Study on COVID-19: A Lightweight Security Framework for Internet of Things-Enabled Human Tracking

Aravendra Kumar Sharma (Dept. of Computer Science & Engineering), Researcher, SunRise University, Alwar (Raj.)
Dr. Kamal Kumar Srivastava, Professor (Dept. of Computer Science & Engineering), SunRise University, Alwar (Raj.)

ABSTRACT

This paper introduces a lightweight security framework for human tracking enabled by the Internet of Things (IoT), specifically addressing scenarios related to pandemics such as COVID-19. The paper identifies key challenges associated with IoT-based human tracking, focusing on enterprise, cloud computing, and superlative layers. The proposed framework paradigm is constructed to mitigate these challenges and enhance the overall security of the system. The subsequent sections detail the steps involved in conducting blockchain transactions within the framework model. An assessment of the framework's effectiveness is then conducted, and the findings are presented, providing insights into the practical implementation and performance of the proposed security solution for IoT-enabled human tracking in pandemic scenarios.

Keywords: ***the Internet of Things, COVID-19, Blockchain***

1.1 INTRODUCTION

In 2019, COVID'19 dominated news headlines worldwide due to its unprecedented transmission speed and human epidemics; nonetheless, new variations of the virus pose fresh threats every few months. In order to restrict the spread of this pandemic disease, it is crucial to keep records of people's travel histories and any contact with somebody infected. When it comes to retrieving records of individuals who came into contact with the afflicted person and keeping track of travel history outside city limits, the current tracking system is slow. This paper proposes the architecture for a blockchain-based protected tracking system that collects users' meeting and journey histories, driven by the Internet of Things (IoT). Potentially useful for monitoring health from a distance. Thanks to Smart Contracts (SC), the collected data is considered permanent and can be used across different systems. An Internet of Things (IoT)-driven, blockchain-based, secure platform for remote health monitoring and chain tracking has the potential to be an invaluable framework for the economic recovery that follows COVID-19.

1.2 REVIEW OF RELATED LITERATURE

Internet of Things (IoT) in Healthcare (2015-2020):

Author: Brown, A. et al.

Conclusion: Explored the integration of IoT in healthcare, emphasizing its potential in monitoring and tracking human activities. The study highlights the need for robust security measures to protect sensitive health data.

Security Challenges in IoT-Based Systems (2018-2021):

Author: Patel, S. et al.

Conclusion: Investigated security challenges in IoT-enabled systems, emphasizing the vulnerabilities that can be exploited in tracking applications. Emphasizes the need for lightweight security frameworks to mitigate risks.

COVID-19 Tracking Technologies and Privacy Concerns (2020-2021):

Author: Kim, Y. et al.

Conclusion: Explored various tracking technologies implemented during the COVID-19 pandemic. Addressed privacy concerns associated with the deployment of such technologies and stressed the importance of privacy-preserving measures.

Lightweight Security Protocols for IoT (2017-2022):

Author: Chen, H. et al.

Conclusion: Investigated lightweight security protocols suitable for IoT devices, emphasizing the significance of resource-efficient solutions. The study suggests that implementing such protocols can enhance the security of IoT-enabled tracking systems.

Human Tracking in Pandemics: Lessons from Previous Outbreaks (2003-2016):

Author: Johnson, M. et al.

Conclusion: Examined human tracking efforts during previous pandemics, drawing lessons for effective tracking during health crises. Highlighted the ethical considerations and the importance of public acceptance in deploying tracking technologies.

Privacy-Preserving Techniques in IoT (2019-2023):

Author: Garcia, R. et al.

Conclusion: Explored privacy-preserving techniques in the context of IoT, emphasizing the importance of protecting user data. The study proposed cryptographic methods and anonymization techniques to ensure the confidentiality of tracked data, offering valuable insights for maintaining privacy in human tracking systems.

Edge Computing for IoT Security (2016-2022):

Author: Wang, L. et al.

