Journal of Intelligent Systems and Internet of Things
Vol. 17, No. 01, PP. 159-176, 2025
DOI: https://doi.org/10.54216/JISIoT.170112

Cloud Enabled Blockchain and IoT Integrated Assisted Living System Supporting Quality of Life and Privacy in 6G Networks

Mohanaprakash T. A.[1,*], Nagalingam Mythili[2], V. Pandarinathan[3], Santhi Karuppiah[4]
R. Saravanan[5], P. Sangeetha[6]

[1]Department of Computer Science and Engineering, R.M.K Engineering College, Kavarapettai, India

[2]Department of Computer Science and Engineering, St.Joseph's Institute of Technology, OMR, Chennai, Tamilnadu, India

[3]Department of Computer Science and Engineering, Mohamed Sathak A.J. College of Engineering,Siruseri, Chennai - 603103, India

[4]Department of Computer Science and Engineering, Vel Tech High Tech Dr Rangarajan Dr Sakunthala Engineering College, Avadi, Chennai- 600062 Tamilnadu, India

[5]Department CSE, Rajalakshmi Institue of Technology, Chennai, TamilNadu, India

[6]Department of Physics, Panimalar Engineering College, Chennai, India

Emails: tamohanaprakash@gmail.com; mythilin@stjosephstechnology.ac.in; v.pandarinathan@gmail.com; sarasanthi.k@velhightech.com; 24071970@gmail.com; chandran.sange@gmail.com

Abstract

Due to emerging disruptive technologies, the Internet of Things (IoT) is essential in innovative living domains, such as elderly and disabled healthcare services, home security and safety monitoring, and computerization control services. The IoT can improve inhabitants' quality of life and the quality of life of smart ambient assisted living (AAL) environment users. The sixth (6G) network will enable a completely linked world with terrestrial wireless communications. Blockchain-based approaches offer decentralized privacy and security, yet they include vital delay, computational, and energy overhead inappropriate for most resource-reserved IoT devices. Hence, this study proposes a Blockchain and IoT-based Assisted Living System (BIoT-ALS) using 6G communication. The nodes in our proposed paradigm use smart contracts to specify norms of interaction while working together to provide storage and computing resources. Our suggested approach has encouraged confidence-free interaction and boosted user privacy through the blockchain approach. This paper aims to explain the sensor layer, a distributed signal processing system in vast, physically connected, wirelessly networked, and energy-restricted networks of sensor items. A comprehensive experimental test series shows each sensor type's accuracy and probable usage. The numerical results show that the suggested BIoT-ALS model improves the performance ratio of 99.1%, accuracy ratio of 98.8%, reliability ratio of 94.8%, an efficiency ratio of 93.6%, the throughput rate of 97.6%, and reduces the network delay of 19.2%, latency ratio 10.2%, and execution time of 20.4% compared to other popular models.

Received: January 31, 2025 Revised: February 28, 2025 Accepted: April 12, 2025

Keywords: Assisted Living; Internet of Things; Blockchain Technology; 6G; Smart Home

1. Introduction

The ageing population has recently increased, and older people's health and medical concerns have become major social difficulties [1]. As the major priority of the elderly is to monitor and preserve their health, it makes their life easier to avoid and resolve health problems [2]. Due to their physical limitations, older folks spend

considerable time indoors rather than outdoors [3]. With increasing indoor activities, research on the intelligent house has become important, providing health information monitoring, crime prevention, and elder safety services [4]. The IoT is formed from the notion that devices, objects, and devices like computers, sensors, or mobile phones may be connected, worked together, and operated together efficiently to fulfil various tasks internationally [5]. IoT includes essential network components like computers and smartphones, vulnerable components such as sensors and RFID tags, and other technology [6]. Because of this, networking is the major difficulty in IoT, which is concerned with integrating heterogeneous massive network elements and achieving effective data transfer [7]. Wireless sensor networks (WSNs) that connect objects and machines are important in gathering environmental and contextual information [8]. The sensor node connects the sensor network wirelessly to a central gateway that links the sensor network to the cable world, where the measured data are collected, processed, analysed, and presented [9]. To govern the WSN configuration that spans several tasks, WSNs form the base of smart home and ambient living applications [10]. These tasks, such as managing scalable network structures and automatic healing capabilities by identifying and removing incorrect nodes or controlling their configuration, must be managed effectively to improve the situation [11]. Therefore, effective smart home and environmental support applications tested in the natural environment must be developed and designed [12]. First, 6G will be an independent network to get people into a new paradigm that centres on humans and machinery. 6G will offer many means of interacting with end devices, including neural impulses, the eyes, fingers, etc [13]. Thirdly, 6G may have higher reliability, robustness, and efficiency criteria to progress from network software to intelligence [14]. Big Data Analysis, which may enhance the service quality and optimize situational sensitization of 6G networks, is one of the main activities of all these applications [15]. First, users may explore past data for network performance insight, such as traffic assessment and energy efficiency. Secondly, the information obtained may be used to forecast future events, such as access to resources, preferences, and behaviour [16].

Future computing applications can anticipate human demands by incorporating sensors, omnipresent computers, and wireless communication into normal objects [17]. However, the shortage of devices that incorporate the necessary hardware and software makes it challenging to establish ubiquitous computing in these daily objects [18]. In this regard, researchers propose the base for low-power smart objects of a compact computer with wireless connection, sensors, and actuators [19]. Blockchain's distributed nature makes operating independently in a smart home extremely safe. Blockchain has an indisputable public record of data secured by peers. Blockchain sanctions enhance efficient and expedited communication without any single failure point with the increase of the 6G network and edge devices [20].

Smart contracts play an essential part in automating critical operations. According to the Health Monitoring and Alert Contract, healthcare providers are notified when patient health data from IoT devices go above acceptable limits. By regularly checking in with patients and their caregivers, the Medication Management Contract ensures they take their medications as prescribed and follow their treatment plans. Protecting private patient information and guaranteeing compliance with privacy requirements, the Access Control Contract also limits data access to approved individuals exclusively. In a 6G-enabled setting, these contracts maximize patient care, increase data privacy, and increase automation.

Blockchain technology compatible with 6G networks improves processing speed, security, and connection. It ensures immediate responses from health monitoring devices by providing very low latency (as little as 1 millisecond) for real-time data transfer from IoT devices. It can analyze enormous quantities of health data effectively because of its high throughput, which can handle gigabits per second. Designed specifically for assisted living facilities, the design enables massive connectivity, supporting as many as one million devices per square kilometre. It promotes interoperability between applications for healthcare and Internet of Things devices and enhances privacy and security with robust encryption and decentralized storage. Overall, this 6G-enabled blockchain improves living conditions by establishing a trustworthy and effective network of technologies for assisted living environments.

Since blockchain technology is decentralized, it establishes the resilience and scalability of using node resources and removes multi-to-one traffic. It reduces the time to overcome the failure of a single point. Distributed blockchain technology enables new use cases of household device diagnostics, energy savings, and damage protection in natural disasters. IoT is recommended as a crucial component of Ambient Assisted Living (AAL) to improve the well-being, safety, and health of millions of older persons globally because of the nature of its connective power and its sensory capabilities. Therefore, vital statistics on health may be made available by continuously obtaining data that assist longevity from the body and surroundings. Recognition of activities is essential for various aid technologies, including intelligent home technologies such as Ambient Assisted Living (AAL). AAL aims to help persons affected by their health preserve their freedom for the greatest benefit. However, it is vital to know with a high degree of certainty, which course of action the individual takes to provide significant help. It must be stressed that not all activities have to be known, but those actions that require and welcome assistance are known.

The main contribution of the study is

- Designing the Blockchain and IoT-based Assisted Living System (BIoT-ALS) model for elderly and disabled healthcare services in smart homes.
- Evaluating the mathematical model for assisted living using IoT and Blockchain with 6G communication.
- The numerical outcomes have been performed, the proposed BIoT-ALS model enhances the efficiency, reliability, and performance and reduces the delay, latency, and execution time compared to other existing models.

The rest of the paper is arranged: Section 1 discusses the introduction, and Section 2 discusses the existing systems. In section 3, the proposed BIoT-ALS model has been deliberated. In section 4, the numerical outcomes have been executed. Finally, section 5 concludes the research article.

2. Literature Study on Assisted Living in Smart Home

Weixian Li et al. [21] recommended the Smart Energy Theft System (SETS) for IoT-based smart homes. The first step is the predictive model, which employs multi-mode prediction systems. There are 3 phases of decision-making modules. This system blends several machine-learning models into one predictive power consumption prediction system. The second phase is the principal decision-making mechanism, which employs an abnormally filtered Simple Moving Average (SMA). The second phase of choice on energy voles is the secondary decision model.

