the contracts.

Blockchain based mobile applications:
Blockchain-based mobile applications are mobile applications that leverage blockchain technology to provide various features and functionalities. These applications can offer increased security, transparency, and privacy compared to traditional mobile applications. Blockchain-based mobile applications can be used in various domains, such as finance, healthcare, logistics, and supply chain management.

Some examples of blockchain-based mobile applications are:
1. *Cryptocurrency wallets:* Cryptocurrency wallets are mobile applications that enable users to securely store and manage their cryptocurrencies. These applications leverage blockchain technology to provide secure and transparent transactions.
2. *Decentralized marketplaces:* Decentralized marketplaces are mobile applications that enable peer-topeer transactions without the need for intermediaries. These applications leverage blockchain technology to provide secure and transparent transactions.
3. *Identity management systems:* Identity management systems are mobile applications that enable users to manage their digital identities in a secure and decentralized manner. These applications leverage blockchain technology to provide tamper-proof and secure identity management.
4. *Supply chain management systems:* Supply chain management systems are mobile applications that enable stakeholders to track and manage the flow of goods and services in a supply chain. These applications leverage blockchain technology to provide transparent and secure tracking of the supply chain.
5. *Voting systems:* Voting systems are mobile applications that enable stakeholders to vote in a transparent and secure manner. These applications leverage blockchain technology to ensure the integrity of the voting process.

Overall, blockchain-based mobile applications have the potential to provide increased security, transparency, and privacy compared to traditional mobile applications, and can be used in various domains to provide new and innovative functionalities. However, there are also several challenges that need to be addressed in the development and deployment of blockchain-based mobile applications, such as scalability, interoperability, and security concerns.

Performance evaluation:
Performance evaluation is a critical aspect of distributed mobile cloud computing systems as it enables the identification of bottlenecks and performance issues that affect the overall performance of the system. Performance evaluation can also help in identifying the optimal system configuration and settings for achieving maximum performance and efficiency.

There are several metrics that can be used to evaluate the performance of distributed mobile cloud computing systems, including:
1. *Response time:* Response time measures the time taken for a request to be processed and responded to by the system. Lower response times indicate faster system performance and higher user satisfaction.
2. *Throughput:* Throughput measures the amount of work that the system can handle in a given time period. Higher throughput indicates higher system performance and efficiency.
3. *Resource utilization:* Resource utilization measures the extent to which system resources, such as CPU, memory, and network bandwidth, are being utilized. Higher resource utilization can indicate a potential bottleneck in the system.

4. *Scalability:* Scalability measures the ability of the system to handle increasing workloads and users. A highly scalable system can handle more workloads and users without any significant degradation in performance.
5. *Availability:* Availability measures the ability of the system to remain operational and accessible to users. Higher availability indicates a more reliable and stable system.

To evaluate the performance of distributed mobile cloud computing systems, various testing methodologies can be used, such as load testing, stress testing, and performance profiling. Load testing involves simulating multiple users accessing the system simultaneously to measure its

response time and throughput. Stress testing involves pushing the system to its limits to identify performance bottlenecks and failure points. Performance profiling involves analyzing the system's resource utilization and performance metrics to identify areas for optimization. Overall, performance evaluation is essential for identifying and addressing performance issues in distributed mobile cloud computing systems, ensuring maximum performance and efficiency for the system. Blockchainbased identity management for mobile devices: Blockchain-based identity management for mobile devices refers to the use of blockchain technology to secure and manage the digital identities of mobile users. Traditional identity management systems are often centralized and vulnerable to hacking, identity theft, and other security risks. Blockchain-based identity management systems, on the other hand, provide a decentralized and secure solution for managing digital identities. In a blockchain-based identity management system for mobile devices, user identities are stored on a blockchain network, which is a distributed ledger that enables secure and transparent transactions. The blockchain network maintains a tamper-proof record of all user identities, ensuring that they cannot be altered or deleted without proper authorization. Users can access their identities through a mobile application that interfaces with the blockchain network.

