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 tamper-proof 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-to-peer 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. Blockchain-based 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 blockchain-based 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, 1572-1595.
[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 privacy-aware 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.