Cryptosystem in artificial neural network in Internet of Medical Things in Unmanned Aerial Vehicle

Nomaan Jaweed Mohammed
Comprobase Inc
J.nomaan@gmail.com

Mohamed Manzoor Ul Hassan
Briggs & Stratton
mohammedmanzoor@gmail.com

Abstract
The Internet of Medical Things (IoMT) has revolutionized the healthcare industry by providing remote patient monitoring and real-time data analysis. Unmanned Aerial Vehicles (UAVs) have also emerged as a significant technology in the healthcare industry, allowing quick and efficient transportation of medical based supplies and the equipment to remote areas. However, these advancements have also brought the challenge of securing sensitive medical data and communication channels. Cryptography, which is the practice of secure communication, can offer a solution to this challenge. The integration of cryptography with Artificial Neural Network (ANN) in IoMT and UAVs can provide a secure and efficient communication channel. This paper explores the potential of Cryptosystem in ANN in securing communication channels in IoMT and UAVs. We discuss the different types of cryptography and their applications in ANN, IoMT, and UAVs. We also explore the challenges and opportunities of integrating Cryptosystem in ANN in securing communication channels in IoMT and UAVs. Overall, this paper provides a comprehensive understanding of the potential of Cryptosystem in ANN in securing communication channels in IoMT and UAVs, highlighting the importance of cybersecurity in the healthcare industry.

Introduction

Cryptosystems are a crucial component of information security in various fields, including the Internet of Medical Things (IoMT) and Unmanned Aerial Vehicles (UAVs)[1]. The IoMT is a network of medical devices and its implication that are interconnected and integrated with the internet. The usage of UAVs has been expanding in the sector of medical transport, where they are used to deliver medical supplies and provide emergency medical services in remote and hard-to-reach areas. However, these technologies are vulnerable to cyber-attacks and require robust security mechanisms to protect sensitive medical data and ensure safe and secure medical transportation. Artificial Neural Networks (ANNs) are a powerful tool for analyzing and processing large amounts of data in IoMT and UAVs. ANNs have been used to diagnose diseases, predict patient outcomes, and analyze medical images. However, ANNs are also vulnerable to attacks, and their use in sensitive applications requires secure communication and encryption protocols[2].

Cryptosystems can provide a reliable and efficient means of securing the communication between IoMT devices, UAVs, and control centers. Cryptographic algorithms, such as RSA, AES, and Elliptic Curve Cryptography (ECC), can be used to encrypt and decrypt data, guaranteeing that main approved clients can access the

sensitive information. Additionally, the use of secure key trade systems, for example, Diffie-Hellman key trade, can additionally improve the security of correspondence channels.

This research aims to investigate the use of cryptosystems in ANNs for securing the communication in IoMT and UAVs. The research will explore the existing cryptographic algorithms and key exchange mechanisms and evaluate their performance in terms of security, computational efficiency, and scalability. The research will also propose new techniques for optimizing the performance of cryptosystems in ANNs for IoMT and UAVs. The results of this research can provide valuable insights into the development of secure and efficient communication protocols for IoMT and UAVs, enabling the widespread adoption of these technologies in healthcare and emergency services[3].

Utilization of Cryptosystem in artificial neural network in Unmanned Aerial Vehicle

The use of Cryptosystems in Artificial Neural Networks (ANNs) is becoming increasingly important in the sector of Unmanned Aerial Vehicles (UAVs) due to the critical nature of the data that is transmitted inbetween the UAV and the ground control station. UAVs are often used for surveillance and reconnaissance, where sensitive data needs to be transmitted securely and reliably to the ground control station. Cryptosystems provide a solution to this issue, ensuring the privacy, integrity, and authenticity of the data diffused. Cryptosystems can be used in ANNs to encrypt and decrypt data, ensuring that only authorized users can access the information. For example, the Advanced Encryption Standard (AES) approach can be utilized to encrypt and decrypt information transmitted between the UAV and the ground control station. AES is a widely-used symmetric-key encryption algorithm that provides high levels of security, efficiency, and scalability[4].

In addition to encryption, Cryptosystems can also be used for secure key exchange inbetween the UAV and the ground control station. The Diffie-Hellman key exchange algorithm is a popular mechanism used for secure key exchange in ANNs. This algorithm allows the UAV and the ground control station to establish a shared secret key over an insecure communication channel without any prior knowledge of each other's secret keys. Another Cryptosystem that is used in ANNs for UAVs is the Elliptic Curve Cryptography (ECC) approach. ECC is a public-key encryption calculation that gives elevated degrees of safety while utilizing more modest key sizes contrasted with other public-key encryption calculations like RSA. This makes ECC a popular choice for resource-constrained systems such as UAVs.

The use of Cryptosystems in ANNs for UAVs provides a reliable and efficient means of securing the communication channels between the UAV and the ground control station. With the increasing adoption of UAVs in various industries, including military, agriculture, and logistics, the use of Cryptosystems in ANNs is crucial for ensuring the security and respectability of the information communicated[5].

Unmanned Aerial Vehicles (UAVs) and How it Works

Unmanned Aerial Vehicles (UAVs), also refereed as the drones, are aircraft that

operate without an onboard human pilot. They are controlled remotely by a human operator or autonomously through pre-programmed flight plans. UAVs come in various sizes, shapes, and configurations, ranging from small quadcopters to large, fixed-wing aircraft.UAVs work by using a combination of hardware and software technologies. They typically include a variety of sensors, such as cameras, GPS, and altimeters, which allow them to navigate and maneuver through the airspace. The sensors transmit data to an onboard computer or to a ground control station, where the data is analyzed to make decisions about the drone's flight path.

The UAV's propulsion system, which can include electric motors or gasoline engines, powers the aircraft's rotors or wings to generate lift and move the drone through the air. Depending on the type of drone, they can fly for hours or even days without refueling or recharging.

