# Managing Cybersecurity in Smart Cities With Blockchain Technology

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

[1]Department of Computer Engineering, AI and Robotics Institute, Research Center for AI and IoT, Near East University Nicosia, Mersin10, Turkey
[2]Artificial Intelligence Engineering Dept., 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

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

**Abstract:** Smart cities, which use cutting-edge technologies like the Internet of Things (IoT), big data analytics, and artificial intelligence (AI) to enhance the efficiency, sustainability, and livability of cities, are quickly developing as a new paradigm for urban development. But as cities become increasingly networked and data-driven, they also become more susceptible to cyberattacks, which can jeopardize residents' security, privacy, and safety as well as threaten vital infrastructure systems like power grids, transportation networks, and emergency services. We investigate how blockchain technology might be used to oversee cybersecurity in smart cities. Blockchain technology, a type of distributed ledger, offers a decentralized, impenetrable record for handling and protecting data. Blockchain technology can aid in ensuring the integrity and privacy of sensitive information such as personal data, financial transactions, and crucial infrastructure systems by applying cryptographic algorithms and consensus procedures. Three categories can be used to categorize blockchain systems:

- General: a public or unrestricted a decentralized open-source technology called blockchain makes it possible for anybody to use it and engage in mining.
- Private: A private or permissioned blockchain is a decentralized network that permits the sharing of private data within an organization or among a specific set of people.
- Consortium: A consortium blockchain is a combination of a private and public blockchain in which a group of organizations manages both the consensus and block validation processes as well as who has access to the blockchain.

**Keywords:** Distributed ledger technology, smart cities, Cyber Security, Blockchain Technology

## 1. Introduction

Smart cities are urban environments that use advanced technologies to improve the quality of life for citizens, enhance sustainability, and streamline operations.

The world's population is becoming increasingly urbanized, with more people living in cities than ever before. As cities grow, the demand for infrastructure such as transportation, water, and waste management systems also increases. Smart cities play an important role in meeting the needs of those citizens.
Here are some of the key characteristics that define a smart city:

- Advanced infrastructure: Smart cities use advanced infrastructure systems such as sensors, cameras, and communication networks to collect and analyze data about various aspects of the city, such as traffic patterns, air quality, energy consumption, and water usage. This data is then used to inform decision-making and optimize the use of resources. Connected systems: Smart cities use interconnected systems to share data and communicate with each other. This allows different systems, such as transportation, energy, and public safety, to work together in a coordinated manner.
- Citizen engagement: Smart cities prioritize citizen engagement and participation, using technology to enable citizens to provide feedback, report issues, and collaborate with government agencies and other stakeholders.
- Sustainability: Smart cities focus on sustainability, using technologies such as renewable energy, green buildings, and smart grid systems to reduce environmental impact and improve resource efficiency.
- Mobility: Smart cities focus on mobility, using technologies such as connected vehicles, intelligent transportation systems, and bike-sharing programs to improve transportation options and reduce congestion.
- Quality of life: Smart cities prioritize the well-being of their citizens, using technologies such as public health monitoring, community services, and cultural events to enhance the quality of life.
- Innovation: Smart cities are innovative, using emerging technologies such as artificial intelligence, blockchain, and augmented reality to improve services and drive economic growth.

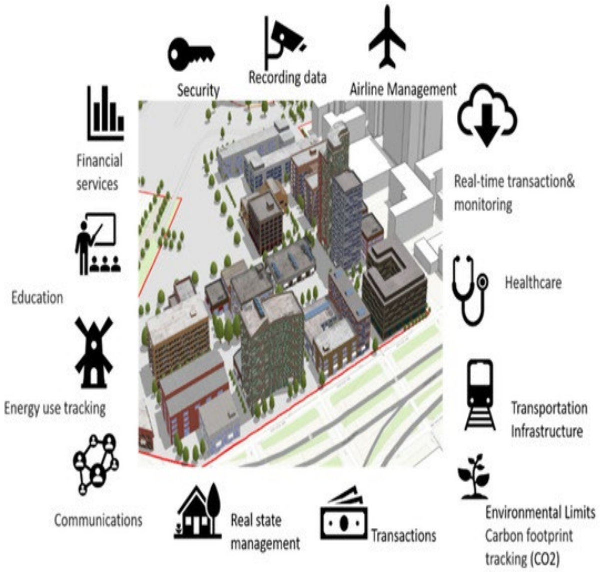

***Figure 1***. *Blockchain in the Infrastructure of smart cities*

Blockchain technology is a promising solution for security in smart cities due to its unique characteristics that make it suitable for managing sensitive data and ensuring secure transactions.