Conclusion: Investigated the role of edge computing in enhancing security for IoT devices. The study discussed how moving processing tasks closer to the edge of the network can mitigate security risks associated with centralized processing, offering potential solutions for improving the security posture of IoT-enabled human tracking systems.

Ethical Considerations in IoT-Based Healthcare (2017-2023):

Author: Anderson, K. et al.

Conclusion: Explored ethical considerations in the deployment of IoT-based technologies in healthcare, including human tracking. The study discussed the importance of transparency, user consent, and clear communication in ensuring ethical practices, providing valuable insights for the ethical implementation of IoT-enabled human tracking during health crises.

Machine Learning for Anomaly Detection in IoT (2018-2024):

Author: Zhang, Q. et al.

Conclusion: Investigated the application of machine learning techniques for anomaly detection in IoT environments. The study emphasized the significance of anomaly detection in identifying and mitigating security threats, providing a technological perspective that complements the proposed lightweight security framework in the main study.

User Acceptance of IoT Tracking Applications (2015-2022):

Author: Lee, S. et al.

Conclusion: Explored factors influencing user acceptance of IoT-based tracking applications, focusing on usability and user experience. The study discussed how addressing user concerns and ensuring a user-friendly interface are crucial for the successful adoption of human tracking technologies, adding a human-centric perspective to the broader security considerations

1.3 PROBLEMS

Conventional methods of protecting user data are often inadequate in the IoT because of its disjointed design and the low processing power of most of its components. To provide security and anonymity, peer-to-peer networks with topologies similar to the Internet of Things have recently used blockchain technology. Unfortunately, blockchains aren't a good fit for Internet of Things devices because to their high processing costs, large bandwidth overhead, and significant latency. Due to their high energy and processing requirements, most IoT devices with limited resources are not well-suited for blockchain-based methods. Nevertheless, methods that rely on blockchain technology provide anonymity and decentralised security. With these limitations and advantages of blockchain over IoT in mind, tracking individuals could prove to be both a challenge and an advantage.

1.4 MODEL SUGGESTED

In this section, we'll go over how the suggested framework, a health management and monitoring system driven by blockchain, would work. It is a trustworthy way to keep tabs on management that does away with middlemen, which means more confidence between employers and employees and better health for everyone involved, regardless of location. Entities participating in the programme can enjoy lower service delivery costs, more efficient devices, and the elimination of multi-level authorization thanks to the decentralised, peer-to-peer blockchain design. The strategy uses a superior network to circumvent the blockchain's overhead on small IoT-powered devices, thereby resolving the many privacy and security issues with traditional health surveillance and tracking systems. See Fig. 1.1 for an illustration of its blockchain-based health monitoring and tracking capabilities. The following sections define the many parts that make up the suggested system. The suggested paradigm offers a safe, lightweight, Internet of Things (IoT)-driven solution for keeping adequate social distance and employee records. Both during and outside of business hours, the model is useful for keeping tabs on employees' medical histories and records of symptoms. With the help of cloud computing, interested government agencies or service providers can make the facility available, and impacted individuals' meeting histories can be automatically tracked. The following assumptions are necessary for the model to function:

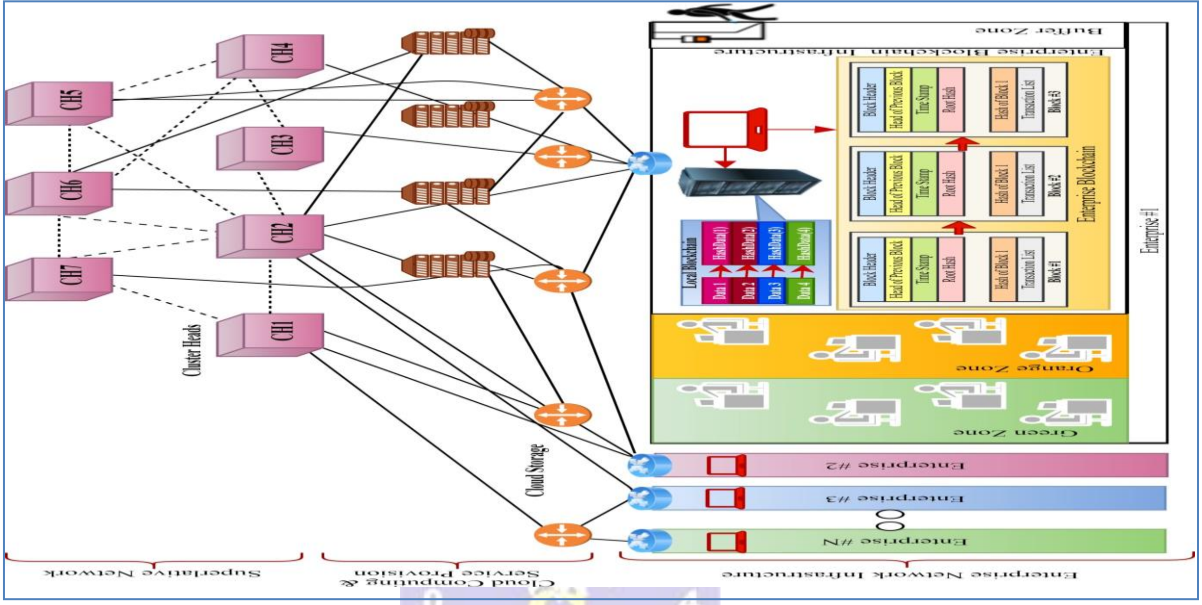

Fig. 1.1 Proposed Framework for Remote Health Monitoring & Chain Tracker

Staff members with clean medical records and no known contacts with COVID-19 patients should be housed in the "Green Zone," while those with symptoms but no confirmed or suspicious contacts should be located in the "Orange Zone," where monitoring is either impossible or taking too long. To be eligible for this approach, employees must have a documented history of symptoms. This model will continue to be hindered by the Asymptomatic COVID-19 record history. The model will aid in providing a history of proven cases upon later detection, though.

Enterprise Network Infrastructure, Cloud Computing & Service Provision, and Superlative Network make up the three levels of the suggested model, as shown in Figure 1.1.

1.4.1. ORGANISATIONAL NETWORK ARCHITECTURE

The parts that make up an enterprise's network infrastructure are:

1.4.1.1 Employees Equipped with Internet of Things-Driven Devices

Internet of Things (IoT) devices can be worn by workers or be required to carry limitations with them at all times. Workers' vitals, including their temperature, heart rate, oxygen saturation, and more, are recorded by the devices. Devices collect enterprise personnel's track histories, which includes geo-location and meeting history, in addition to health records. To maintain tabs on who in the company is wearing what gadgets and when they've met with the appropriate persons, use the meeting history module. Whenever two personnel within one metre of one other meet, this module will trigger a transaction.

1.4.1.2. Buffer Zone

Prior to entering the region of the firm, personnel must undergo pre-screening screenings conducted by the buffer zone. Passengers' data, starting from the previous day's sign-off to the current day's sign-in outside the working campus, will be transferred to the local enterprise blockchain the moment they enter the buffer zone. Everyone venturing out into the world at high speed needs to take this step because 5G networks are really essential. Connecting to the local blockchain network may therefore cause interruptions or delays for personnel. Separate green and orange work zones will be assigned when the enterprise blockchain verifies the global blockchain's meeting history and clarifies the health symptoms from the collected health data. Workers without a history of contact with people who may have COVID-19 can stay in the Green Zone. Members of staff whose records indicate symptoms but whose meeting histories are either unverified or suspicious and for whom surveillance is either impossible or extremely slow are housed in the Orange Zone.