Alexandre Bissoli et al. [22] suggested the Human–Machine Interface Based on Eye Tracking for Controlling and Monitoring system (HMI-ETCMS) for smart homes using IoT. The technology enabled a person with a serious disability to manage daily devices such as light, TV, fan, and radio in their home. Moreover, her caregiver may monitor her device usage in real-time over the Internet on a distant basis. The here-built user interface contains several features that improve the system's usability. All participants responded to a questionnaire on the system usability scale (SUS), showing that the group assessed the assisting system with a mean value of 89.9% and 92.5% without impairments and those with serious disabilities.

Mohammed Alshahrani and Issa Traore [23] discussed the Cumulative Keyed-hash chain (CKHC) mechanism for automated access control and secure mutual authentication for IoT smart homes. CKHC mechanisms are developed to confirm the sender's identity (through challenge-response). Furthermore, we leverage fog computing to strengthen the assurance of identification. Finally, the Automated Validation of Internet Security Protocols and Applications (AVISPA) and the Burrows-Abadi-Needham (BAN) logic toolbox provide an official assessment and prove the safety of our protocol.

Prankit Gupta et al. [24] deliberated the kernel density estimation (KDE) to discover patterns in unlabelled sensor information in the smart home. KDE is used to pre-process the information and t-distributed stochastic neighbour embedding and uniform various approximations and projections for visualizing changes. This study shows that an adaptive segmentation methodology, KDE, is an appropriate option to find a temporal cluster of unlabelled sensor events that potentially signify an activity. It is shown that the data may be mapped for several days of the week to visualize and modify distinct repeated patterns of activity. The article then shows how trends may be tracked across more extended periods, which might assist in identifying variations in the daily behaviour of the user.

Sudipto Bhattacharyya et al. [25] proposed a Blockchain in Hybrid Cloud Communication System for IoT-Enabled Intelligent and Secure Manufacturing Model. IoT-Enabled Intelligent and Secure Manufacturing ModelThe proposed swarm-based approach evaluates the health of the sensor nodes. To decrease communication overhead and latency for Internet of Things (IoT) components in a hybrid cloud system, a resource scheduling technique based on deep neural networks (DNN-RSM) has been developed. All requests from the cluster head are classified using DNN according to their processing, storage, and bandwidth requirements for optimal resource allocation. The proposed structure produces superior energy consumption, latency, and safety results. The simulation's findings support that the suggested approach is better than the existing one. Strict safety measures, less power consumption, less delay, and effective use of resources are all part of the proposed strategy.

Rajawat et al. [26] suggested a Blockchain Technology for Cloud-Enabled e-banking Payment Security Implementation. Based on the survey, there are several problems in implementing an efficient assisted living environment. Hence, in this paper, the BIoT-ALS model has been proposed to overcome the existing challenges. The following section briefly discusses the BIoT-ALS model. This article introduces a novel approach to

enhancing the safety of online banking transactions by integrating blockchain and cloud computing. The system's intended use case is hosting business apps and services in the cloud, using blockchain technology for the safe recording and verification of transactions. Smart contracts simplify payment and transaction management by facilitating trust and transparency in financial transactions. Encryption technology further protects private data and the user's identity. This technology's several advantages are that it makes electronic banking more secure, transparent, and efficient. Research papers and experimental findings show the practicality and efficacy of the suggested method. Security concerns and the unreliability of online payments may be addressed by combining blockchain technology with cloud banking.

Yurong Luo et al. [27] presented a hierarchical secure data-sharing platform empowered by cloud-fog integration. The author suggests a novel protocol for group authentication and key agreement that does not involve interaction and is based on zero-knowledge proofs. This protocol may facilitate the one-to-many exchange of collections of IoT data, particularly SG data. Results from the security formal verification tool confirm that the suggested method can accomplish both ends of the authentication process, secure data exchange and mutual authentication, while keeping data providers' identities secret. The suggested approach outperforms earlier Internet of Things (IoT) data-sharing schemes in terms of computational and transmission efficiency, and its benefits grow as the amount of shared data or the number of users increases.

Abdullah Ayub Khan et al. [28] investigated a Hyperledger Sawtooth that provides a secure cloud forensics chain-of-custody investigation architecture. Malicious attacks are becoming more common across the cloud computing lifecycle as more users share, access, manipulate, scale, and reuse data storage. A major challenge is offering a trustworthy, reliable, secret, and secure platform in a cloud forensics setting. Members of a forensics team that want to collaborate and digitally sign off on various components of an investigation could establish a private block-based ledger network. In contrast, a chain of custody transaction may be automated using chain codes. This article bridges the gap using blockchain technology by facilitating innovative, trustworthy, and open cloud forensics chain-of-custody research procedures.

Hongliang Tian and Junyuan Tian [29] deliberated a Blockchain-Based Access Control Scheme for Reputation Value Attributes of the Internet of Things. Potential risks associated with the IoT access control method include data manipulation and single-point-of-failure environments. To tackle these problems, we provide an Internet of Things (IoT) reputation value attribute access control mechanism based on the blockchain. To begin with, by including the reputation value as an attribute in the access control policy and then implementing the policy in the blockchain system's smart contract, the system may provide more granular access control. Second, it increases system performance by storing extensive IoT resources in the Inter Planetary File System (IPFS). Link resource access activities to qualification credentials to enhance the access control system's performance.

Rayan Anwar Abutaleb et al. [30] proposed an Integrity and Privacy-Aware, Patient-Centric Health Record Access Control Framework Using a Blockchain. Modern technology has the potential to revolutionize healthcare and other data-driven businesses. Because of both external and internal assaults by healthcare workers, patient privacy has grown increasingly susceptible to electronic healthcare services, even if they have made treatment easier and more accessible. As a result, we set out to create a system for managing patients' medical information that would allow them to elect which individuals had access to their data. This system will document all actions using blockchain technology and use control. An efficient and placable blockchain operating system was selected after conducting trials and reviewing the literature. Finally, the results of the performance test proved that the operating system and smart contracts function at a satisfactory pace.

Based on the survey, there are several issues with existing models in attaining high efficiency, reliability, and performance, reducing the delay, latency, and execution time. Hence, this study proposes a Blockchain and IoT-based Assisted Living System (BIoT-ALS) using 6G communication.

3. Blockchain and IoT-based Assisted Living Systems (BIoT-ALS)

This study proposed the BIoT-ALS model for elderly and disabled healthcare services in a smart home using 6G communication. Assisted living provides personal and medical help to persons (typically older adults) while prioritizing mobility. Those needing assistance receive services ranging from personal care and skilled nursing to senior housing. As an expanding field of applications incorporating several technologies, IoT and intelligent homes combine to smartly control the current home environment by incorporating different intelligent chips into home equipment. A smart home system is a typical omnipresent computer environment, and numerous challenges

must be overcome. The system, sensor, and service differentiate the environment. Smart Homes with a tracking system are open to security susceptibilities because of the network interrelation of diverse structures. Based on the system, the AAL market is sub-segmented into security and safety systems, communication systems, power management systems, medical support systems, transportation, entertainment, communication systems, etc. This paper clarifies the blockchain models applied in smart home networks to manage device transactions using 6G communication. Blockchain technology improves smart home security by utilizing the data log passed from one house to another and eliminating miscommunication. Blockchain is a decentralized network that allows all participants to transact in a reliable network. The blockchain features a distributed leader with connected transaction blocks for all network participants. Home automation's security and privacy challenges may be solved with blockchain technology.

For instance, older people could fall on the floor or become aware on a sofa. The device should react promptly, or the caregiver should receive an alarm from them. Therefore, human conduct abnormalities in such support systems are particularly desired. However, typical behavioural anomaly detection techniques rely on the robot or ambient sensors to provide a visual sensor. Solutions based on vision normally include substantial calculation costs, whereas environmental sensors have considerable maintenance costs. These systems use several sensors to track the characteristics of everyday life activities using different AAL-orientated sensors. A wide range of features may include home automation and control (for example, interfacing with home lighting or heating systems), security, mobility assistance and compensation, computational monitoring, etc. Sensors may be supported and controlled at home. Home devices may be connected to the Internet to provide remote surveillance, maintenance, and communication services. Therefore, the "intelligence," one or more home processing units, and optionally, external cloud services are spread amongst the sensing unit ("smart" things themselves). The sensors are distributed in various locations throughout the rooms.

The sensor's location concerning the location of the possible fire (i.e., the sensor's contiguity to the fire) is a significant feature when making a precise choice. The data manager recorded data from individual sensor modules, stamped dates, and recorded the acquired data continually. Networks for sensors and actuators (SANETs) contain nodes for sensors and actuators that conduct distributed sensing and actuating operations. A study of sensors related to mobilize nodes will be presented in this section. Finally, a sensor has been picked for each size. Technical or commercial concerns influence the reason for the choice. As for the actuator, certain actuator nodes are spread throughout the furniture, as mentioned in this section.