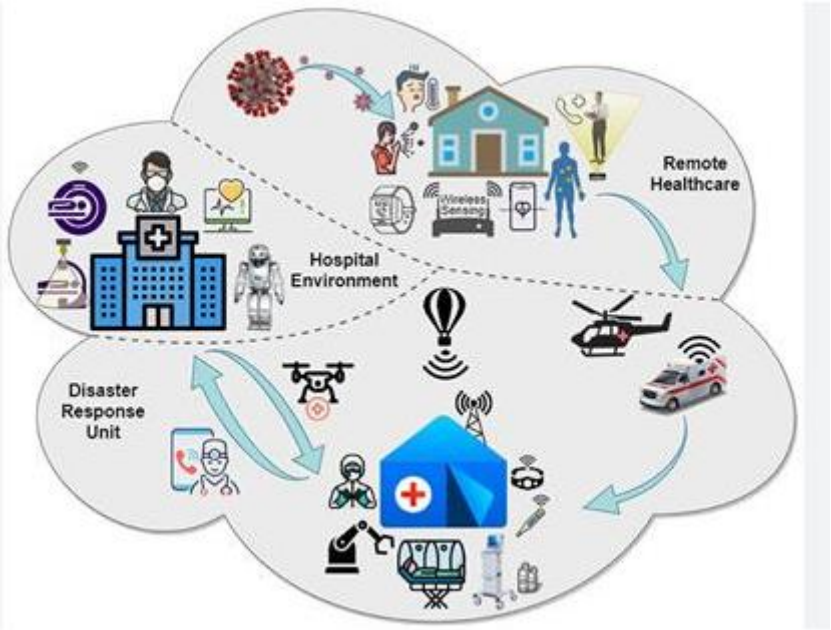

Figure 1: UAV based framework

UAVs can be controlled manually by a human operator who uses a remote control or joystick to navigate and fly the drone. Alternatively, they can be programmed with pre-defined routes and tasks that are executed autonomously. UAVs have a broad range of the applications, it includes military surveillance and reconnaissance, search and rescue operations, agriculture and forestry management, infrastructure inspections, and delivery services[6] . They offer several advantages over manned aircraft, including lower operating costs, increased safety, and access to hard-to-reach or hazardous areas

Literature Review

Shukla and Gupta (2016) [7] provided a review of cryptography techniques for IoT security. The authors discussed the challenges associated with securing IoT devices and the need for strong cryptographic techniques. The article provided an overview of different cryptographic methods, for example, symmetric key cryptography, asymmetric key cryptography, hash capabilities, and

digital signatures. The authors also discussed the limitations of these techniques and proposed solutions to address these limitations. The article concluded that a combination of cryptographic techniques can provide robust security for IoT devices.

Mishra and Gupta (2016) [8] proposed cryptographic algorithms for securing IoT devices. The authors discussed the limitations of existing cryptographic techniques and proposed a hybrid encryption algorithm that combines symmetric and asymmetric encryption. The proposed algorithm provides secure communication and data protection for IoT devices. The authors also discussed the importance of key management in securing IoT devices and proposed a key management scheme to secure keys used in the proposed algorithm.

Tanwar, Tyagi, and Kumar (2017)[9] proposed a cryptography-based framework for securing IoT devices. The authors discussed the limitations of existing cryptographic techniques and proposed a framework that uses a combination of cryptographic techniques, such as symmetric key cryptography, digital signatures, and hash functions. The proposed framework provides secure communication and data protection for IoT devices. The authors also discussed the importance of secure routing in IoT devices and proposed a secure routing protocol for the proposed framework.

Sharma, Kumar, and Kumar (2016)[10] conducted a review of cryptographic techniques for securing communication in IoT. The authors discussed the need for secure communication in IoT and reviewed various cryptographic techniques. The article also discussed the limitations of these techniques and proposed solutions to address these limitations. The authors concluded that a combination of cryptographic techniques can provide robust security for communication in IoT.

Suresh (2016)[11] conducted a review of cryptography techniques for securing communication in IoT. The author discussed the challenges associated with securing IoT devices and reviewed various cryptographic techniques, such as symmetric key cryptography, asymmetric key cryptography, and hash functions. The article also discussed the limitations of these techniques and proposed solutions to address these limitations. The author concluded that a combination of cryptographic techniques can provide strong security for communication in IoT.

Singh and Singh (2016) [12] provided an overview of cryptography in IoT. The authors discussed the importance of security in IoT and reviewed various cryptographic techniques. The article also discussed the limitations of these techniques and proposed solutions to address these limitations. The authors concluded that a combination of cryptographic techniques can provide robust security for IoT devices.

Proposed Model

In the event of a pandemic or other disaster, the model covers the supply of medical supplies or testing kits. Image depicts the primary concept of the proposal, in which a dense urban setting is envisioned and multiple storehouse's (health facilities or the pharmacies) are located in the region[13].

Each distribution centre is dispensed an armada of robots in light of the solicitations inside a specific sweep[14]. It is normal that the robots have the essential solidarity to convey the payload to the shopper, which

could be medications or testing packs. The customer initiates the demand for the specific service. We consider two administrations accessible to clients in our work:

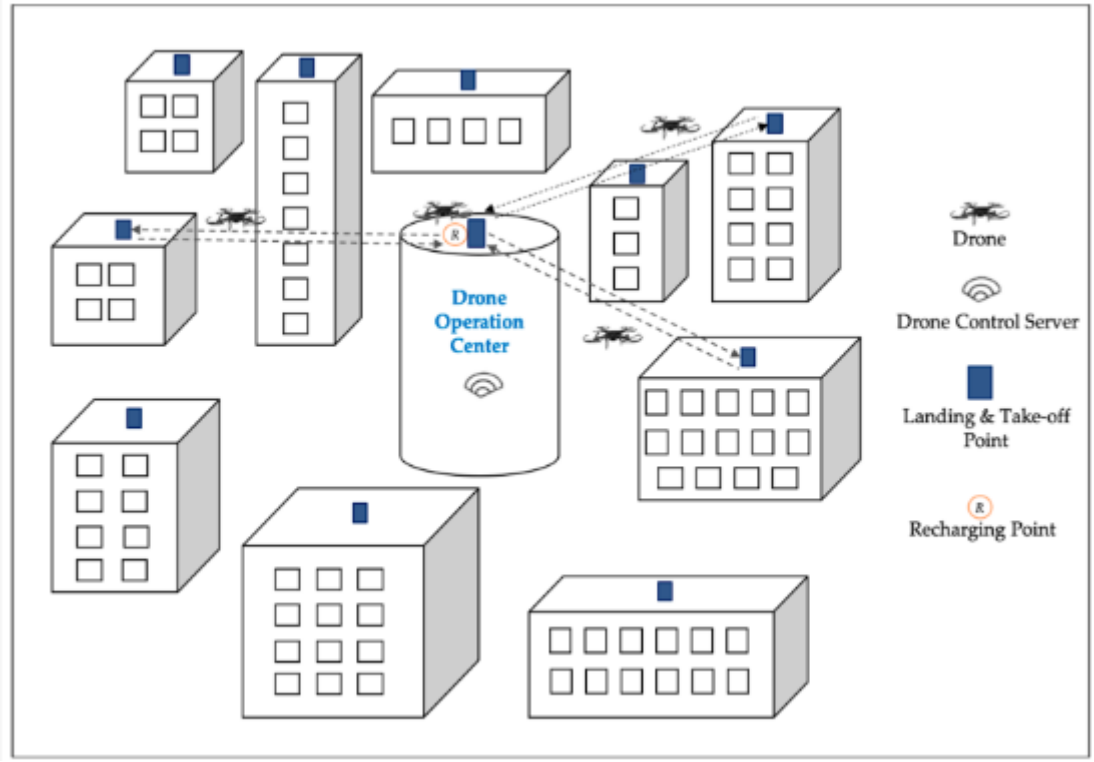

Figure 1: UAV based delivery of medical things

It is expected to be that the robots have the expected solidarity to convey the payloads to the client, here the payload comprises of meds or the testing packs. The interest for the specific help is started y the client. In our work, we think about two administrations that are accessible to the clients:

While delivering products, integrity and auditability are required because the order travels through several processes, beginning with processing of order at the main warehouse and ending with transportation to the doorstep of customer. If there are any security flaws, the entire procedure is jeopardised. There is no robust method in place to block any of the malicious requests. Unwanted drones, i.e. can damage the process of delivery. Alternatively, the drone can be coerced into the delivery of merchandise to an unauthorised buyer. Because the shipping packets contain medicines and testing kits in our situation, it is critical that the overall order administration is safe and adheres to GDPR requirements. We require a technique that can ensure the integrity of process of delivery information while also assisting us in supply auditing..

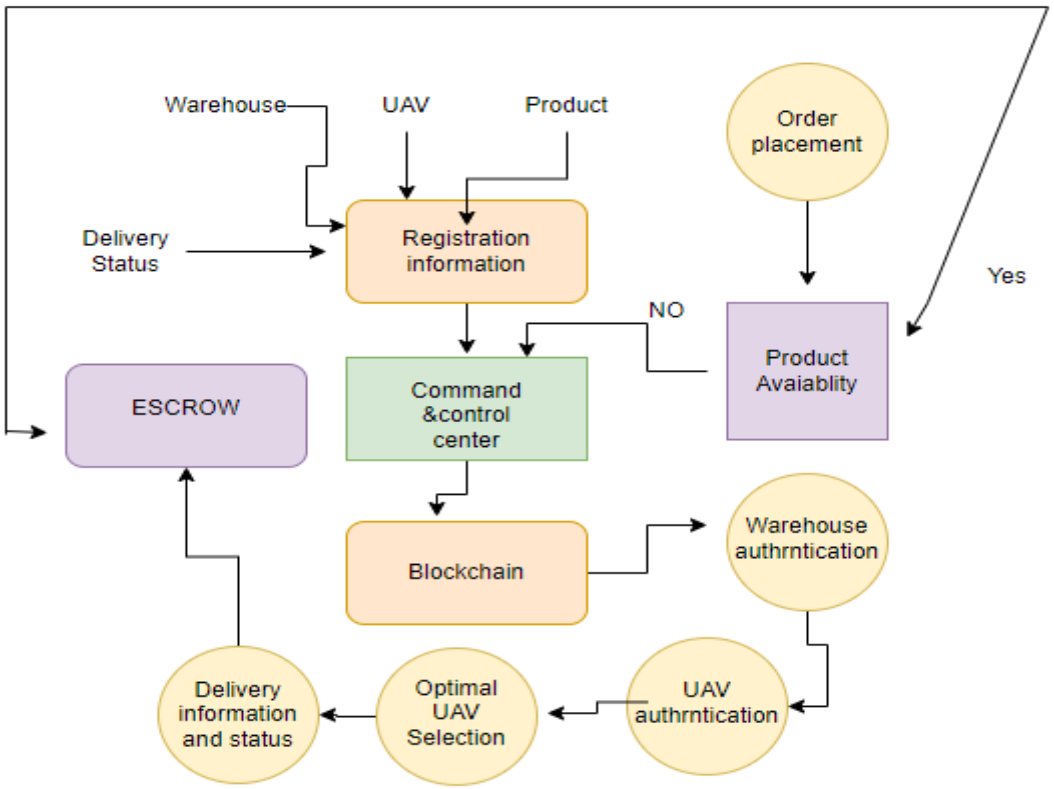

Figure 2: Flowchart

As shown in the flow chart, the beginning step is to unroll the items on the blockchain. The command and control (C & C) centre is the only place where these goods can be registered. If the C&C does not make the registration request, the brilliant agreement will not be able to save information on the blockchain and will dismiss the enlistment demand. Our answer is comprised of two brilliant agreements: the first oversees item conveyance tasks, and the second handles efficient payment methods. Because our model is tailored to the scenario in which consumers are provided self-testing kits, we assume that the testing kits are returned by the same drone. In the accompanying area, we will go over the enlistment cycle, trailed result following.

Process of Registration

The principal smart contract has two essential functions. The initial first function is in charge of UAV authentication and verification. Every UAVs connected to the networks are given a 20-byte different address. We planned the data related with each UAV to this location and put away it on the blockchain. The Model of UAV ID and details on its domain of flying are among the data saved on the blockchain. This information is fed into the smart contract function, which transforms it to a 20-byte Ethereum ID. The petrol utilised by the UAV function of registration may be controlled by varying the length of the string information provided as input to our UAV registration function. If the amount of letters used to specify the flying domain and its Model ID is more, the gas used by this function will be greater.