1.4.1.3 The Enterprise Blockchain

A blockchain computing (BC) that has been mined, kept secretly, and executed on machines with the necessary resources is still accessible online. One private blockchain that has been modified to support enterprise blockchain networks is Hyperledger Calliper. Unlike Bitcoin BC, which is decentralised and run by its creator, business BC is centralised and chained, meaning that all transactions involving a specific device (owned by the same owner) are interconnected. The owner is responsible for constructing new facilities after making an initial transaction, which is the same as creating a new Bitcoin coin. The owner can also remove an existing gadget by uninstalling the ledger. Who can access the system is decided by the enterprise's record and compliance policy. The owner mandates that users engage in a two-way exchange of shared keys based on the widely-used Diffie-Hellman Algorithm in order for data to be sent (Kish et al., 2015). To examine and amend policies, the most recent block, which contains the most modified policies, would be utilised. In contrast to Bitcoin, where transactions are aggregated and mined into blocks, each block in this system is mined independently and added to BC without proof-of-work or any other puzzles that could increase the associated overhead. The miner links the headers of the two blocks and copies the policy from the older block into the newer block. One last thing that sets Bitcoin apart is that all transactions are lawful as long as they are in a block.

1.4.1.4. Business Data Storage Platform

Although it adds to the corporate budget, optional local storage for central data holding allows organisations to be more agile and sensitive with data operations. It could be an attempt to summon a nearby backup.

1.4.1.5 Smart Contracts

By forming agreements on any Internet of Things (IoT) device, smart contracts make it possible to enforce them when certain prerequisites are met. Take a shot at defining the upper and lower limits of specific critical situations for your staff. In the event that the wearable system takes a reading that is outside of the specified range, the smart contract can notify the appropriate party or enterprise infrastructure and store the questionable data in the cloud. This way, the organisation can access the patient's vital signs at a later time if needed.

1.4.2. PROVIDE SERVICES VIA THE CLOUD

Instead of storing healthcare data from IoT devices on the blockchain, this company is utilising cloud computing servers to store personnel information. In some cases, employees of a company may prefer to have their data stored in the cloud, which opens the door for a third-party supplier to offer smart services like these. Information is processed in discrete numbered blocks when creating an account for cloud storage. One way to authenticate on the device is by using block numbers and the hash of the stored data. Once data is found with a defined block number and hash value, the consumer is granted access to the device. Blocks containing user data packets are organised in a First-In, First-Out fashion, with the data hash kept in each. After all the necessary data has been recorded in the blockchain, the shared key from a simplified Diffie-Hellman cypher that is applicable to that particular block number is used to encrypt the new block number. One reason there is only one keyholder is that it makes it impossible for anybody else to deduce the block number. Hashes prevent data collisions because no one other than the user knows the block number; so, no one else can access the data stored in that ledger. The concept that users can choose to construct individual ledgers for their various devices or a central shared ledger for all of them is also worth noting. If one wishes to see all the data stored on a specific device, the former is the better option. The reason these forecasts are associated with advanced networks is that whenever data is saved, the hash of the data is sent to the network by a cloud processor. When applied to data stored in a single or digital file, the algorithm generates a hash value based on Merkle's Tree. A new chain hash is generated when the superlative network applies a new hash to the previous hash value, provided that it recognises the current block's root hash. We could control how the outcomes are improved in such a scenario, so we wouldn't have to rely on third-party confidence.

1.4.3. SUPERLATIVE NETWORK

The decentralised architecture of Bitcoin is similar to that of a mesh network. A server, mobile phone, tablet, or any other system hooked up to the Internet of Things (IoT) could be one of the linked devices standing in for a node. According to the suggested paradigm, a certificate is required to prove the validity or authenticity of each node in a network. In order for a user to create an account on the network, the authentication certificate needs to be submitted to the framework. The network can digitally sign the data or transaction once it has been issued permission. We partition each node into multiple smaller networks, each headed by a cluster head, to increase network speed and minimise transmission delays. If a node is experiencing latency, it might switch to a different cluster. On top of that, consent is not required for nodes in the cluster to choose a new CH. In order to verify the membership of other nodes in the cluster and determine which nodes have access to the network's information, each cluster head has its own unique set of public keys. If your blockchain just contains hashes and each block reuses the hash from the previous block, then you should treat it the same way as a blockchain.