To ensure data security in IoT contexts, blockchain technology uses consensus algorithms like Proof of Authority (PoA) or Proof of Stake (PoS) to verify transactions quickly and with little energy. Implementing smart contracts in this blockchain architecture automates care activities and guarantees that only authorized individuals can access sensitive data, effectively securing it. To allow real-time monitoring and response, network protocols, especially 6G protocols that are lightweight and designed for the IoT, enable devices to exchange data quickly and with minimal delay. To further improve system efficiency, IoT integration approaches like device interoperability and edge computing enable data to be processed closer to its source, resulting in reduced reaction times.

The first role is to support and assist users throughout their everyday tasks, and the second is to aid older carers. These Wireless actuator knots have a twofold function. The user's temperature is of great relevance to measuring. The AAL system can identify abnormal temperature models and, when needed, produce particular warnings by using user temperature data. Moisture sensor incorporation permits the detection of liquid leaks on the bed or sofa. Even though some viable humidity sensors have some difficulties, some difficulties in integrating such sensors into furniture structures. Older adults spend adequate time lying or sitting on furniture, and many of them are overweight or, at least, require their weight to be tracked. They are incorporating weight sensors in furniture to control the user's weight without hassle. These kinds of sensors are integrated into armchairs and beds. Some weight sensors are commercially available, like the widespread load cells or Flexiforce sensor.

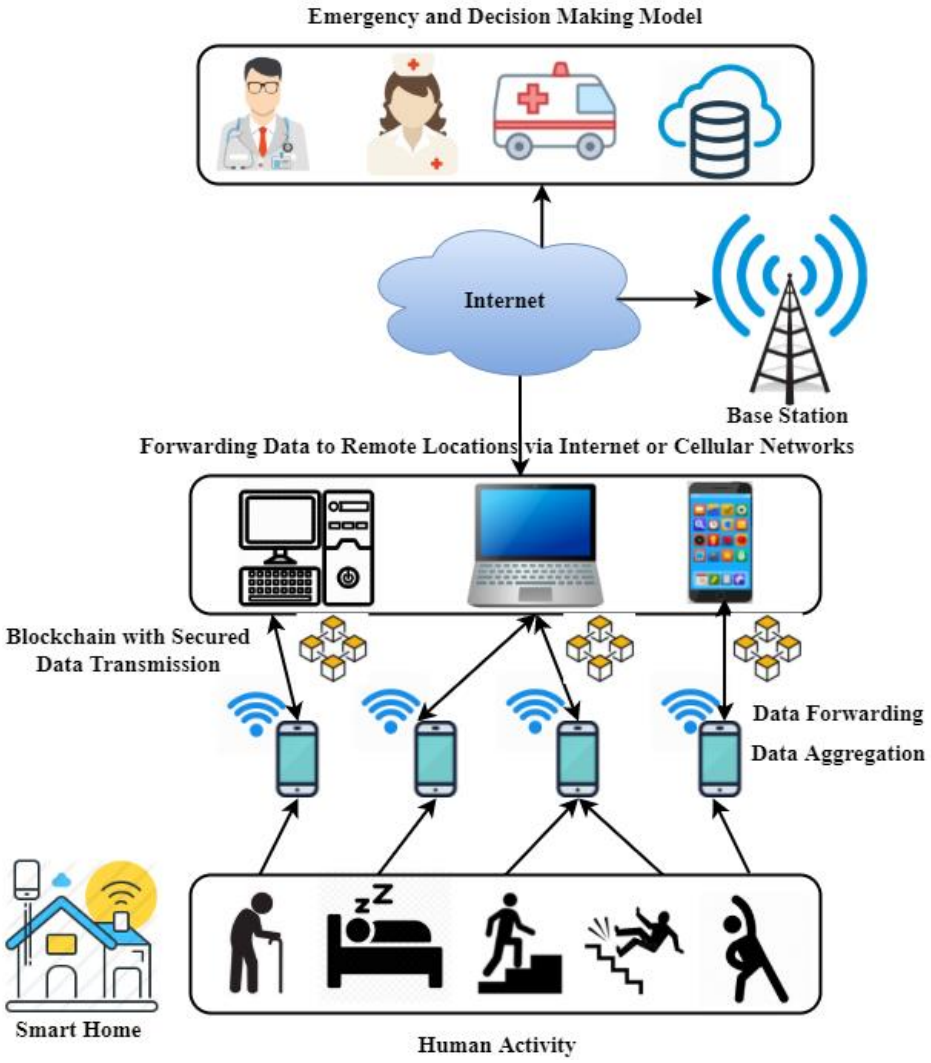

Figure 1. Proposed BIoT-ALS

Figure 1 shows the proposed BIoT-ALS model. The life expectancy of humans has risen as medical science progresses, leading to a rising number of elders in society. Aged persons are more sensitive to chronic illnesses that need regular well-being monitoring. Regrettably, healthcare is becoming more costly than other daily needs. Thus, individuals at home prefer to depend upon automated devices that regularly check health indicators. However, these automated systems, based on sensor devices worn or fixed inside the body, are cost-effective compared to traditional treatments to identify physical problems. This tendency has now become an incentive for study in the field of AAL. A heterogeneous implantable/wearable and environmental sensors network spreads throughout the site and can record, monitor, and even identify occurrences regularly. The Body Area Network (BAN), a similar AAL technology, has many mobile sensors inside a human body, either worn or implanted, that monitor a person's health, such as blood sugar, body temperature, blood pressure, heartbeat, behavioural rhythms, and other physical activity. The data may be promptly transmitted to the appropriate medical centre if a critical deviation from normal may be recognized without human involvement via wireless transmission. This information should be collected and sent to a BAN coordinator (BANC).

In the following level, the BANC distributes the data directly or indirectly via the forwarder node to the sinks, mobile devices, display coordinators, or other devices. Finally, these sinks transfer data to hospitals or nursing centres for further study. BAN and sinks are part of an AAL system. Since the sensor node is battery power-dependent and cannot readily be substituted, energy is the key resource. Thus, methods should be conceived for minimal energy use for such networks.

Furthermore, AAL systems must address other issues, such as channel interference, quality of service (QoS), and user mobility. In response to all these problems, critical health information is reliably sent through relay nodes. The BANC transmits the AAL routing data from the sink. For example, energy efficiency, multiple BAN

interference, and node mobility are frequent challenges that must be addressed. Body sensors may only move during BAN routing due to postural changes; this is termed limited mobility. In numerous networks owned and administered by numerous entities, permanent recordings mean the data may be followed when data transactions occur. Intrinsically transparent are records from Blockchain.

With network connections, you can track and analyse all activities. Organic sensors are connected to the human body to monitor biological factors like blood pressure, heart rate, glucose, body temperature, and perspiration. The actuator picks up the event and sends it as a sink node to the digital band on human wrists. The sink nodes connect via Bluetooth to a smartphone to send the packets. Other sensors or intelligent nodes catch events from older people's daily lives and transfer them through Bluetooth to your smartphone. The Bluetooth connection Smartphone application is receiving. Read packets received from sensors or sinks when Bluetooth is connected and read system time. If the sensor nodes have nothing to perform, they are in low-power sleep mode. Smartphone inserts a timestamp for packets and inserts packets in line with the specifications.

Packages are sent to the nearest physical gateway, enabling homogenous transmission over heterogeneous networks. Intelligent health monitor site transmissions of data packets. A cloud environment is used to improve service cost-effectiveness on a server location. This makes the server site a cloud client for pay-per-usage use of third-party services. Numerous public clouds, like the aged person profile provider cloud, context service provider cloud, and social service provider cloud, provide good service to older people. One application, notably a context management system (CMS), employs a context aggregator to combine every data to produce context models. It can examine the basic patterns of behaviour of elderly persons to detect if an emergency occurs. This application includes sensor data and the senior positions on X, Y, and Z coordinates, its presence in the mapped area (within the smart home), and its actual activity to decide the event's relevance. The decision for the context model is directed to the health monitor's website. If an emergency happens, the health officer will be alerted to respond immediately. The caution is directed towards the older person in minor incidents. Other health workers can frequently utilize biometric authentication-enabled user interfaces to access patient data according to their right to access routine check-ups.