Blockchain-based identity management for mobile devices provides several benefits, including:
1. *Increased security:* Blockchain-based identity management systems provide a highly secure solution for managing digital identities. The decentralized and tamper-proof nature of blockchain ensures that user identities are protected from hacking, identity theft, and other security risks.
2. *Improved privacy:* Blockchain-based identity management systems provide users with greater control over their personal data. Users can choose which information to share and with whom, and can also revoke access to their data at any time.
3. *Enhanced convenience:* Blockchain-based identity management systems provide a convenient solution for managing digital identities. Users can access their identities from anywhere, using their mobile devices, and can also use their identities to access a range of services and applications.
4. *Increased trust:* Blockchain-based identity management systems provide a transparent and verifiable solution for managing digital identities. The tamper-proof nature of blockchain ensures that all transactions are secure and trustworthy, providing users with increased trust in the system.

Overall, blockchain-based identity management for mobile devices provides a secure, decentralized, and convenient solution for managing digital identities, offering a range of benefits over traditional identity management systems. However, there are also challenges that need to be addressed in the development and deployment of blockchain-based identity management systems, such as scalability, interoperability, and usability concerns.

4. Blockchain-based supply chain management:

Blockchain-based supply chain management refers to the use of blockchain technology to secure and manage the supply chain processes of a business. In traditional supply chain management, there are often numerous intermediaries involved, which can lead to delays, errors, and increased costs. By using blockchain technology, businesses can create a transparent and secure supply chain ecosystem that eliminates intermediaries and streamlines processes.

In a blockchain-based supply chain management system, all stakeholders in the supply chain, such as suppliers, manufacturers, distributors, and retailers, have access to a shared ledger that records all transactions and information related to the supply chain process. Each transaction is cryptographically secured, and once entered into the ledger, it cannot be altered or deleted without consensus from all participants.

Blockchain-based supply chain management offers several benefits, including:

1. *Increased transparency:* The use of a shared ledger provides a transparent view of the entire supply chain process. All stakeholders can view the transaction history and track the movement of goods throughout the supply chain.
2. *Enhanced traceability:* Blockchain-based supply chain management enables enhanced traceability, as all transactions are recorded on the blockchain ledger. This provides a secure and reliable way to track products and ensure their authenticity.
3. *Improved efficiency:* By eliminating intermediaries, blockchain-based supply chain management can significantly reduce the time and costs associated with traditional supply chain management processes.
4. *Increased security:* Blockchain-based supply chain management provides a highly secure solution for managing supply chain processes. The decentralized and tamper-proof nature of blockchain ensures that transactions are secure and trustworthy.

Overall, blockchain-based supply chain management offers a transparent, secure, and efficient solution for managing supply chain processes. However, there are also challenges that need to be addressed in the development and deployment of blockchain-based supply chain management systems, such as interoperability, scalability, and standardization concerns.

Cloud Computing Services and Blockchain Technology

Distributed Mobile Cloud Computing Services and Blockchain Technology can vary depending on the specific study. However, here are some common materials and methods used in this area of research [20] – [24]:

1. *Distributed mobile cloud computing infrastructure:* To study distributed mobile cloud computing services, researchers typically use a distributed mobile cloud computing infrastructure that comprises mobile devices, cloud servers, and communication networks. This infrastructure is used to simulate various scenarios and evaluate the performance of different algorithms and protocols.
2. *Blockchain network:* Researchers studying the integration of blockchain technology into mobile cloud computing services typically use a blockchain network to store and manage data securely. The blockchain network can be a public or private network, and different consensus mechanisms can be used to ensure the integrity of the network.