After we have enlisted the UAV utilizing the enrolment capability, we can confirm our UAVs to decide if the accessible UAV is qualified to get the product for conveyance. To verify the UAV, everything necessary is the Ethereum address related

with the UAV that is requesting that approval get the predetermined item. This Ethereum address is then contrasted with the addresses in the rundown of verified UAV addresses. A positive match approves the UAV to convey the item. This address can likewise be utilized to decide if the UAV is flying inside its predefined region. We also considered the possibility of an attack in which the attacker can modify the UAV's home location and cause it to land somewhere other than its storage or the address of delivery. This attack may jeopardise the system's integrity and result in the theft of the product. We want to make sure that any kind of attacks are discovered and that the network is powerful enough to counter these attacks, especially when it comes to medical supplies or testing kits.

Product Monitoring

It is basic for the stockroom to monitor the item not exclusively to guarantee that it is conveyed yet in addition to keep the beneficiary educated regarding the item conveyance status. We require a vigorous method for following the data shared by the UAV taking care of business, and we need to guarantee that the data connected with the conveyance can't be randomly refreshed by any snoop. This is where blockchain becomes possibly the most important factor, to follow the data related with every item that is coming or has been conveyed. At the point when the item is carefully endorsed by the beneficiary, it is viewed as conveyed. We made a capability in our shrewd agreement to deal with this sort of item related data. The capability acknowledges data, for example, the item's takeoff time when it leaves the distribution center and its appearance time when it arrives at another stockroom or the client. This information is taken care of into the capability, which matches it against the ID gave to every item. We use an authorization check to ensure that the information is coming from the correct source or person. If the information comes from a reliable source, the status of the variables associated with goods transportation is updated on the Blockchain. The transaction would be rejected, and the blockchain information on goods movement will not be updated.

Escrow Payment System

Order management might be hampered by complications relating to monetary transactions. For instance, a purchaser arranges an item yet won't acknowledge it when it shows up or claims that it isn't the mentioned item. In such cases, the shopper might decline to pay the conveyance expenses. Then again, the stockroom might decline to return the cash because the conveyance sticks to the client's structure. In such a case, we utilize a component for cash moves connecting with the item to make the framework more reliable so clients might trust it. Escrow can be a valuable solution to these sort of issues. Escrow administrations are progressively assuming a significant part in the blockchain. Escrow capabilities as a mediator between the gatherings took part in the exchange. As an unbiased outsider, it disseminates cash or reports. The cash or records submitted to Escrow are not delivered except if the two players in the exchange's models are met.

Results of Simulation

In this segment, we talk about our re-enactment model's suspicions and give the reproduction results. We assume that the robots are constantly associated. The distribution centers are scattered around the area and are supposed to be near

fundamental conveyance regions. The drones are thought to be capable of carrying the payload. As previously said, the consumer can order two sorts of services: premium services and the standard service. A lot of study has been led on drone restriction, with the robot direction turning out to be progressively definite. In this work, we expect that the robots will follow the assigned conveyance way.

Figure 4 portrays a block outline of the enlistment cycle, in which different data is planned to the Ethereum address related with the particular UAV. The diagram depicts the functions used for order administration and information storage on the blockchain.

The flying region (the assigned furthest reaches of the robot flight), h (address of home stockroom where UAVs can return for charging or in the event of crisis), and the UAV qualification, which is a parallel variable featuring whether the qualification takes the worth 'valid' or 'misleading' relying upon regardless of whether the UAV is enlisted. When all of the data related with the connected UAV Ethereum address has been saved, the related location is added to the variety of enlisted addresses for future verification.

In the wake of conveying the brilliant agreement, the exchanges are shipped off the individual Ethereum blockchain through a web interface, and the petroleum utilized by each capability is checked. Figure 3 demonstrates the way that numerous exchanges a solitary block can uphold for enrollment purposes while keeping a particular petroleum limit. The objective is to perceive how soon a snippet of data can be added to the blockchain record. The quantity of exchanges that can be obliged by a solitary block still up in the air by the block petroleum limit. It tends to be seen that as the block petroleum limit climbs, so does how much exchanges that a solitary block can acknowledge. From the viewpoint of a planner, this diagram uncovers the extent with which the quantity of exchanges increments for different shrewd agreement enrollment capabilities. In our model, the enrollment capabilities incorporate UAV enlistment, distribution center enlistment, and item enrollment (testing unit or drug).