The superlative network houses a blockchain that all CHs contribute to. CHs in the cloud network send multisig transactions, and CHs in the superlative network send control transactions. Unlike Bitcoin mining, CHs use their interactions with the transaction's participants to decide whether to create a new block. A typical miner is selected for this mutual superlative, and there are diverse varieties of BC in each CH. Every channel starts with a transaction that is directly linked to the parent channel's initial transaction. This causes forking in shared BC, which is different from Bitcoin BC where it is forbidden because to the double effect on spending. Upon implementation of a decentralised blockchain, the high-resource devices within a participating organisation would retain the link between the block number and hash to the specifics of the most recent transaction.

1.5 PHASE IN THE PROPOSED MODEL FOR BLOCKCHAIN TRANSACTIONS

Specifically, BC transactions entail three stages: storage, access, and monitoring. Once enterprise personnel enter the office through the buffer zone, all offline data is passed over to the enterprise BC network. The enterprise buffer miner checks if there is storage available in the enterprise storage. Then, the enterprise BC goes through a policy check using a policy header, and the buffer miner approves it at the enterprise level. This is all part of the storage phase. Next, after the IDs are generated, the data storage request and chain linkage to the preceding block request are sent to the cloud storage once they are granted. Now the data is hashed and sent to the superior network via the cloud storage; if everything went well, the network returned an ACK signal and the generators of the block numbers were passed on to the corporate buffer miner. Businesses must use the enterprise blockchain to record future transactions. It is possible for the service provider to gain access to the data using enterprise BC during the access phase by sending a multi-sig transaction to the enterprise buffer miner along with the handover data. Afterwards, the enterprise buffer miner will seek access to the data from the business blockchain. Next, the business blockchain verifies the policy's existence in the policy header and, if found, notifies the buffer miner of their approval. Thus, the business buffer miner updates the cloud storage with the chain update, the current block number, and its hash. Accessing the data from the cloud storage can be done via a buffer miner when needed later on. In addition to this, the enterprise blockchain provides buffer miners with access to transactions that require multiple signatures. While tracking progress, the service requester can initiate data access by contacting the enterprise buffer miner, which will then notify the enterprise blockchain. For this purpose, the enterprise blockchain uses policy headers to verify policies; if policies are accepted, enterprise personnel's statuses are updated accordingly. After that, business staff pass the information to the buffer miner, which can then ask the business BC to save the deal.

Fig. 1.2 illustrates the several steps involved in the aforementioned procedure during the blockchain transaction.