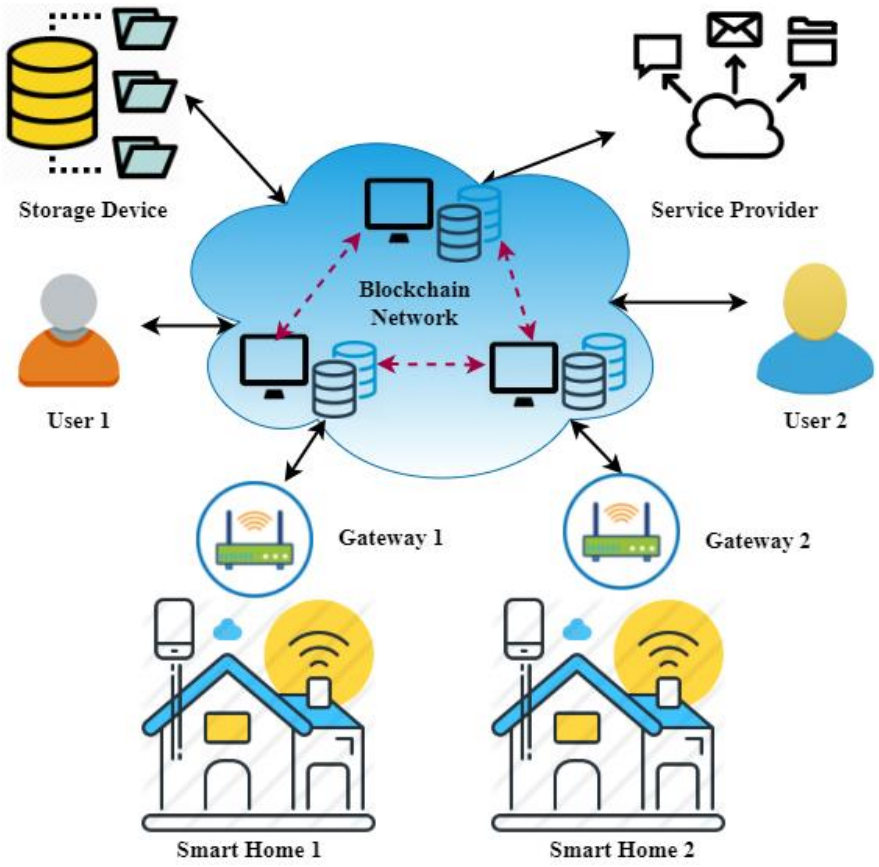

Figure 2. IoT-Blockchain for Smart Home

Figure 2 shows the IoT and blockchain for the smart home. In the smart home, IoT devices usually comprise sensors, switches, actuators, and light bulbs. It is hard to accommodate blockchain technologies that demand a high capacity and many IoT providers, as well as heterogeneity, battery life, and low computational power supplies for IoT devices. The service provider is a device or a group that may interact with the Internet of Things device and storage device to give consumers service guidelines. Sets of storage devices that can store the data from the IoT devices acquired. The user has a system that enables users to enjoy the advice supplied by service providers and receive data from or upload data to their storage devices via a device (such as laptops or smartphones). A smart house that connects IoT devices and enables users to monitor IoT devices at any time. IoT devices generally have sensors that can sense and convey environmental information to the service provider or consumers because IoT devices cannot be connected directly to blockchain networks at a smart home. Therefore, the IoT gateway connects the smart home to blockchain networks. Every IoT portal brings together a group of IoT devices through short-term communication technology, such as Wifi, to a blockchain network. 6G networks are in the beginning stages and need extensive implementation techniques. Continuous data transmission from wearables and IoT sensors causes the system to create large amounts of data, which increases the need for storage and processing. This may strain resources in the cloud and at the edge. The security advantages of blockchain come with the danger of latency, which might compromise time-sensitive health monitoring, and it is challenging to maintain real-time performance while ensuring data privacy. Additionally, operating costs and sustainability are affected by the energy-intensive nature of blockchain and IoT networks, and it is challenging to integrate varied IoT devices inside a defined protocol to ensure effortless interoperability.

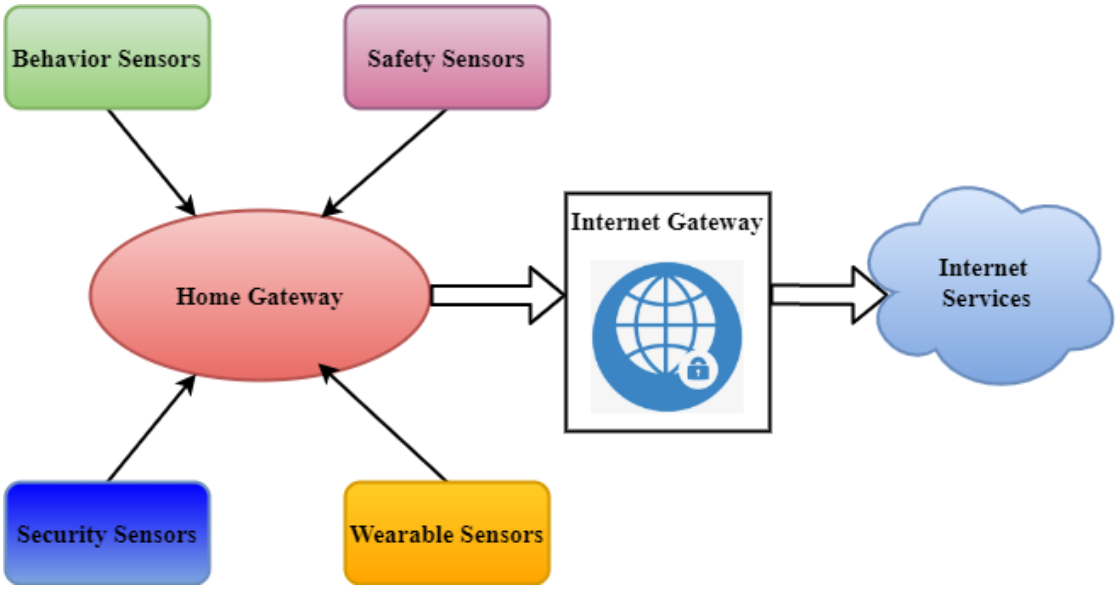

Figure 3. Home sensors system for Ambient Assisted Living application

Figure 3 shows the home sensors system for Ambient Assisted Living applications. A home gateway for the storage, aggregation and processing of sensor information and an Internet connection to cloud-based services employing sensor networks at home is a challenging design development challenge because of the following mentioned issues about non-intrusiveness, usability, and acceptability: Initially, the home sensor systems used proprietary protocols and depended on their communication via wireless technology.

A visitor U with identity ID_U, a smart home administrator with an identity ID_B, and a set of smart devices $C_1, C_2, \dots C_m$ with identities $ID_1, ID_2, \dots ID_m$ are involved in private blockchain-based access control.

Data transmission throughout 6G is affected by intercepted conversations and denial-of-service attacks, and there are security concerns with devices that might allow unwanted access due to inadequate authentication or obsolete software on Internet of Things devices. Furthermore, blockchains are not entirely secure. For example, a 51% attack or significantly designed smart contracts might lead to serious consequences. There is also the possibility of insider threats, in which verified individuals exploit their access to private health information. Effective data security measures, such as end-to-end encryption for data in transit and at rest, and stringent access control mechanisms, such as role-based access and multi-factor authentication, to restrict access to authorized users only, are necessary to reduce the impact of these vulnerabilities. To proactively find and fix vulnerabilities, it is vital to regularly conduct security audits and assessments of blockchain components and IoT devices. While the General

Data Protection Regulation (GDPR) emphasizes their rights over their data by demanding express permission for data processing and the right to be lost in time, HIPAA compliance requires the secure management of all health information to ensure its confidentiality, integrity, and availability. These methods enhance users' privacy and safety in the BIoT-ALS environment, comprising a complete security architecture.

Initialization

For security parameters, the initialization model selects groups H_1, H_2 of prime order q, symmetric encryption algorithm $E_l()$, signcryption algorithm $SC_l()$, and hash function $G:\{0,1\} \rightarrow Z$. In particular, $Para = \{H_1, H_2, q, E_l, SC_l, G\}$.

- B has an administrator-specific key pair (wl_B, ql_B), where $wl_B \in H_1, ql_B \in H_2$, and U has a visitor-specific key pair (wl_U, ql_U), where $wl_U \in H_1, ql_U \in H_2$.
- B shares l_{UB} with U and shares a symmetric key l_j with device ID_j , where $ID_j \in \{ID_1, ID_2, \dots ID_m\}$ then it updates the local QL list and writes access control policies.