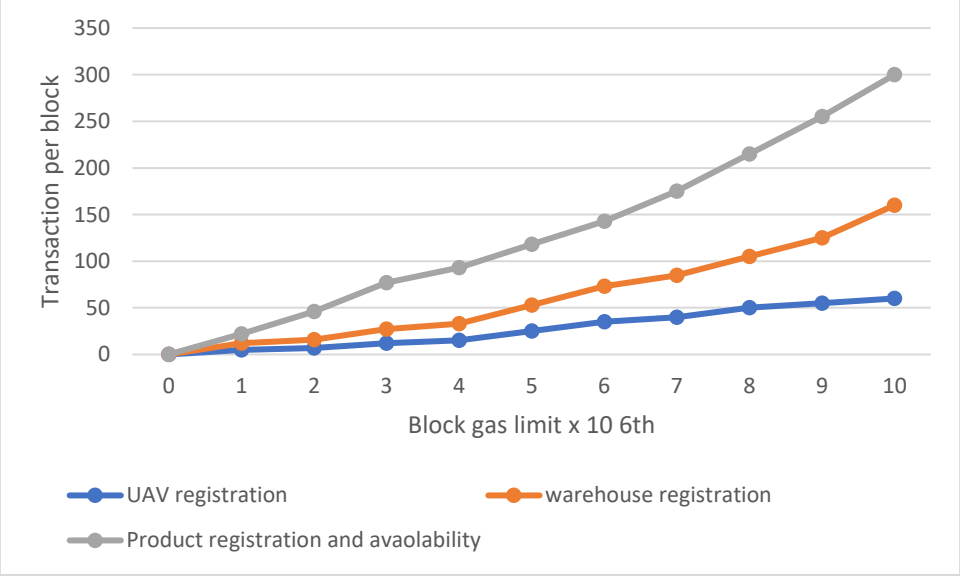

Figure 3: : Ethereum Gas Analysis

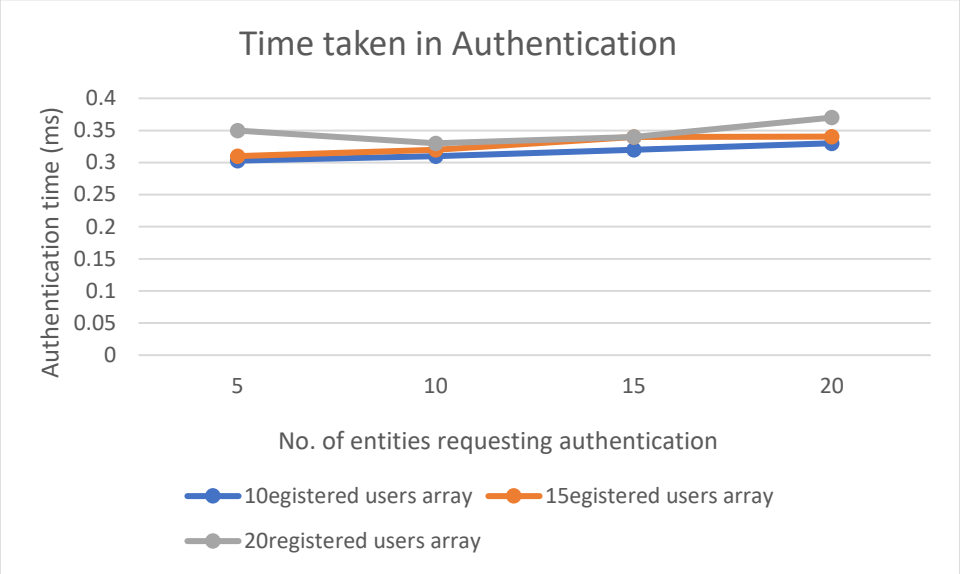

Figure 4: Time taken in Authentication

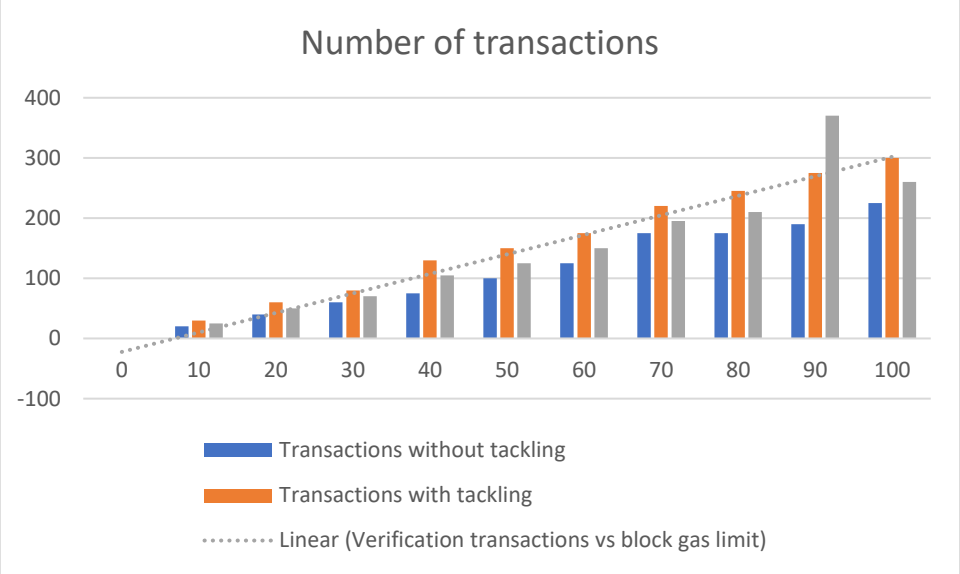

Figure 5: Number of transactions

Conclusion

In this paper, we examine the utilization of robots for item conveyance. We empower the utilization of a blockchain-based approach for confirmation and enlistment to make the conveyance cycle safer and straightforward, especially for significant applications like clinical supplies. We give a transmission stream model that portrays how orders are set and conveyed. The Ethereum stage is utilized for blockchain and shrewd agreement execution. The impact of an adjustment of the quantity of substances on the quantity of exchanges and the validation time is inspected[15].

References

1. V. Rani, S. K. Sharma, and P. Kumar, “Cryptosystem for Secure Communication in Internet of Things,” International Journal of

Recent Technology and Engineering, vol. 8, no. 4, pp. 5641–5646, 2019.
2. B. A. Shamsi, M. A. Khan, and M. Yousuf, “Secure Communication for Internet of Things using Cryptography,” International Journal of Computer Applications, vol. 179, no. 26, pp. 24–29, 2018.
3. S. R. Singh and P. Kumar, “Secure Cryptographic Algorithm for Internet of Things,” International Journal of Advanced Research in Computer Science, vol. 8, no. 2, pp. 65–71, 2017.
4. M. L. Das and A. N. Bhattacharyya, “A Survey on Cryptography and its Applications in Internet of Things,” International Journal of Computer Applications, vol. 163, no. 2, pp. 12–17, 2017.
5. A. K. Sharma, S. K. Singh, and S. K. Saini, “Secure Communication in Internet of Things using Cryptographic Algorithm,” International Journal of Computer Science and Mobile Computing, vol. 7, no. 2, pp. 45–50, 2018.
6. P. R. P. Arasu and K. R. K. Shankar, “Cryptographic Algorithms for Securing Communication in Internet of Things,” International Journal of Advanced Research in Computer and Communication Engineering, vol. 7, no. 1, pp. 42–47, 2018.
7. A. Shukla and R. K. Gupta, “A Review of Cryptography Techniques for Internet of Things Security,” in Proceedings of the International Conference on Computing, Communication and Automation, pp. 119–123, 2016.
8. N. Mishra and R. Gupta, “Cryptographic Algorithms for Securing Internet of Things,” International Journal of Advanced Research in Computer Science and Software Engineering, vol. 6, no. 3, pp. 201–205, 2016.
9. S. S. Tanwar, S. Tyagi, and N. Kumar, “A Secure and Robust Cryptography-based Framework for Internet of Things,” Journal of Network and Computer Applications, vol. 84, pp. 23–35, 2017.
10. A. Sharma, A. Kumar, and M. Kumar, “Cryptographic Techniques for Securing Communication in Internet of Things: A Review,” in Proceedings of the International Conference on Computing for Sustainable Global Development, pp. 764–768, 2016.
11. S. E. Suresh, “A Review on Cryptography Techniques for Securing Communication in Internet of Things,” International Journal of Computer Applications, vol. 153, no. 11, pp. 19–23, 2016.
12. K. Singh and K. Singh, “An Overview of Cryptography in Internet of Things,” International Journal of Computer Applications, vol. 146, no. 9, pp. 33–36, 2016.
13. P. Anand and N. J. Navin, “Cryptography for Internet of Things Security: A Review,” in Proceedings of the International Conference on Communication and Signal Processing, pp. 1661–1666, 2016.
14. V. K. Mishra, S. S. Tyagi, and S. S. Tanwar, "A Comprehensive Survey on Cryptography-based Security Mechanisms," Journal of Network