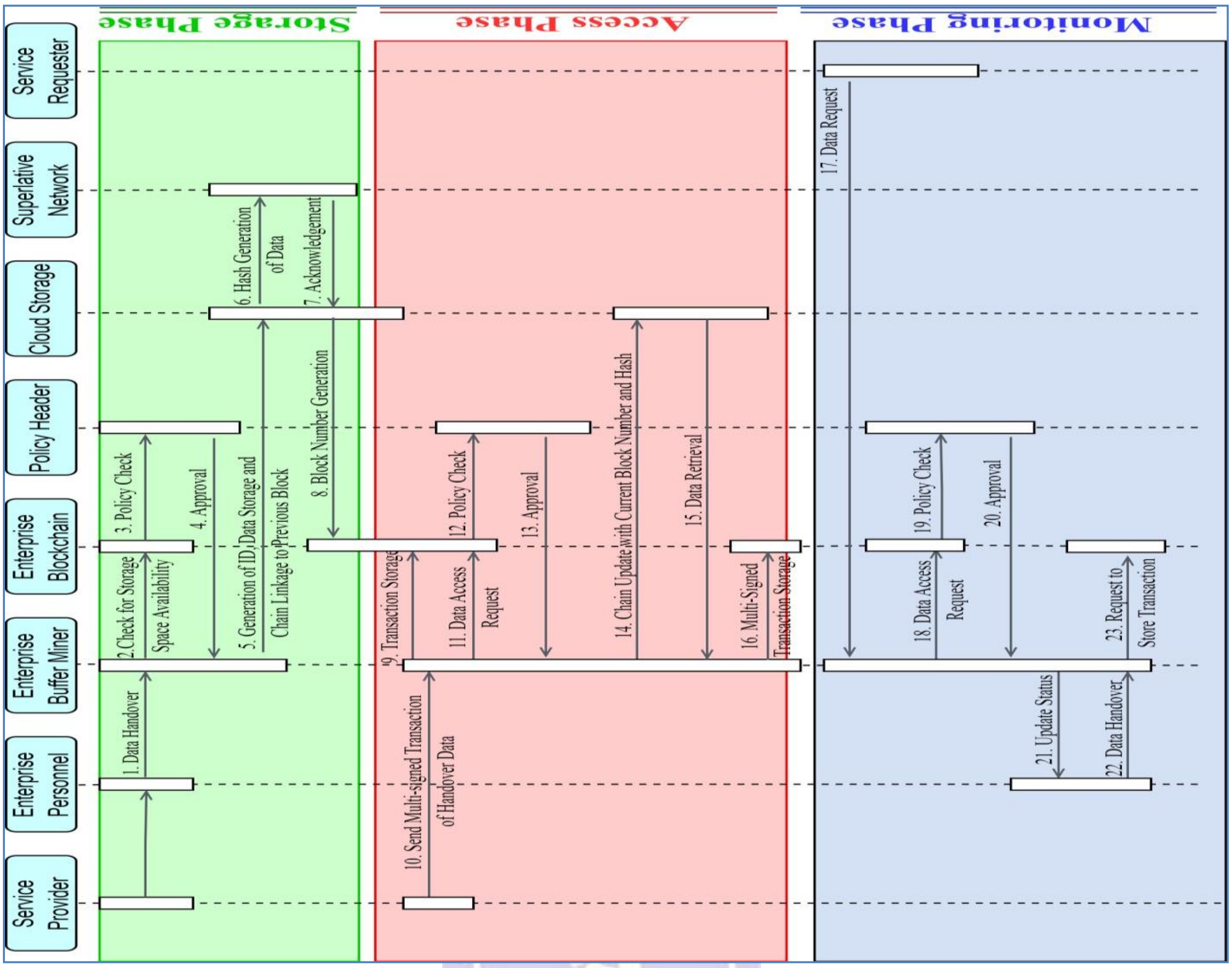

Fig. 1.2 Phases of Blockchain Transactions

1.6 EVALUATING PERFORMANCE

The results in a simulated setting allow us to assess how well our method works. The suggested solution is put through its paces using a business blockchain that is constructed on Hyperledger Calliper. This is accomplished using Docker Composer V1.130, Docker Engine 18.06-ce, with a node description indicating V8.11.4. Figure 1.3 displays the average, minimum, and maximum latency for beginning a transaction and running the query function in the suggested system with 500 employees across 10 corporate networks. The next step was to put the exceptional network through its paces using NS3, which was built on the Solidity blockchain. This was done in a VirtualBox virtual machine with two CPUs and 4 GB of RAM, while the host system had an Intel i5@2.5Ghz processor and 8 GB of RAM. Overhead packets in a superb network with several cluster heads are illustrated in Fig. 1.4.