3. *Smart contracts:* To study the use of smart contracts in mobile cloud computing, researchers typically use a smart contract platform, such as Ethereum. Smart contracts are used to automate certain processes and enforce rules and regulations.
4. *Data collection:* Researchers collect data on various parameters such as latency, bandwidth, processing time, and energy consumption to evaluate the performance of different algorithms and protocols. Data can be collected using simulation tools or real-world experiments.
5. *Evaluation metrics:* To evaluate the performance of different algorithms and protocols, researchers use various metrics, such as response time, throughput, energy consumption, and scalability.
6. *Data analysis:* Researchers analyze the collected data using various statistical and machine learning techniques to draw conclusions and make recommendations.

Overall, the materials and methods used in research related to Distributed Mobile Cloud Computing Services and Blockchain Technology are diverse and can involve a combination of simulation, experimentation, and data analysis techniques. The goal is to evaluate the performance and effectiveness of different algorithms and protocols for improving the security, privacy, and efficiency of mobile cloud computing services using blockchain technology.

5. Results and discussions:

The results and discussions of research related to Distributed Mobile Cloud Computing Services and Blockchain Technology can vary depending on the specific study. However, here are some common results and discussions found in this area of research [25] – [32]:

1. *Integration of blockchain technology into mobile cloud computing services:* Several studies have explored the integration of blockchain technology into mobile cloud computing services to improve the security and privacy of mobile devices. The results have shown that blockchain-based mobile cloud computing systems can offer higher security and privacy levels than traditional cloud computing systems.
2. *Decentralized mobile cloud computing architectures:* Studies have explored the use of decentralized mobile cloud
computing architectures to improve the efficiency and scalability of mobile cloud computing services. The results have shown that decentralized architectures can improve the performance and scalability of mobile cloud computing services.
3. *Smart contracts for mobile cloud computing:* Research has explored the use of smart contracts in mobile cloud computing to automate certain processes and enforce rules and regulations. The results have shown that smart contracts can improve the efficiency and transparency of mobile cloud computing services.
4. *Performance evaluation of distributed mobile cloud computing systems:* Studies have evaluated the performance of distributed mobile cloud computing systems using various metrics, such as response time, throughput, energy consumption, and scalability. The results have shown that different algorithms and protocols can significantly impact the performance of distributed mobile cloud computing systems.
5. *Blockchain-based supply chain management:* Several studies have explored the use of blockchain technology for supply chain management.

The results have shown that blockchainbased supply chain management can improve the transparency, traceability, and security of supply chain processes.

Overall, the results and discussions of research related to Distributed Mobile Cloud Computing Services and Blockchain Technology highlight the potential benefits and challenges of using blockchain technology for improving the security, privacy, efficiency, and transparency of mobile cloud computing services and supply chain management. Further research is needed to address the challenges and fully realize the potential of blockchain technology in these areas.

6.Conclusion:

Blockchain technology and distributed mobile cloud computing services are two quickly developing fields that have the potential to completely change how we manage supply chains and use mobile devices. While blockchainbased supply chain management can improve the transparency, traceability, and security of supply chain processes, mobile cloud computing services that integrate blockchain technology can greatly improve the security, privacy, efficiency, and transparency of mobile devices. While smart contracts can automate procedures and enforce laws and regulations, decentralized mobile cloud computing architectures can offer a scalable and effective foundation for mobile cloud computing services. Studies on performance evaluation have demonstrated that the performance of distributed mobile cloud computing systems can be considerably impacted by various algorithms and protocols. Notwithstanding the possible advantages, there are certain issues that must be resolved. New security and privacy vulnerabilities may arise from the integration of blockchain technology with mobile cloud computing services, and new performance and scalability problems may arise from the usage of distributed architectures and smart contracts. Furthermore, there needs to be a lot of cooperation and standardization between many companies and stakeholders in order to adopt blockchain-based supply chain management. In summary, blockchain technology and distributed mobile cloud computing services are emerging fields that have the potential to greatly enhance supply chain management and mobile device security, privacy, efficiency, and transparency. To overcome the obstacles and reach the full potential of these technologies, more research is necessary. In order to facilitate the widespread adoption of these technologies across a range of applications and sectors, researchers, practitioners, and regulators must collaborate to build resilient and secure protocols, standards, and architectures.