Authentication

Stage 1: Usends B request to authenticate the identity and access rights, where r_1 is a random number.

$$req_1 = ID_U \| SC_{wl_u}(ID_U, ID_B, r_1) \quad (1)$$

Stage 2: B inquires about the stored QL list. When U is included in the list, B useswl_B and ID_U to decrypt the signcryption message and check U's identity $ID_U$and r_1 . After checking the freshness of the message, B sends to U to assign a key l_{UD_j} and token T , where $T = E_{lj}\left(l_{UC_j}, ID_U, ID_B, t_1, EC, n_j\right)$ is a token produced by B that is used to access ID_j, t_1 is a timestamp, EC is the expiration date of l_{UD_j}, n_j denotes the device data that the visitor is allowed to access, and $hash_0 = G(ID_U, ID_B)$.

$$assign = SC_{wl_B}\left(l_{UC_j}, ID_U, ID_B, EC, hash_0, t_1, r_1, r_2\right) \vee T \quad (2)$$

Access

Stage 1: U sends the data request to the device ID_j , where t_2 is a timestamp.

$$req_2 = T \| E_{l_{UC}}(ID_U, t_2) \quad (3)$$

Stage 2: C_j decrypts token T with l_j to obtain a shared secret key l_{UC_j} and then recovers the identity of the visitor ID_U . Next, $C_j$sends U and B data package

$$\varphi = E_{l_{UC_j}}\left(ID_j, n_j, t_5\right) \quad (4)$$

As shown in equation (4) where $t_5$is a timestamp.

Blockgen:

Stage 1: After auditing the integrity of mi in, U generates a signature and sends it to where t_2 is the timestamp of requesting device data n_j.

$$sign_1 = sign_{wl_U}\left(ID_U, n_j, t_2\right) \quad (5)$$

Step 2: When U's signature on $n_j$is valid, B generates $N_{ij} = \left(ID_B, ID_U, n_j, t_2, t_4\right)$ and $W_{ij} = sign_{wl_B}\left(ID_B, sign_{wl_U}\left(ID_U, n_j, t_2\right), t_4\right)$, where W_{ij} represents the ordered multiple signatures of U and B found on an access record about n_j, and N_{ij} denotes the collection of all φ in one access, where i denotes that U visits C_j for the $i-th$ time. Then B sends the entire i–block to where $TX_{ij} = \left(W_{ij}, N_{ij}\right)$ and $TX_i = \left\{TX_{i1}, TX_{i2}, \dots, TX_{ij}\right\}$.

$$block_i = TX_i \| sign_{wl_B}(TX_i, hash_{i-1}) \quad (6)$$

Stage 3: After confirming the validity of the block checking and signature, the integrity and authenticity of TX_i, U computes the block signature and sends it to B. U then stores all of the data in the shared private blockchain.

$$sign_2 = sign_{wl_U}(TX_i, hash_{i-1}) \quad (7)$$

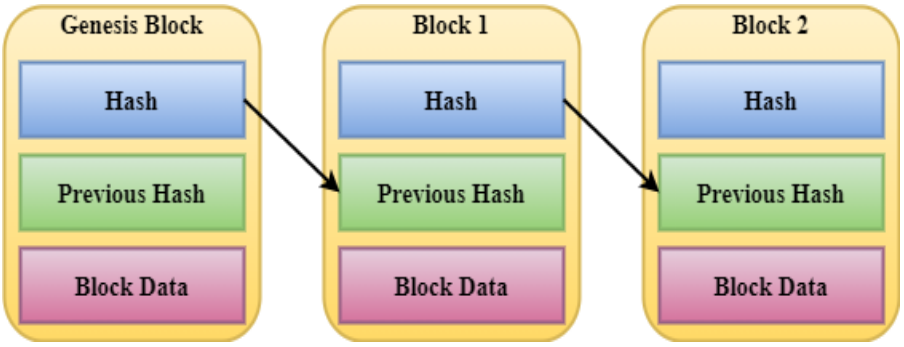

Figure 4. Blockchain Model

Figure 4 shows the blockchain model. A blockchain is an innovative trust less proof mechanism for every transaction on networks. Users can trust the public ledgers stored in universal, decentralized nodes preserved by miner accounts. The blockchain is opposed to establishing and maintaining trust with a third-party intermediary. The public ledger continually grows as miners verify the transaction and add a new block to record the recent transaction. The node in the blockchain means the computer-connected blockchain network using a client to perform the transaction and validation.

Horizontal scalability is integrated into the architecture; cloud resources may be dynamically allocated to handle increasing users and IoT devices. This allows for the effortless incorporation of new devices, such as wearable health monitors, into the system. The system uses a hybrid blockchain method to secure and record sensitive health data on a private ledger and non-sensitive information on a public blockchain. Throughput tests with 1,000 linked devices demonstrated an average reaction time of 200 ms and a throughput of around 500 TPS, with CPU and memory usage remaining below 75%, according to analysis of performance carried out using simulations with NS-3 and IoT simulators. Data from a three-month trial run with fifty users confirmed these hypotheses, with crucial concern reaction times on average falling below 250 ms and user satisfaction rising by 20%. Along with improving user privacy and quality of life, dynamic load-balancing algorithms' ability to successfully control network traffic during peak use confirmed the system's resilience. This makes the system ready for real-world implementation in assisted living conditions.

Each node contains all transactions and addresses from the genesis block, the first blockchain transaction. Each block in the chain included the transaction information and a reference to the previous block. The cryptography that operates into making a block varies depending on which blockchain protocols are employed, and mainly, one can traverse via the whole blockchain to the genesis block. The hashing algorithm ensures the blockchain cannot be tampered with unless the attacker controls over 50% of the blockchain network's mining hash rate. Therefore, the blockchain keeps itself secure and essentially indestructible. Transactions are known as 6G communications between local devices or overlay nodes. The BC smart home has several transactions, each having a distinct purpose. The data-saving devices create the transaction in the store. Service providers or homeowners produce a cloud-based access transaction. The homeowner or service provider generates a monitoring transaction to monitor the information of a device regularly. A smart device is added to the smart home through a Genesis transaction, while a deletion transaction removes a device. A shared key is used to secure communication for the above-specified transactions. Lightweight tampering is used to identify transaction content changes during transmission. The local private BlockChain keeps every transaction to or from the smart home.

A smart home administrator is an online home server with access to numerous resources that manage access control for smart home systems, including maintaining access control policies, authenticating visitor identities, and handling smart devices. Smart devices, restricted by resources, collect data from people in a smart home environment. When visitors have the access token an admin provides, each intelligent device gives visitors the desired information. A visitor requests data from smart devices and these data are used to deliver services to the smart homeowner. The visitor receives smart device data only when he or she has legitimate access rights. However, visitors can access data beyond access rights or forge access records to deceive the smart homeowner. In addition, the visitor maintains the private blockchain that stores requested data and access records.

When visitors serve multiple smart homes, they maintain a private blockchain, which all administrators can access. The word "mining" indicates adding a new block to the blockchain using legitimate nodes on the so-called miner network, nodes in the Ethereum network task. The miner collects in a block and implements consensus on the work consensus technique. The miner continuously supposes random numbers to solve highly complicated encoding problems associated with his block until one winner can publicize the block to authenticate. If the authentication procedure succeeds, additional nodes will add the new block, and the block will be removed.