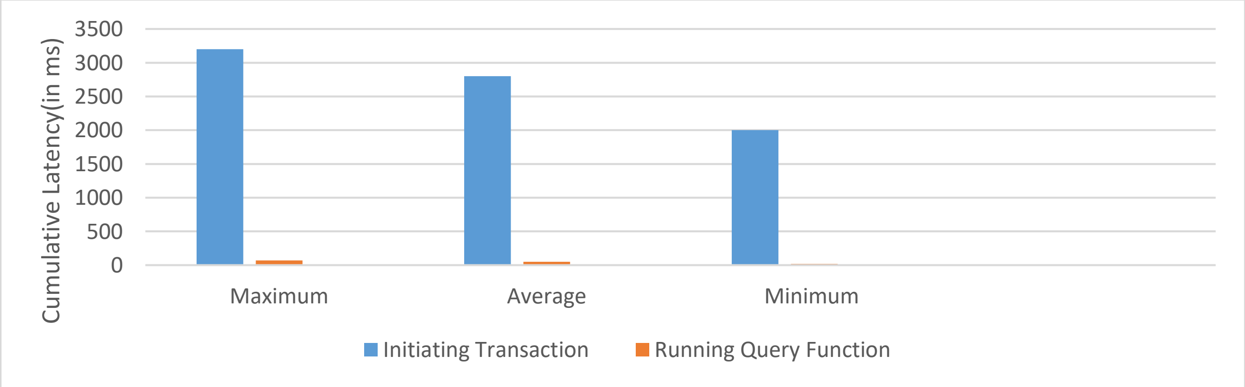

Fig. 1.3 Cumulative Latency during Transaction Flows

In the worst-case scenario, the time complexity for trust establishment and mining can be expressed as O(n) for packet overhead, O(n/t) for transaction delay and computation overhead, and O(b) for storage overhead. Here, n is the number of clusters, t is the level of trust, b is the size of the block, h is the hop count, s is the block size for each blockchain, and tx is the number of transactions in each block. In contrast, the storage and packet overhead for a new miner's network enrollment is size-dependent. On the other hand, the processing overhead and transaction latency are proportional to the blockchain's block count and transaction volume. We may thus express the worst-case temporal complexity for the first two as O(b) and for the second two as O(s.tx).

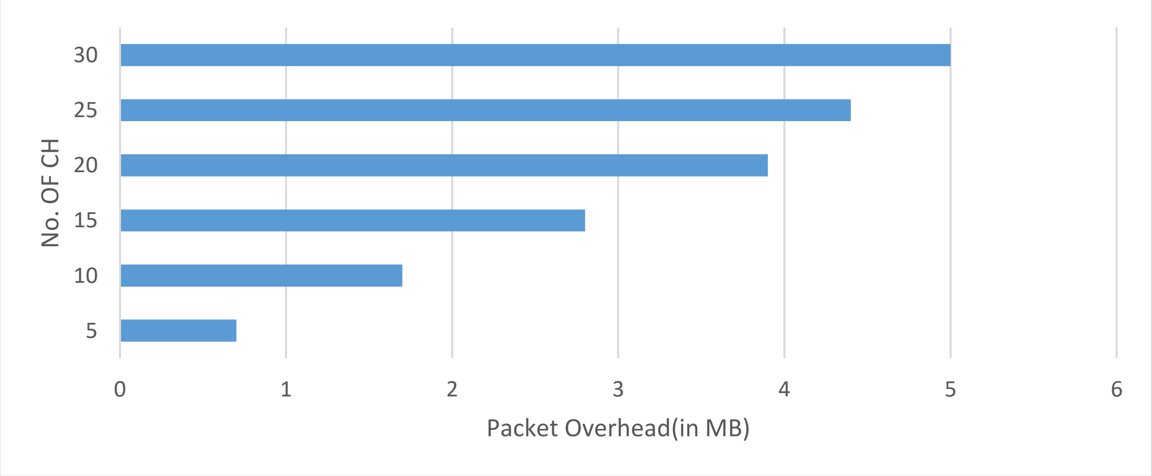

Fig. 1.4 Superlative Network Performance in Terms of Packet Overhead and Number of ClusterHeads

Both local and global network storage have a constant factor, O(1), that represents the worst-case time to store. Nevertheless, it may take O(h) time, where h is the number of hops from the source to the resource in the cloud for storage. Given that the worst-case scenario's access and monitoring times are impacted by factors such as the total number of clusters that may have to be traversed and the number of hops that must be covered, as well as transaction delays and packet overhead, considering it as O(n.h), the overhead associated with storage stays the same. On the other hand, the computational overhead is more cluster-specific. So, O(1) and O(n) are two ways to express them.