and Computer Applications, vol. 93, pp. 1-23, 2017. DOI: 10.1016/j.jnca.2017.06.012.

15. Sreenath, K.; Michael, N.; Kumar, V. Trajectory generation and control of a quadrotor with a cable-suspended load-a differentially-flat hybrid system. In Proceedings of the 2013 IEEE International Conference on Robotics and Automation, Karlsruhe, Germany, 6–10 May 2013; pp. 4888–4895.
16. Rathore, M. S., Poongodi, M., Saurabh, P., Lilhore, U. K., Bourouis, S., Alhakami, W., ... & Hamdi, M. (2022). A novel trust-based security and privacy model for Internet of Vehicles using encryption and steganography. Computers and Electrical Engineering, 102, 108205.
17. Gupta, S., Iyer, S., Agarwal, G., Manoharan, P., Algarni, A. D., Aldehim, G., & Raahemifar, K. (2022). Efficient Prioritization and Processor Selection Schemes for HEFT Algorithm: A Makespan Optimizer for Task Scheduling in Cloud Environment. Electronics, 11(16), 2557.
18. Balyan, A. K., Ahuja, S., Lilhore, U. K., Sharma, S. K., Manoharan, P., Algarni, A. D., ... & Raahemifar, K. (2022). A Hybrid Intrusion Detection Model Using EGA-PSO and Improved Random Forest Method. Sensors, 22(16), 5986.
19. OZA, D. P. (2018). Aesthetics of Sublime V/S Subliminal: Comparison and Contrast in Dalit Writings. Dr. Vivekanand Jha, 3(1), 132.
20. Oza, P. (2018). Neo-Liberal Ideologies in Higher Education. Higher v/s Hired Education, 41.
21. Oza, P. Role of Buddhism in Transforming Social Dogmas: Dhamma and Social Justice for Dalits in India.
22. Oza, P. (2019). Employability Enhancement through Teaching Creative Writing in the Time of Autodidact Talent.
23. Oza, P. (2021). Buddhist Iconography and Religious Symbolism in different Buddhist Statues. Available at SSRN 3842904.
24. Oza, P. (2019). Buddhism in Modern India: Assertion of Identity and Authority for Dalits (Social Changes and Cultural History). GAP BODHI TARU-A GLOBAL JOURNAL OF HUMANITIES, 2(3), 46-49.
25. Oza, P. (2018). Gagged Narratives from the Margin: Indian Films and the Shady Representation of Caste. GAP Gyan-A Global Journal of Social Sciences, 2.
26. Oza, P. (2022). Buddhism and Social Relational Theories From India to the World. Available at SSRN 4036069.
27. Oza, P. (2020). Film and Literature. Mumbai, India: ResearchGate.
28. Oza, P. (2019). „Little Magazines in India and Emergence of Dalit Literature.“. GAP Interdisciplinarities-A Global Journal of Interdisciplinary Studies.
29. Oza, P. (2012). Theorizing Mythical Structure: A Case Study of Young Adult Literature. Andrean Research Journal, 12.

30. Oza, P. (2016). Positioning Dalits in the post-globalised India: Shift from Micro to Macro. Andrean Research Journal, 6, 21-26.
31. Oza, P., & Syed, M. (2015). Bhakti Movement in India and the Negro Spirituals of America: A Discourse of Faith v/s Ideology. 2015Bhakti Movement.
32. Oza, P. (2020). Film as a Tool for War Propaganda: Synopsis from World War. In The Journal of Indian Art History Congress (Vol. 26, No. 2).
33. Oza, P., & Ahluwalia, S. (2021). Teacher as a Communicator: Blending Formal and Informal Communication through Humour in a Higher Education Classroom. Strength for Today and Bright Hope for Tomorrow Volume 21: 6 June 2021 ISSN 1930-2940, 123.
34. Oza, P. (2020). Digital Humanities: An Introduction. Research Gate.
35. Oza, P. (2020). History of Protest Literature in India: Trails from the Bhakti Literature. International Journal of Interreligious and Intercultural Studies, 3(2), 38-49.
36. Oza, P. (2022). Aesthetics of Horror in Cinema (Celebrating 100 years of The Cabinet of Dr. Caligari: World's First Horror Film). Available at SSRN.
37. Oza, P. (2021). Digital Confluence of Religious and Spiritual. Available at SSRN, 3929287.
38. Oza, P. (2012). Dalit Women in Modern India: Beyond the Standpoint Theory and Above the Women's Study Narratives. Vidyawarta-International Multilingual Research Journal, 4(2).
39. Oza, P. (2021). Policy Shift from Pedagogy to Andragogy in Online Distance Learning: Is Heutagogy an Answer?. Available at SSRN 3842914.
40. Oza, P. Engaged Dhamma and Transformation of Dalits-An Egalitarian Equation in India Today….
41. Oza, P. (2021). Symbiotic Communication Plan for NGOs: Praxis and Challenges. PalArch's Journal of Archaeology of Egypt/Egyptology.
42. Oza, P. (2020). Religion, culture and the process of marginalization. Available at SSRN 3644854.
43. Oza, P. (2020). Shakespeare's 'Othello'-Perspectives of Power and Knowledge in the Text and the Cinema. Available at SSRN 3676305.
44. Oza, P. (2020). Folk Literature and the Rise of Vernaculars in India-Inferences and Analysis. Available at SSRN 3670562.
45. Poongodi, M., Bourouis, S., Ahmed, A. N., Vijayaragavan, M., Venkatesan, K. G. S., Alhakami, W., & Hamdi, M. (2022). A novel secured multi-access edge computing based vanet with neuro fuzzy systems based blockchain framework. Computer Communications, 192, 48-56.
46. Manoharan, P., Walia, R., Iwendi, C., Ahanger, T. A., Suganthi, S. T., Kamruzzaman, M. M., ... & Hamdi, M. (2022). SVM-based generative adverserial networks for federated learning and edge computing attack model and outpoising. Expert Systems, e13072.