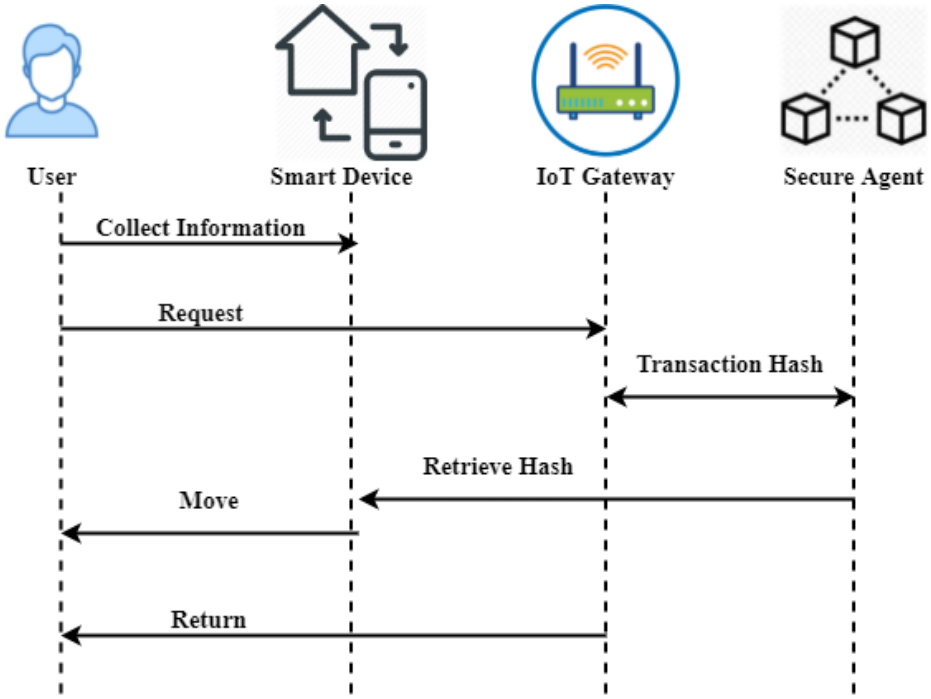

Figure 5. Sequence diagram

Figure 5 shows the sequence diagram. The user measures and collects information from the Temperature Sensor. The user requests that the IoT Gateway migrate to the Smart Device. The Security Agent generates the hash of the user's source code. The hash of the agent source code is registered in the Blockchain Ethereum Network. The result of this operation is an identifier of the transaction validated on the Blockchain in the form of a transaction hash. The Security Agent registers the transaction hash in the whitelist by associating it with the user's aid, for which the source code has been saved in the Blockchain. The IoT Gateway allows the user to migrate. After migrating and generating graphs in the Smart Device, the user requests to return to the Temperature Sensor. The IoT Gateway requests the Security Agent verify the user's integrity and authentication after migration. The hash of the user's source code stored in the Blockchain is returned to the Security Agent. The Security Agent compares the hash recovered from the Blockchain with the current user hash. If the hashes are the same, then the Security Agent allows the user to return to the sensor. Actively assisted living technologies based on IoT, blockchain, and 6G can entirely revolutionize how older people age, reduce risks and increase independence. This must be considered in conjunction with the data protection consequences of monitoring technology. Blockchain is a new technology that provides immutability and decentralization to enhance process transparency. This research article outlined the trust problems present in the permission management process of AAL technologies and offered a conceptual framework for blockchain to reduce trust problems. The suggested framework can be implemented in several sectors that deal with sensor data. The proposed BIoT-ALS model enhances the performance, accuracy, reliability, efficiency, and throughput and reduces the network delay, latency, and execution compared to other existing models.

4. Numerical Results and Discussion

The suggested architecture has been thoroughly evaluated in different scenarios. The study carried out an accurate identification test in a smart home utilizing network traffic for the attack detection model. The security model investigates the identification of anomalies in the smart home network. This section presents the assessment results. In addition, this study assesses the performance evaluation of the smart home and overlay blockchain technology for its autonomous operations. Experiments based on an opportunistic network environment are used to examine the performance of the suggested metric. In this environment, a group of 40 6G users with an operating frequency of 8 GHz is employed to access a ratio of 1:2 virtualized resources of 4 to 8. Each resource has a capacity of 500 GB. The virtual servers may handle 100-200 requests during a communication period. An application is invalid when they started period exceeds 60 ms. Delay is verified based on a set of attributes 10 for a maximum number of requests. The blockchain employs 20 MB of delegated memory and privacy for privacy and access controls.

(i) Execution Time and Network Delay

The execution time is taken at the starting point for the creation and processing of the block. The number of blocks and transactions increases in execution and network time in milliseconds (ms). The overhead network in blockchain applications is the overhead network traffic. The delayed change linked with the IoT device's number of nodes displays a greater delay as the network's number of nodes increases. Figure 6 (a) shows the execution time of the proposed BIoT-ALS model. Because blockchain technology is decentralized, it determines scalability and resilience using participating node resources and reduces many-to-one traffic. It reduces the time required to overcome the one-point failure. Figure 6 (b) demonstrates the network delay of the proposed BIoT-ALS model.

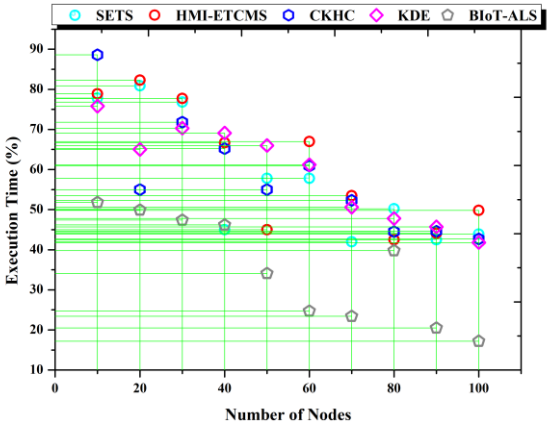

Figure 6 (a). Execution Time

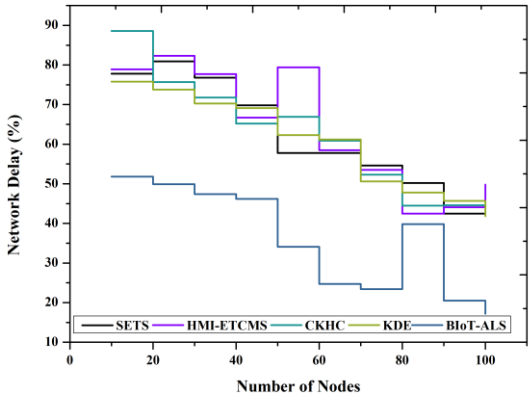

Figure 6 (b). Network Delay

(ii) Latency Ratio

The latency ratio is initially low since the number of nodes in the network is reduced. However, as the network size increases, the latency rate increases due to longer node processing time. The necessary low-latency data may be obtained from visitors. To assess the legality of a visitor's identification quickly, the smart home manager may swiftly check on the authenticity of a visitor's signature. With the volume growing, latency is a problem. Therefore, latency and resource management are noticeable exchanges between the two blockchains. Figure 7 shows the latency ratio of the proposed BIoT-ALS model.

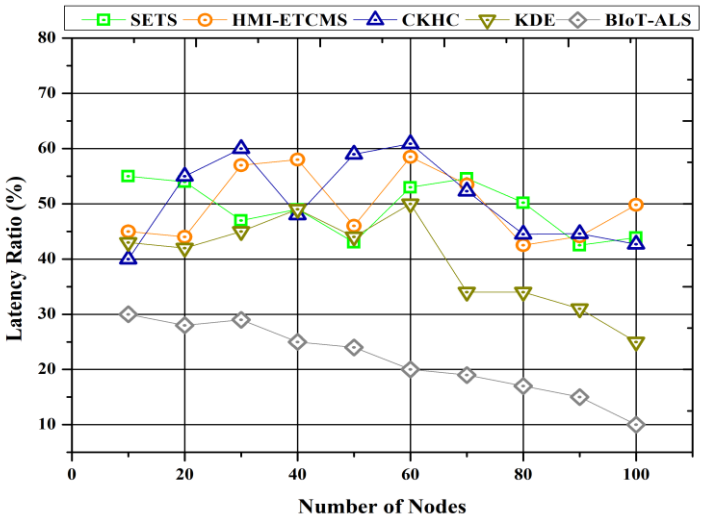

Figure 7. Latency Ratio

(iii) Throughput Ratio

The throughput of our suggested approach is around 75 Mbps, as seen in Figure 8. Typically, the number of blocks grows, and the output grows for increasing transactions. At the time of t, when the block number is 1000, the data attacks occur in the network, and system output reduces instantly because of excessive congestion and network packet processing. After some time, it becomes uniform, gradually grows, and heals to some degree. The throughput of the suggested architecture will rise as the IoT nodes in Figure 8 increase the number of requests. The output results in this figure provide higher throughput in the proposed model than other existing methods.

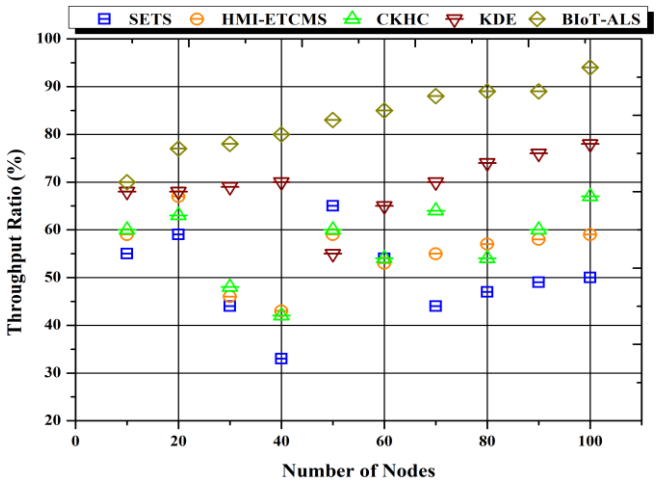

Figure 8. Throughput Ratio

(iv) Performance Ratio

The blockchain-based architecture uses computing and packages overhead to provide enhanced security and privacy for smart home devices and mine operators. The IoT system wants to ensure particular application performance and must be elastic enough to sustain availability at the appropriate level. The overall system capacity is an important factor as all device groups within radio ranges use the same (spectrum) resources (but not those further away because of the concept of space division multiplexing). In wireless networks, packet collisions have been considered to distract from the substantial effort of random access technology. Consequently, every node's power consumption must be limited to maximize network life. Especially for those nodes selected as Relay Nodes, it is vital to deliberately employ them as delivery since their data may be sent to the sink, except as a mediator for another node (because of the direct communication with the sink). Figure 9 demonstrates the performance ratio of the proposed BIoT-ALS model.