A blockchain is a database that is distributed across a network of computers, rather than being stored in a central location. Each computer in the network, or "node," has a copy of the database, which is constantly updated and synchronized with the other nodes.
This means that there is no single point of failure or control, and the data is more resilient to hacking, data loss, or other types of attacks.

One of the key features of a blockchain is that it uses cryptographic algorithms to secure the data and prevent tampering or unauthorized access. Each block in the blockchain contains a unique digital signature, or hash, that is created by combining the data in the block with a secret key or "nonce." This hash is then added to the previous block in the chain, creating a chain of blocks that is difficult to modify or forge.

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 [3]. 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. Previously published work

“Blockchain for the Cybersecurity of Smart City Applications” reviews how different smart city applications use blockchain technology. The different applications are smart healthcare, smart transportation, and smart agriculture.

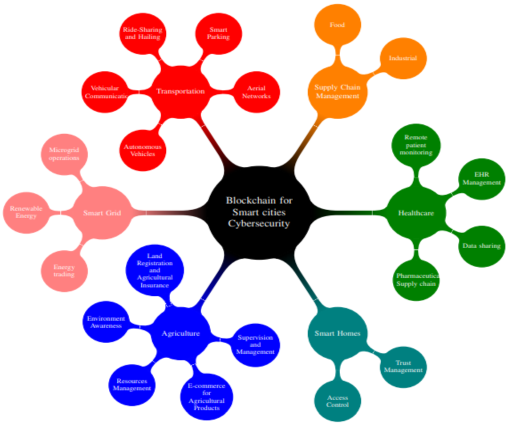

***Figure 2.*** *Smart Cities Applications studied*

### 2.1 Using blockchain for smart healthcare has various benefits, such as:

- Decentralization: Since healthcare applications are frequently shared among numerous stakeholders, a distributed management system is necessary. Blockchain can offer this form of decentralized administration, allowing all participants and stakeholders to independently manage who has access to patient data without the need for a central authority.
- Improved data security and privacy: Due to the immutability of blockchain technology, it helps safeguard patient data from tampering or manipulation. Additionally, the use of cryptographic keys hides the true identity of patients, enhancing patient privacy.

- Health data ownership: Blockchain can implement user-centric healthcare systems where the patient can manage access to his health data through smart contracts. The user may choose which medical professionals to grant access to and the duration of that access thanks to smart contracts that are clearly stated.
- Availability and robustness: The data is duplicated across numerous nodes and stored on the blockchain in a manner that is distributed. This makes it possible to ensure data availability and improves system resiliency.
- Transparency and trust: The open and transparent character of the blockchain increases confidence among its various actors and stakeholders.
- Intelligent Transportation System (ITS) applications in smart cities require connecting vehicles securely and dependably to protect what or who is transported.
- Due to the constantly developing security concerns, cars may be targeted by a variety of malicious attacks that endanger the security of users, services, and data.

### 2.2 Blockchain plays a vital role in ITS applications, with numerous benefits such as:

- Security and Safety: Securing the data, execution, and communications of the applications as well as the safety of the application users (drivers and passengers) is one of the most crucial elements in the success of ITS applications. The blockchain can defend the ITS applications from harmful attacks and ensure participant safety thanks to its decentralized validation and immutable data.
- Drivers' and passengers' privacy: The most crucial factor in handling private data is trust. To keep sensitive information out of the hands of hackers, an effective trust-based distributed blockchain method that makes use of cryptography and hashing operations should be implemented.
- Decentralized mechanism removes the single point of failure (SPoF) problem: The SPoF issue affects most centralized management and storage systems. Because each node in a blockchain retains a copy of the ledger and works together to make blockchain-related decisions, the SPoF problem is resolved.
- Automatization: A self-organized, self-adaptive, and decentralized autonomous ITS ecosystem can be created by using the blockchain for the lifetime management and monitoring of ITS equipment.
- Providing strong trust for ITS users: ITS users trust the blockchain data used by the ITS applications because the blockchain is transparent and all network exchanges are expressly stated as immutable transactions within the blockchain blocks.
- Scalability: ITS networks have the potential to expand to have many nodes. According to some research papers, partitioning, sharding, and directed acyclic graphs (DAGs) are effective methods for scaling the blockchain. The blockchain-based ITS application may be improved to an extensive degree and meet the needs of the transportation network by implementing similar solutions.

## 3. Managing Cyber Security in Smart Cities with Blockchain Technology

To add a new block to the blockchain, a process called "mining" is used. Mining involves solving a complex mathematical puzzle that requires a significant amount of computational power. The first node to solve the puzzle earns a reward in the form of cryptocurrency, and the new block is added to the blockchain. This process helps ensure that the blockchain is secure and decentralized, as it requires a large network of nodes to verify and validate the transactions.