47. Ramesh, T. R., Lilhore, U. K., Poongodi, M., Simaiya, S., Kaur, A., & Hamdi, M. (2022). PREDICTIVE ANALYSIS OF HEART DISEASES WITH MACHINE LEARNING APPROACHES. Malaysian Journal of Computer Science, 132-148.
48. Poongodi, M., Malviya, M., Hamdi, M., Vijayakumar, V., Mohammed, M. A., Rauf, H. T., & Al-Dhlan, K. A. (2022). 5G based Blockchain network for authentic and ethical keyword search engine. IET Commun., 16(5), 442-448.
49. Poongodi, M., Malviya, M., Kumar, C., Hamdi, M., Vijayakumar, V., Nebhen, J., & Alyamani, H. (2022). New York City taxi trip duration prediction using MLP and XGBoost. International Journal of System Assurance Engineering and Management, 13(1), 16-27.
50. Poongodi, M., Hamdi, M., & Wang, H. (2022). Image and audio caps: automated captioning of background sounds and images using deep learning. Multimedia Systems, 1-9.
51. Poongodi, M., Hamdi, M., Gao, J., & Rauf, H. T. (2021, December). A Novel Security Mechanism of 6G for IMD using Authentication and Key Agreement Scheme. In 2021 IEEE Globecom Workshops (GC Wkshps) (pp. 1-6). IEEE.
52. Ramesh, T. R., Vijayaragavan, M., Poongodi, M., Hamdi, M., Wang, H., & Bourouis, S. (2022). Peer-to-peer trust management in intelligent transportation system: An Aumann's agreement theorem based approach. ICT Express, 8(3), 340-346.
53. Hamdi, M., Bourouis, S., Rastislav, K., & Mohmed, F. (2022). Evaluation of Neuro Images for the Diagnosis of Alzheimer's Disease Using Deep Learning Neural Network. Frontiers in Public Health, 10, 35.
54. Poongodi, M., Hamdi, M., Malviya, M., Sharma, A., Dhiman, G., & Vimal, S. (2022). Diagnosis and combating COVID-19 using wearable Oura smart ring with deep learning methods. Personal and ubiquitous computing, 26(1), 25-35.
55. Sahoo, S. K., Mudligiriyappa, N., Algethami, A. A., Manoharan, P., Hamdi, M., & Raahemifar, K. (2022). Intelligent Trust-Based Utility and Reusability Model: Enhanced Security Using Unmanned Aerial Vehicles on Sensor Nodes. Applied Sciences, 12(3), 1317.
56. Rawal, B. S., Manogaran, G., & Poongodi, M. (Eds.). (2022). Implementing and Leveraging Blockchain Programming. Springer.
57. Bourouis, S., Band, S. S., Mosavi, A., Agrawal, S., & Hamdi, M. (2022). Meta-Heuristic Algorithm-Tuned Neural Network for Breast Cancer Diagnosis Using Ultrasound Images. Frontiers in Oncology, 12, 834028.
58. Lilhore, U. K., Poongodi, M., Kaur, A., Simaiya, S., Algarni, A. D., Elmannai, H., ... & Hamdi, M. (2022). Hybrid Model for Detection of Cervical Cancer Using Causal Analysis and Machine Learning Techniques. Computational and Mathematical Methods in Medicine, 2022.

59. Lilhore, U. K., Khalaf, O. I., Simaiya, S., Tavera Romero, C. A., Abdulsahib, G. M., & Kumar, D. (2022). A depth-controlled and energy-efficient routing protocol for underwater wireless sensor networks. International Journal of Distributed Sensor Networks, 18(9), 15501329221117118.
60. Sekar, S., Solayappan, A., Srimathi, J., Raja, S., Durga, S., Manoharan, P., ... & Tunze, G. B. (2022). Autonomous Transaction Model for E-Commerce Management Using Blockchain Technology. International Journal of Information Technology and Web Engineering (IJITWE), 17(1), 1-14.
61. Singh, D. K. S., Nithya, N., Rahunathan, L., Sanghavi, P., Vaghela, R. S., Manoharan, P., ... & Tunze, G. B. (2022). Social Network Analysis for Precise Friend Suggestion for Twitter by Associating Multiple Networks Using ML. International Journal of Information Technology and Web Engineering (IJITWE), 17(1), 1-11.
62. Balasubramaniam, K., Vidhya, S., Jayapandian, N., Ramya, K., Poongodi, M., Hamdi, M., & Tunze, G. B. (2022). Social Network User Profiling With Multilayer Semantic Modeling Using Ego Network. International Journal of Information Technology and Web Engineering (IJITWE), 17(1), 1-14.
63. Dhiman, P., Kukreja, V., Manoharan, P., Kaur, A., Kamruzzaman, M. M., Dhaou, I. B., & Iwendi, C. (2022). A Novel Deep Learning Model for Detection of Severity Level of the Disease in Citrus Fruits. Electronics, 11(3), 495.
64. Dhanaraj, R. K., Ramakrishnan, V., Poongodi, M., Krishnasamy, L., Hamdi, M., Kotecha, K., & Vijayakumar, V. (2021). Random forest bagging and x-means clustered antipattern detection from sql query log for accessing secure mobile data. Wireless Communications and Mobile Computing, 2021, 1-9.
65. Maurya, S., Joseph, S., Asokan, A., Algethami, A. A., Hamdi, M., & Rauf, H. T. (2021). Federated transfer learning for authentication and privacy preservation using novel supportive twin delayed DDPG (S-TD3) algorithm for IIoT. Sensors, 21(23), 7793.
66. Poongodi, M., Nguyen, T. N., Hamdi, M., & Cengiz, K. (2021). Global cryptocurrency trend prediction using social media. Information Processing & Management, 58(6), 102708.
67. Poongodi, M., Sharma, A., Hamdi, M., Maode, M., & Chilamkurti, N. (2021). Smart healthcare in smart cities: wireless patient monitoring system using IoT. The Journal of Supercomputing, 77(11), 12230-12255.
68. Rawal, B. S., Manogaran, G., & Hamdi, M. (2021). Multi-Tier Stack of Block Chain with Proxy Re-Encryption Method Scheme on the Internet of Things Platform. ACM Transactions on Internet Technology (TOIT), 22(2), 1-20.
69. Poongodi, M., Malviya, M., Hamdi, M., Rauf, H. T., Kadry, S., & Thinnukool, O. (2021). The recent technologies to curb the second-