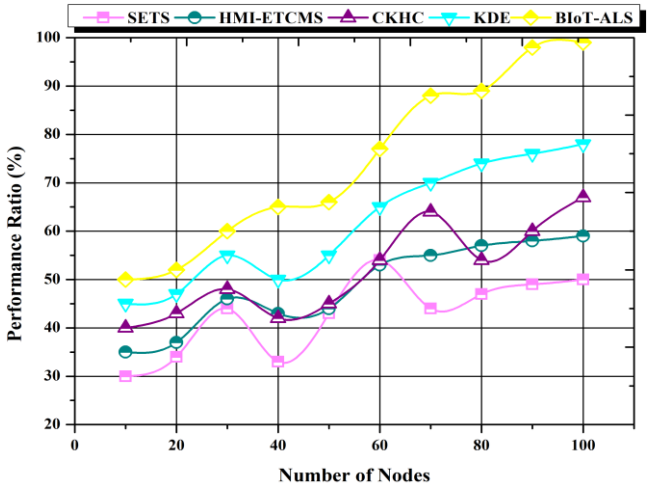

Figure 9. Performance Ratio

(v) Accuracy Ratio

To audit access records' integrity, accuracy, and timeliness, private blockchain-based access control uses the blockchain technique, whereby each access record is recorded in a blockchain once it is generated and authenticated. Due to its inherent verification of a blockchain, its resistance to modifying chained blocks, and the fact that each record is marked on time once recorded in the chain, homeowners and malicious service providers cannot compromise the integrity, precision, and timeliness of the chained access records. Developing trustworthy systems requires sensor precision, while transparency and invisibility contribute considerably to perceiving intrusion and comfort. Figure 10 shows the accuracy ratio of the proposed BIoT-ALS model.

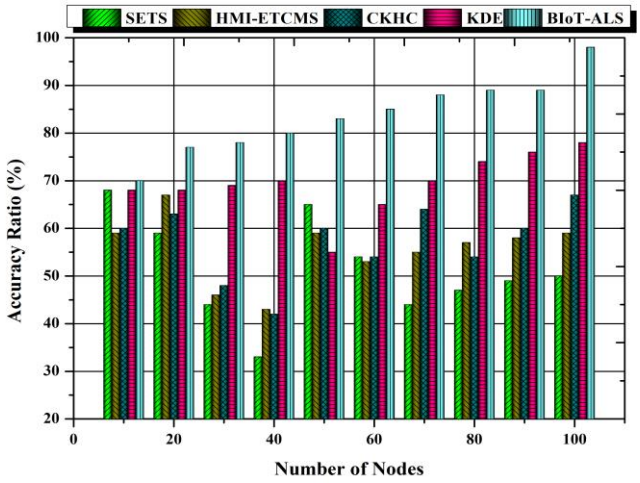

Figure 10. Accuracy Ratio

(vi) Precision and Recall Ratio

IoT is the greatest choice for visualizing assisted living in the smart home concept in reality and requires integrating all approaches across a heterogeneous network. This study analyses the output of every node in the experiment. The entire model detects a fire or anomaly if one node has identified a fire or attack. This study calculates precision (the number of items properly categorized as positive) and recall (the number of precise positive items separated by the overall number of positive classes). Figure 11 (a) demonstrates the precision ratio of the proposed BIoT-ALS model.

In contrast, this study uses (3) to compute the *F*- measure (harmonic mean of recall and precision). To attain great accuracy in prediction, the method must have high recall and precision values. The recall measure is based on the false-negative value. Figure 11 (b) illustrates the recall ratio of the suggested BIoT-ALS model.

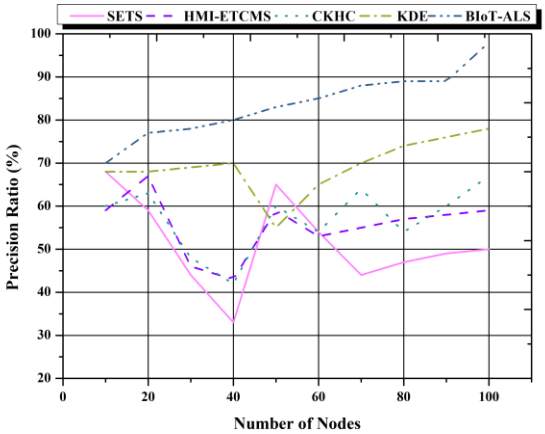

Figure 11 (a). Precision Ratio

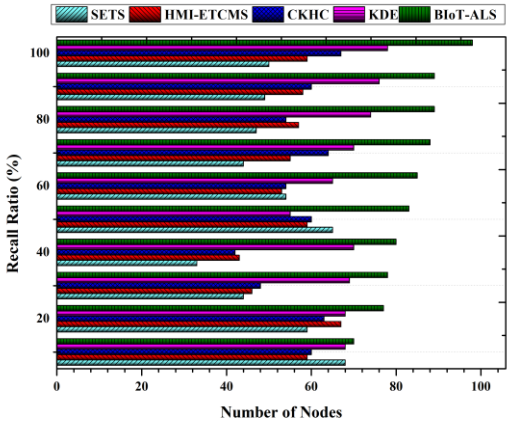

Figure 11 (b). Recall Ratio

Table 1: Reliability Ratio

Number of Nodes	SETS	HMI-ETCMS	CKHC	KDE	BIoT-ALS
10	62.3	55.9	67.8	19.21	77.6
20	75.4	56.6	67.7	59.3	73.7
30	79.0	64.5	71.4	69.6	80.1
40	71.0	64.2	67.5	73.9	82.3
50	74.8	66.4	67.7	73.5	85.7
60	76.8	72.1	68.2	83.4	90.6
70	77.7	74.2	68.3	85.6	91.7
80	70.9	73.0	72.6	80.2	92.9
90	70.57	76.1	73.8	73.5	93.2
100	55.2	74.1	74.1	83.9	94.8

Table 1 shows the reliability ratio of the proposed BIoT-ALS model. Nowadays, many smart home systems applications give consumers recommendations, including energy reduction, warning of faulty equipment, dependable equipment, software choice, diagnosis, etc. The construction of applications based on IoT provides several innovations, including dependable data transfer, quick event detection, prompt data transfer, etc. In this circumstance, it is necessary to create a specialized network to provide reliable handling of the home environment via intelligent network node placement. However, this is not an important technological constraint, the acceptability and usability of the user may be compromised. This is particularly true if the home has a large or uneven surface area or spans many situations requiring significant network replacement devices.

Table 2: Efficiency Ratio

Number of Nodes	SETS	HMI-ETCMS	CKHC	KDE	BIoT-ALS
10	42.3	55.9	54.8	69.2	70.2
20	45.0	56.6	55.7	69.3	73.1
30	49.9	64.5	56.4	70.6	80.1
40	41.2	64.2	67.5	73.9	80.1
50	44.8	66.4	57.7	73.5	81.2
60	46.5	62.1	58.2	73.4	91.4
70	47.2	54.2	68.3	75.6	91.2
80	48.7	53.0	68.6	80.2	92.2
90	50.7	56.1	68.8	83.5	92.2
100	55.2	60.1	69.1	83.9	93.6

Table 2 shows the efficiency ratio of the proposed BIoT-ALS model. The requirement of a safe and energy-efficient smart home with a supported living environment is dependable, scalable, and managed, and a motive to research a smart house, explore obstacles, and provide a solution. A user interface is meant to communicate with home devices via a handheld device, i.e., smartphones or tablets, so the homeowner can effectively operate and monitor the state of any intelligent items inside the aided living room. Therefore, the most important component of a home automation system is the user interface.

The proposed BIoT-ALS model enhances the performance, accuracy, reliability, throughput, and efficiency and reduces the network delay, latency, and execution compared to other existing Smart Energy Theft Systems (SETS), Human–Machine Interface Based on Eye Tracking for Controlling and Monitoring system (HMI-ETCMS), Cumulative Keyed-hash chain (CKHC), kernel density estimation (KDE) methods.

The proposed system design includes a legal framework to ensure responsibility and efficient data governance. In addition, the system has to include ways to get patients' informed permission and observe how their data will be gathered, processed, and shared on the user interfaces. Strict access restrictions, data anonymization, and encryption are necessary to ensure compliance with legislation like General Data Protection Regulation (GDPR) and Health Insurance Portability and Accountability Act (HIPAA). Ethically, the system should safeguard sensitive health information from illegal access and misuse by prioritizing patient privacy via enhanced security measures. Regardless of a patient's socioeconomic background or level of technical competence, the technology should be accessible and equitable, allowing them to use it. Making instructional materials available and creating user-friendly interfaces are two possible ways to achieve this objective. Lastly, with displays or alerts, patients may be informed about how their data is being used, which is essential for ethical responsibility in data management methods.