### *3.1 Blockchain-Based Framework in Smart Cities*

The typical blockchain-based framework in smart cities consists of four layers:

**User authentication layer**: It is designed to make sure that only authorized users can access the specified application by ensuring authentication. Authenticated access is provided by straightforward procedures like biometric verification or retina scanning with an OTP or user password.

**Data management layer**: This layer's main function is to coordinate user actions between the blockchain layer and the application layer. To create the transaction block, it performs all the processes, including data parsing, data encryption, data packaging, etc. Consensus rules, which are a set of accepted requirements, control the data changes.

**Application layer**: The entire architecture is supported by this layer. It organizes the many operations into categories based on the services it provides and is also in charge of implementing a technology to connect each layer.

**Blockchain-based record cum storage layer**: It is a crucial layer in terms of security. It enables the application service to read and write encrypted data transactions which are secure and completely compliant with cybersecurity standards.

### *3.2 Implementation of Blockchain Technologies*

The implementation of blockchain technologies in smart city cybersecurity typically involves several steps. Here are some of the common ones:

**Blockchain platform**: The first step in implementing blockchain technology for smart city cybersecurity is to select a blockchain platform that meets the specific requirements of the use case. There are several blockchain platforms available, including Ethereum, Hyperledger Fabric, and Corda, each with its strengths and weaknesses.

**Smart contracts**: They are self-executing contracts that are implemented on a blockchain. They are digital programs that automatically execute the terms of a contract when certain conditions are met.

Once a blockchain platform has been selected, smart contracts are typically used to define the rules and logic for transactions on the blockchain. They are used to automate processes such as identity verification, data sharing, and secure communication.

**Cryptography**: Cryptography is a key component of blockchain technology and is used to secure data on the blockchain. Techniques such as public-key cryptography, hash functions, and digital signatures are used in the implementation.

**Consensus algorithms**: Consensus algorithms are used to ensure that transactions on the blockchain are verified and recorded in a secure and tamper-proof manner. Examples of consensus algorithms used in blockchain implementations include Proof of Work (PoW), Proof of Authority (PoA), Delegated Proof of Stake (DPoS), and Byzantine Fault Tolerance (BFT).

In a PoA consensus algorithm, nodes are selected based on their reputation, and transactions are validated by a group of pre-approved nodes. It provides high throughput and fast transaction times. Practical Byzantine Fault Tolerance (PBFT) works by having nodes reach a consensus on the state of the blockchain by exchanging messages and verifying each other's transactions. PBFT provides high throughput and low latency.

Delegated Proof of Stake (DPoS) algorithm is used in some blockchain-based smart city systems, where token holders can vote for block producers to validate transactions. The elected block producers then validate transactions and add them to the blockchain. DPoS provides fast transaction times and low fees.

Proof of Work (PoW) algorithm is not commonly used in smart city applications due to its high energy consumption and slow transaction times. However, it can be used in some systems that require high security and decentralization.

**Integration with other cybersecurity technologies**: In addition to the materials and methods specific to blockchain technology, the implementation of blockchain for smart city cybersecurity often involves integration with other cybersecurity technologies. For example, blockchain can be integrated with machine learning algorithms to detect and prevent cyber-attacks in real time.

**Testing and evaluation**: Finally, any implementation of blockchain technology for smart city cybersecurity should be thoroughly tested and evaluated to ensure that it meets the specific requirements of the use case and is effective in improving cybersecurity. This may involve conducting penetration testing, vulnerability assessments, and other forms of testing to identify and address any weaknesses in the implementation.

### *3.3 Cyber-attacks in Blockchain Technology*

While blockchain technology can enhance the security of smart cities, it is not immune to cyber-attacks.

51% Attack: In a blockchain network, the consensus algorithm requires a majority of the nodes to agree on the validity of transactions. If a single entity gains control of more than 50% of the computing power on the network, it can effectively control the blockchain, allowing them to manipulate the transactions. This can result in double-spending attacks, where an attacker can spend the same cryptocurrency twice, or the deletion of transactions from the blockchain.

Sybil Attack: In a Sybil attack, an attacker creates multiple fake identities or nodes on the blockchain network, allowing them to control the network. This can enable an attacker to gain access to sensitive data, control smart city systems, or execute fraudulent transactions.

Eclipse Attack: In an eclipse attack, an attacker isolates a node on the blockchain network, preventing it from communicating with other nodes, and allowing the attacker to control the node. This can enable an attacker to manipulate the transactions or control the smart city systems connected to the isolated node.