References

[1]. Yu, L., He, M., Liang, H., Xiong, L., & Liu, Y. (2023). A Blockchain-Based Authentication and Authorization Scheme for Distributed Mobile Cloud Computing Services. Sensors, 23(3), 1264.

[2]. Salama, R., Alturjman, S., Altrjman, C., & Al-Turjman, F. (2023). Cloud Computing Services for Distributed Mobile Users and Blockchain Technology. NEU Journal for Artificial Intelligence and Internet of Things, 2(4).

[3]. Vivekanandan, M., VN, S., & U, S. R. (2021). Blockchain based privacy preserving user authentication protocol for distributed mobile cloud environment. Peer-to-Peer Networking and Applications, 14, 15721595.

[4]. Kim, H. W., & Jeong, Y. S. (2018). Secure authentication-management human-centric scheme for trusting personal resource information on mobile cloud computing with blockchain. Human-centric Computing and Information Sciences, 8(1), 1-13.

[5]. Zhang, Y., Xiong, L., Li, F., Niu, X., & Wu, H. (2023). A blockchain-based privacy-preserving auditable authentication scheme with hierarchical access control for mobile cloud computing. Journal of Systems Architecture, 142, 102949.

[6]. Amin, R., Islam, S. H., Biswas, G. P., Giri, D., Khan, M. K., & Kumar, N. (2016). A more secure and privacyaware anonymous user authentication scheme for distributed mobile cloud computing environments. Security and Communication Networks, 9(17), 4650-4666.

[7]. Nguyen, D. C., Pathirana, P. N., Ding, M., & Seneviratne, A. (2019). Blockchain for secure ehrs sharing of mobile cloud based e-health systems. IEEE access, 7, 66792-66806.

[8]. Tsai, J. L., & Lo, N. W. (2015). A privacy-aware authentication scheme for distributed mobile cloud computing services. IEEE systems journal, 9(3), 805-815.

[9]. Chaudhry, S. A., Kim, I. L., Rho, S., Farash, M. S., & Shon, T. (2019). An improved anonymous authentication scheme for distributed mobile cloud computing services. Cluster Computing, 22, 1595-1609.

[10]. Irshad, A., Sher, M., Ahmad, H. F., Alzahrani, B. A., Chaudhry, S. A., & Kumar, R. (2016). An improved multi-server authentication scheme for distributed mobile cloud computing services. KSII Transactions on Internet and Information Systems (TIIS), 10(12), 5529-5552.

[11]. Zheng, R., Jiang, J., Hao, X., Ren, W., Xiong, F., & Ren, Y. (2019). bcBIM: A blockchain-based big data model for BIM modification audit and provenance in mobile cloud. Mathematical Problems in Engineering, 2019.

[12]. Dinh, H. T., Lee, C., Niyato, D., & Wang, P. (2013). A survey of mobile cloud computing: architecture, applications, and approaches. Wireless communications and mobile computing, 13(18), 1587-1611.

[13]. Lo'ai, A. T., & Saldamli, G. (2021). Reconsidering big data security and privacy in cloud and mobile cloud systems. Journal of King Saud University-Computer and Information Sciences, 33(7), 810-819.

[14]. Arumugam, M., Deepa, S., Arun, G., Sathishkumar, P., & Jeevanantham, K. (2021, February). Secure data sharing for mobile cloud computing using RSA. In IOP Conference Series: Materials Science and Engineering (Vol. 1055, No. 1, p. 012108). IOP Publishing.

[15]. Ding, Y., & Sato, H. (2020, August). Bloccess: towards fine-grained access control using blockchain in a distributed untrustworthy environment. In 2020 8th IEEE International Conference on Mobile Cloud Computing, Services, and Engineering (MobileCloud) (pp. 17-22). IEEE.