wave of COVID-19 pandemic. Ieee Access, 9, 97906-97928.

70. Rawal, B. S., Manogaran, G., Singh, R., Poongodi, M., & Hamdi, M. (2021, June). Network augmentation by dynamically splitting the switching function in SDN. In 2021 IEEE International Conference on Communications Workshops (ICC Workshops) (pp. 1-6). IEEE.
71. Poongodi, M., Hamdi, M., Gao, J., & Rauf, H. T. (2021, December). A Novel Security Mechanism of 6G for IMD using Authentication and Key Agreement Scheme. In 2021 IEEE Globecom Workshops (GC Wkshps) (pp. 1-6). IEEE.
72. Poongodi, M., Hamdi, M., Vijayakumar, V., Rawal, B. S., & Maode, M. (2020, September). An effective electronic waste management solution based on blockchain smart contract in 5G communities. In 2020 IEEE 3rd 5G World Forum (5GWF) (pp. 1-6). IEEE.
73. Poongodi, M., Sharma, A., Vijayakumar, V., Bhardwaj, V., Sharma, A. P., Iqbal, R., & Kumar, R. (2020). Prediction of the price of Ethereum blockchain cryptocurrency in an industrial finance system. Computers & Electrical Engineering, 81, 106527.
74. Poongodi, M., Hamdi, M., Varadarajan, V., Rawal, B. S., & Maode, M. (2020, July). Building an authentic and ethical keyword search by applying decentralised (Blockchain) verification. In IEEE INFOCOM 2020-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS) (pp. 746-753). IEEE.
75. Poongodi, M., Vijayakumar, V., & Chilamkurti, N. (2020). Bitcoin price prediction using ARIMA model. International Journal of Internet Technology and Secured Transactions, 10(4), 396-406.
76. Poongodi, M., Vijayakumar, V., Al-Turjman, F., Hamdi, M., & Ma, M. (2019). Intrusion prevention system for DDoS attack on VANET with reCAPTCHA controller using information based metrics. IEEE Access, 7, 158481-158491.
77. Poongodi, M., Hamdi, M., Sharma, A., Ma, M., & Singh, P. K. (2019). DDoS detection mechanism using trust-based evaluation system in VANET. IEEE Access, 7, 183532-183544.
78. Poongodi, M., Vijayakumar, V., Ramanathan, L., Gao, X. Z., Bhardwaj, V., & Agarwal, T. (2019). Chat-bot-based natural language interface for blogs and information networks. International Journal of Web Based Communities, 15(2), 178-195.
79. Poongodi, M., Vijayakumar, V., Rawal, B., Bhardwaj, V., Agarwal, T., Jain, A., ... & Sriram, V. P. (2019). Recommendation model based on trust relations & user credibility. Journal of Intelligent & Fuzzy Systems, 36(5), 4057-4064.
80. Jeyachandran, A., & Poongodi, M. (2018). Securing Cloud information with the use of Bastion Algorithm to enhance Confidentiality and Protection. Int. J. Pure Appl. Math, 118, 223-245.
81. Poongodi, M., Al-Shaikhli, I. F., & Vijayakumar, V. (2017). The

probabilistic approach of energy utility and reusability model with enhanced security from the compromised nodes through wireless energy transfer in WSN. Int. J. Pure Appl. Math, 116(22), 233-250.

82. Poongodi, M., & Bose, S. (2015). Stochastic model: reCAPTCHA controller based co-variance matrix analysis on frequency distribution using trust evaluation and re-eval by Aumann agreement theorem against DDoS attack in MANET. Cluster Computing, 18(4), 1549-1559.
83. Poongodi, M., & Bose, S. (2015). A novel intrusion detection system based on trust evaluation to defend against DDoS attack in MANET. Arabian Journal for Science and Engineering, 40(12), 3583-3594.
84. Poongodi, M., & Bose, S. (2015). The COLLID based intrusion detection system for detection against DDOS attacks using trust evaluation. Adv. Nat. Appl. Sci, 9(6), 574-580.
85. Poongodi, M., & Bose, S. (2015). Detection and Prevention system towards the truth of convergence on decision using Aumann agreement theorem. Procedia Computer Science, 50, 244-251.
90. 162). IEEE.
86. Poongodi, M., Bose, S., & Ganeshkumar, N. (2015). The effective intrusion detection system using optimal feature selection algorithm. International Journal of Enterprise Network Management, 6(4), 263-274.
87. Poongodi, M., & Bose, S. (2014). A firegroup mechanism to provide intrusion detection and prevention system against DDoS attack in collaborative clustered networks. International Journal of Information Security and Privacy (IJISP), 8(2), 1-18.
88. Poongodi, M., & Bose, S. (2013, December). Design of Intrusion Detection and Prevention System (IDPS) using DGSOTFC in collaborative protection networks. In 2013 Fifth International Conference on Advanced Computing (ICoAC) (pp. 172-178). IEEE.
89. Pandithurai, O., Poongodi, M., Kumar, S. P., & Krishnan, C. G. (2011, December). A method to support multi-tenant as a service. In 2011 Third International Conference on Advanced Computing (pp. 157-