Smart Contract Vulnerabilities: Smart contracts are self-executing contracts that run on the blockchain network. However, they can have vulnerabilities that can be exploited by attackers to execute malicious code or steal funds. For example, a smart contract might contain a buffer overflow vulnerability that an attacker can exploit to execute arbitrary code.

Distributed Denial of Service (DDoS) Attack: In a DDoS attack, an attacker overwhelms the blockchain network with a large number of requests, causing the network to slow down or crash. This can result in a disruption of smart city services, which can be particularly damaging in critical infrastructure systems.

Malware Attacks: Malware can be used to gain unauthorized access to the devices and systems connected to the blockchain network, allowing attackers to steal sensitive information or take control of the systems. For example, an attacker might use malware to gain access to a smart city traffic control system and manipulate traffic signals, causing traffic jams or accidents.

To address these risks, smart cities can implement various security measures, such as [15] - [30]:

- Implementing strong access controls to restrict access to sensitive data and systems
- Regularly conducting security audits to identify vulnerabilities and patch them
- Using advanced encryption techniques to protect data on the blockchain network
- Implementing multi-factor authentication to ensure that only authorized users can access the network
- Ensuring that smart contracts are carefully audited and tested before they are deployed on the network
- Having a comprehensive incident response plan in place to detect and respond to any security breaches or cyber-attacks.

## 4. Results and discussion

Blockchain technology can be exploited to help with smart city security in several ways [31]-[42].

**Secure data sharing**: Smart cities generate vast amounts of data from various sources such as sensors, cameras, and other devices. This data contains sensitive information about citizens, businesses, and critical infrastructure systems.

By using blockchain technology, smart cities can securely share this data among different stakeholders, such as government agencies, private companies, and citizens, while ensuring that the data is not tampered with or misused. It also provides a transparent record of who has accessed the data, which can help prevent data breaches and other security incidents.

**Access control and identity management**: Blockchain technology can be used to authenticate users and devices, and control their access to different systems and services in smart cities.

A practical example is using blockchain-based smart contracts to enforce access control policies for critical infrastructure systems such as power grids, transportation networks, and emergency services.

By using blockchain technology to manage access control and identity management, smart cities can prevent unauthorized access and minimize the risk of cyber-attacks.

**Threat detection and response**: the technology is used to detect and respond to cyber threats in real-time, by providing a decentralized platform for sharing threat intelligence and coordinating responses among different stakeholders.
Blockchain-based vulnerability management systems enable smart cities to track and monitor the status of their systems, identify potential weaknesses, and prioritize remediation efforts.
By using blockchain technology for vulnerability management, smart cities can reduce the risk of cyber-attacks and improve the overall security of their systems.

In the early stages of research on blockchain technology in smart city cybersecurity, the focus was primarily on using blockchain to secure data sharing among different stakeholders in a smart city ecosystem. Secure sharing of data from IoT devices, traffic sensors, and other smart city infrastructure.

As the use of blockchain in smart city cybersecurity matured, researchers began exploring the potential for blockchain-based identity management solutions. They use blockchain's ability to securely store and manage identity data and can be used to authenticate users and devices in a smart city ecosystem.

More recently, there has been an increased focus on using blockchain to secure communication channels in smart city ecosystems. As blockchain technology matures, it is increasingly being integrated with other cybersecurity technologies to create more security solutions for smart cities. Additionally, blockchain is used in conjunction with machine learning and artificial intelligence to detect and prevent cyber-attacks in real-time.

## 5. Conclusion

Blockchain technology enables safe online transactions and verifications, and it can be used to support smart cities. Using blockchain technology has advantages in terms of increased connectivity and transparency, quick communication, integrity, and efficiency.

It makes use of a transversal system that allows for real-time data sharing. With blockchain technology, there are no middlemen, allowing for more effective and rapid digital communication between government agencies and the general population.

Additionally, the network of smart cities is being redesigned to build sustainable ecosystems through the integration of blockchain and AI technology. As we endeavor to create smart cities, technological advancements have presented both opportunities and difficulties for us. [1] 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.

## References

[1] 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.

[2] 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.

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

[4] 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).

[5] 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).

[6] 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).

[7] 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).

[8] 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).

[9] 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.

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

[11] Al-Turjman, F., & Salama, R. (2021). Security in social networks. In Security in IoT Social Networks (pp. 1-27). Academic Press.

[12] 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.

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

[14] 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.

[15] Bawa, Harjot, Parminder Singh, and Rakesh Kumar. "An efficient novel key management scheme for enhancing user authentication in a WSN." *International Journal of Computer Network and Information Security* 5.1 (2013): 56.