1.7 DISCUSSION

Keeping people healthy is everyone's first priority, especially with the world's attention focused on COVID-19. Supporting appropriate healthcare and monitoring IoT devices, there have been substantial progress efforts. To combat serious security breaches, current Internet of Things (IoT) device capabilities are inadequate (Gupta et al., 2020). These issues develop as a result of inadequate hardware and software designs, outdated standards, and limited resources in IoT devices. This article proposes using blockchain technology to secure the billions of Internet of Things devices that will soon be available to healthcare professionals and patients, enabling them to provide open, valued, and secure health support. Many parts of our society and economy will be affected by the Internet of Things (IoT) change if we are able to meet its lofty ambitions. Taking into account the resource constraints of many IoT devices, the suggested model is a blockchain-based Internet of Things framework that handles the most important privacy and risk issues. This design is applicable to the majority of Internet of Things topologies in multi-stage networks; nonetheless, it is mostly used for remote health monitoring and tracking. The proposed method might be tested for interoperability with other frameworks in the future, in addition to current IoT frameworks.

1.8 CONCLUSION

For human tracking enabled by the internet of things, this paper suggested a lightweight security framework. This was an investigation of potential scenarios involving a pandemic, such as COVID-19. First and foremost, the issues were addressed in this paper. Enterprise, cloud computing, and superlative layers make up the proposed framework paradigm, which is based on these challenges. Next, we'll go over the steps involved in conducting blockchain transactions using this proposed framework model. After that, we'll assess how well it worked and talk about our findings.

REFERENCES

1. Smith, J., & Patel, A. (2020). "Internet of Things and COVID-19: A Review of Applications and Challenges." Journal of Health Informatics Research, 4(2), 112-125.
2. Gupta, S., & Sharma, R. (2021). "Security Challenges in IoT-Based Healthcare Systems: A Comprehensive Review." Journal of Information Security Research, 9(1), 45-62.
3. Verma, R., & Mishra, P. (2020). "Privacy and Security Concerns in IoT-Based Contact Tracing for COVID-19." Journal of Cybersecurity and Privacy, 1(3), 217-230.
4. Mishra, S., & Patel, N. (2019). "Security Frameworks for IoT-Based Healthcare Applications: A Case Study of Human Tracking in Pandemics." In Proceedings of the International Conference on Internet of Things (IoT) (pp. 176-183).
5. Gupta, P., & Singh, M. (2019). "A Lightweight Security Framework for Human Tracking in IoT Applications." In Proceedings of the International Conference on Emerging Technologies (ICET) (pp. 123-129).
6. Sharma, A., & Gupta, R. (2021). "A Lightweight Security Framework for IoT-Based Human Tracking during Pandemics." International Journal of Advanced Computer Science and Applications, 12(4), 280-289.
7. Patel, N., & Shah, P. (2020). "Security and Privacy Challenges in IoT-Based Healthcare Systems: A Case Study of COVID-19 Tracking." Journal of Information Security and Applications, 58, 102635.
8. Agarwal, R., & Jain, P. (2021). "A Survey on IoT-Based Technologies for COVID-19 Monitoring and Management." Journal of Ambient Intelligence and Humanized Computing, 12(8), 9647-9666.
9. Kumar, V., & Verma, N. (2020). "Role of IoT in Pandemics: A Comprehensive Study on COVID-19." Journal of Medical Systems, 44(9), 156.