[16]. Sheth, H. S. K., & Tyagi, A. K. (2021, December). Mobile cloud computing: issues, applications and scope in COVID-19. In International conference on intelligent systems design and applications (pp. 587-600). Cham: Springer International Publishing.

[17]. Prof.DUX available online: https://dux.aiiot.website/

[18]. Al-Turjman, F. (2023). Enhancing Higher Education Through Prof. DUX: A Practical Approach to Personalized AI Assisted Learning. NEU Journal for Artificial Intelligence and Internet of Things, 1(2).

[19]. Al-Turjman, F. (2023). Familiarizing Teachers/Learners with AI-assisted Learning and Evaluation Implementations–Prof. DUX a Use Case. NEU Journal for Artificial Intelligence and Internet of Things, 2(4).

[20]. Sharma, P., Kumar, R., & Gupta, M. (2021, October). Impacts of Customer Feedback for Online-Offline Shopping using Machine Learning. In *2021 2nd International Conference on Smart Electronics and Communication (ICOSEC)* (pp. 1696-1703). IEEE.

[21]. Gupta, M., Kumar, R., & Dewari, S. (2021). Digital twin techniques in recognition of human action using the fusion of convolutional neural network. In *Digital Twin Technology* (pp. 165-186). CRC Press.

[22]. Kour, S., Kumar, R., & Gupta, M. (2021, September). Analysis of student performance using Machine learning Algorithms. In *2021 Third International Conference on Inventive Research in Computing Applications (ICIRCA)* (pp. 1395-1403). IEEE.

[23]. Gupta, M., Kumar, R., Chaudhary, R. K., & Kumari, J. (2021, December). IoT Based Voice Controlled Autonomous Robotic Vehicle Through Google Assistant. In *2021 3rd International Conference on Advances in Computing, Communication Control and Networking (ICAC3N)* (pp. 713-717). IEEE.

[24]. Gupta, M., Kumar, R., Walia, H., & Kaur, G. (2021, October). Airlines based twitter sentiment analysis using deep learning. In *2021 5th International Conference on Information Systems and Computer Networks (ISCON)* (pp. 1-6). IEEE.

[25]. Kumar, R., Gupta, M., Shukla, S., & Yadav, R. K. (2021, September). E-challan automation for RTO using OCR. In *2021 third international conference on inventive research in computing applications (ICIRCA)* (pp. 1-8).

[26]. Bawa, H., Singh, P., & Kumar, R. (2012). An Efficient Novel Key management scheme using NchooseK algorithm for Wireless Sensor Networks. *International Journal of Computer Networks & Communications (IJCNC) Vol*, *4.*

[27]. Gupta, M., Wu, H., Arora, S., Gupta, A., Chaudhary, G., & Hua, Q. (2021). Gene mutation classification through text evidence facilitating cancer tumour detection. *Journal of Healthcare Engineering*, *2021*, 1-16.

[28]. Gupta, M., Solanki, V. K., Singh, V. K., & García-Díaz, V. (2018). Data mining approach of accident occurrences identification with effective methodology and implementation. *International Journal of Electrical and Computer Engineering*, *8*(5), 4033.

[29]. Gupta, M., Solanki, V. K., & Singh, V. K. (2017). A novel framework to use association rule mining for classification of traffic accident severity. *Ingeniería solidaria*, *13*(21), 37-44.

[30]. Puneet, Kumar, R., & Gupta, M. (2022). Optical coherence tomography image based eye disease detection using deep convolutional neural network. *Health Information Science and Systems*, *10*(1), 13.

[31]. Kumari, M., Gupta, M., & Ved, C. (2021). Blockchain in Pharmaceutical sector. *Applications of blockchain in healthcare*, 199-220.

[32]. Gupta, M., Kumar, R., Larhgotra, A., & Ved, C. (2023). 5 Emergence of Big. *Convergence of IoT, Blockchain, and Computational Intelligence in Smart Cities*, 83.