[16] Bansal, S., Gupta, M., & Tyagi, A. K. (2020). Building a Character Recognition System for Vehicle Applications. In *Advances in Decision Sciences, Image Processing, Security and Computer Vision: International Conference on Emerging Trends in Engineering (ICETE), Vol. 1* (pp. 161-168). Springer International Publishing.

[17] Gupta, M., Kumar, R., Chawla, S., Mishra, S., & Dhiman, S. (2021). Clustering based contact tracing analysis and prediction of SARS-CoV-2 infections. *EAI Endorsed Transactions on Scalable Information Systems*, *9*(35).

[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] Kumar, P., Kumar, R., & Gupta, M. (2021). Deep learning based analysis of ophthalmology: A systematic review. *EAI Endorsed Transactions on Pervasive Health and Technology*, *7*(29).

[20] Jain, R., Gupta, M., Jain, K., & Kang, S. (2021). Deep learning based prediction of COVID-19 virus using chest X-Ray. *Journal of Interdisciplinary Mathematics*, *24*(1), 155-173.

[21] Kaur, R., Kumar, R., & Gupta, M. (2023). Deep neural network for food image classification and nutrient identification: A systematic review. *Reviews in Endocrine and Metabolic Disorders*, 1-21.

[22] Gupta, D., Kaur, H., & Kumar, R. (2016). Detection of sink hole attack in wireless sensor network using advanced secure AODV routing protocol. *International Journal of Computer Applications*, *156*(11).

[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. 165-186). CRC Press.

[24] Kumar, R., Gupta, M., Agarwal, A., Mukherjee, A., & Islam, S. M. (2023). Epidemic efficacy of Covid-19 vaccination against Omicron: An innovative approach using enhanced residual recurrent neural network. *Plos one*, *18*(3), e0280026.

[25] Gupta, M., & Singla, N. (2019). Evolution of cloud in big data with hadoop on docker platform. In *Web services: Concepts, methodologies, tools, and applications* (pp. 1601-1622). IGI Global.

[26] 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.

[27] 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.

[28] Gupta, M., Upadhyay, V., Kumar, P., & Al-Turjman, F. (2021). Implementation of autonomous driving using Ensemble-M in simulated environment. *Soft Computing*, *25*(18), 12429-12438.

[29] 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.

[30] Kumar, R., Gupta, M., Ahmed, S., Alhumam, A., & Aggarwal, T. (2022). Intelligent Audio Signal Processing for Detecting Rainforest Species Using Deep Learning. *Intelligent Automation & Soft Computing*, *31*(2).

[31] Gupta, M., Singh, A., Jain, R., Saxena, A., & Ahmed, S. (2021). Multi-class railway complaints categorization using Neural Networks: RailNeural. *Journal of Rail Transport Planning & Management*, *20*, 100265.

[32] 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.

[33] Gupta, M., Jain, R., Gupta, A., & Jain, K. (2020). Real-Time Analysis of COVID-19 Pandemic on Most Populated Countries Worldwide. *CMES-Computer Modeling in Engineering & Sciences*, *125*(3).

[34] Jain, D. K., Jain, R., Cai, L., Gupta, M., & Upadhyay, Y. (2020, July). Relative vehicle velocity estimation using monocular video stream. In *2020 International Joint Conference on Neural Networks (IJCNN)* (pp. 1-8). IEEE.

[35] Agarwal, A., Kumar, R., & Gupta, M. (2022, December). Review on Deep Learning based Medical Image Processing. In *2022 IEEE International Conference on Current Development in Engineering and Technology (CCET)* (pp. 1-5). IEEE.

[36] Kaur, R., Kumar, R., & Gupta, M. (2021, December). Review on Transfer Learning for Convolutional Neural Network. In *2021 3rd International Conference on Advances in Computing, Communication Control and Networking (ICAC3N)* (pp. 922-926). IEEE.

[37] Gupta, M., & Kumar, P. (2021). Robust neural language translation model formulation using Seq2seq approach. *Fusion: Practice and Applications*, *5*(2), 61-67.

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

[39] 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.

[40] Gupta, M., & Yadav, R. (2011). Statistical approach of social network in community mining. *International Journal of Information Technology and Knowledge Management*, *4*, 43-46.

[41] Kour, S., Kumar, R., & Gupta, M. (2021, October). Study on detection of breast cancer using Machine Learning. In *2021 International Conference in Advances in Power, Signal, and Information Technology (APSIT)* (pp. 1-9). IEEE.

[42] Vaiyapuri, T., & Gupta, M. (2021). Traffic accident severity prediction and cognitive analysis using deep learning. *Soft Computing*, 1-13.