The BIoT-ALS protocol structures the connection between smart home sensors, wearable health monitors, and cloud servers, allowing for real-time data transmission and processing, all made possible by the exceptional speed and minimal latency of 6G. The users wear wrist-mounted sensors that record their vitals (e.g., heart rate, blood pressure, oxygen levels) and send them to servers in the cloud and on the edge, where data are stored securely on a blockchain. The blockchain feature safeguards patient privacy by limiting access to data to authorized caregivers or medical experts exclusively. Users in the trials were able to get fast responses from caregivers when the system notified them via smartphone alerts of any significant changes in their health. Smart home sensors, such as those for motion and falls, track the user is every step, increasing security by sounding alarms in case of unexpected delays or stops in activity. An assisted living experience that is responsive, secure, and streamlined is made possible by this network of linked 6G and IoT devices, which is protected by blockchain. 6G networks are in the beginning stages and need extensive implementation techniques. Continuous data transmission from wearables and IoT sensors causes the system to create large amounts of data, which increases the need for storage and processing. This may strain resources in the cloud and at the edge. The security advantages of blockchain come with the danger of latency, which might compromise time-sensitive health monitoring, and it is challenging to maintain real-time performance while ensuring data privacy. Additionally, operating costs and sustainability are affected by the energy-intensive nature of blockchain and IoT networks, and it is challenging to integrate varied IoT devices inside a defined protocol to ensure effortless interoperability.

5. Conclusion

This paper presents the BIoT-ALS model for assisted living using 6G communication. Protecting safety and privacy remains a big concern in the Internet of Things (IoT), mainly as IoT networks are widely distributed and decentralized. In Smart Homes, the information systems are often based on data sharing via smart devices (IoT) and built-in sensors. Every sensor produces data for central system processing or assembly. The architecture described was constructed and tested to enhance intelligent homes' confidentiality, integrity, authorization, availability, privacy, and legacy elements such as transparency and interoperability. A smart household miner is a device that centrally processes incoming and outgoing transactions with data for the environment from and to the smart home. Home-based health monitoring might contribute to the safety and security of the homes of a larger proportion of the expanding senior population. The central role of these technologies means that trust management is a major topic for smart environments. The work is now being carried out at all tiers of the proposed architecture to implement and analyse new security mechanisms. Our objective is to develop a prototype of a safe and smart house frame that would ensure that the ageing populations of the globe live independently and safely. The numerical outcomes show that the recommended BIoT-ALS model enhances the performance ratio of 99.1%, accuracy ratio of 98.8%, reliability ratio of 94.8%, an efficiency ratio of 93.6%, the throughput rate of 97.6%, and reduces the network delay of 19.2%, latency ratio 10.2%, and execution time of 20.4% compared to other popular models. Depending on cloud infrastructure may lead to delays, especially when decisions must be made in real-time since data must be sent to the cloud, analysed, and returned. Any interruptions to the internet connection may

significantly affect the availability of services and the user experience, affecting the system's performance. The hybrid blockchain paradigm improves data security and scalability but adds complexity, which might make solving problems more difficult without significant technical expertise. Future studies will extend the pilot deployment to a broader and more diversified user community, which is essential to ensure the system's flexibility and efficacy in different assisted-living environments. Additionally, more investigation is required to enhance the system's capacity for real-time processing.

Funding: There is no funding to report.

Conflicts of Interest: The authors report no financial or other conflicts of interest in this work.

Ethical Approvals: This study does not involve experiments on animals or human subjects.

Data Availability: The datasets used and/or analysed during the current study are available from the corresponding author upon reasonable request.

Acknowledgement: Not Applicable.

Ethics approval and consent to participate: Not Applicable

Consent for Publication: Not Applicable

Competing interests: The authors declare no competing interests.

References

[1] D. Minoli, "Positioning of blockchain mechanisms in IoT-powered smart home systems: A gateway-based approach," *Internet of Things*, vol. 10, pp. 100147, 2020.

[2] D. T. Do, M. S. Van Nguyen, T. N. Nguyen, X. Li, and K. Choi, "Enabling Multiple Power Beacons for Uplink of NOMA-Enabled Mobile Edge Computing in Wirelessly Powered IoT," *IEEE Access*, vol. 8, pp. 148892-148905, 2020.

[3] Y. Lee, S. Rathore, J. H. Park, and J. H. Park, "A blockchain-based smart home gateway architecture for preventing data forgery," *Human-centric Computing and Information Sciences*, vol. 10, no. 1, pp. 1-14, 2020.

[4] K. Seyhan, T. N. Nguyen, S. Akleylek, K. Cengiz, and S. H. Islam, "Bi-GISIS KE: Modified key exchange protocol with reusable keys for IoT security," *Journal of Information Security and Applications*, vol. 58, pp. 102788, 2021.

[5] R. Vinayakumar, M. Alazab, S. Srinivasan, Q. V. Pham, S. K. Padannayil, and K. Simran, "A visualized botnet detection system based deep learning for the internet of things networks of smart cities," *IEEE Transactions on Industry Applications*, vol. 56, no. 4, pp. 4436-4456, 2020.

[6] Y. Cao, F. Jia, and G. Manogaran, "Efficient traceability systems of steel products using blockchain-based industrial Internet of Things," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 9, pp. 6004-6012, 2020.

[7] M. A. Khan, I. M. Nasir, M. Sharif, M. Alhaisoni, S. Kadry, S. A. C. Bukhari, and Y. Nam, "A Blockchain Based Framework for Stomach Abnormalities Recognition," vol. 67, pp. 141-158, 2021.

[8] J. Huang, C. C. Xing, S. Y. Shin, F. Hou, and C. H. Hsu, "Optimizing M2M communications and quality of services in the IoT for sustainable smart cities," *IEEE Transactions on Sustainable Computing*, vol. 3, no. 1, pp. 4-15, 2017.

[9] O. Samuel, S. Javaid, N. Javaid, S. H. Ahmed, M. K. Afzal, and F. Ishmanov, "An efficient power scheduling in smart homes using Jaya based optimization with time-of-use and critical peak pricing schemes," *Energies*, vol. 11, no. 11, pp. 3155, 2018.

[10] S. Kazmi, N. Javaid, M. J. Mughal, M. Akbar, S. H. Ahmed, and N. Alrajeh, "Towards optimization of metaheuristic algorithms for IoT enabled smart homes targeting balanced demand and supply of energy," *IEEE Access*, vol. 7, pp. 24267-24281, 2019.

[11] S. K. Mydhili, S. Periyanayagi, S. Baskar, P. M. Shakeel, and P. R. Hariharan, "Machine learning based multi scale parallel K-means++ clustering for cloud assisted internet of things," *Peer-to-Peer Networking and Applications*, vol. 13, no. 6, pp. 2023-2035, 2020.

[12] M. Kaur, G. Kaur, P. K. Sharma, A. Jolfaei, and D. Singh, "Binary cuckoo search metaheuristic-based supercomputing framework for human behavior analysis in smart home," *The Journal of Supercomputing*, vol. 76, no. 4, pp. 2479-2502, 2020.

[13] B. Le Nguyen, E. L. Lydia, M. Elhoseny, I. Pustokhina, D. A. Pustokhin, M. M. Selim, and K. Shankar, "Privacy preserving blockchain technique to achieve secure and reliable sharing of IoT data," *Computers, Materials & Continua*, vol. 65, no. 1, pp. 87-107, 2020.

[14] P. Gomathi, S. Baskar, and P. M. Shakeel, "Concurrent service access and management framework for user-centric future internet of things in smart cities," *Complex & Intelligent Systems*, pp. 1-10, 2020.

[15] G. Manogaran, B. S. Rawal, V. Saravanan, P. M. Kumar, O. S. Martínez, R. G. Crespo, and S. Krishnamoorthy, "Blockchain based integrated security measure for reliable service delegation in 6G communication environment," *Computer Communications*, vol. 161, pp. 248-256, 2020.

[16] R. Zhang and R. D. Jackson Samuel, "Fuzzy efficient energy smart home management system for renewable energy resources," *Sustainability*, vol. 12, no. 8, pp. 3115, 2020.

[17] P. M. Shakeel, S. Baskar, H. Fouad, G. Manogaran, V. Saravanan, and Q. Xin, "Creating Collision-Free Communication in IoT with 6G Using Multiple Machine Access Learning Collision Avoidance Protocol," *Mobile Networks and Applications*, pp. 1-12, 2020.

[18] Y. Zhang, Y. Wang, and J. Liu, "A novel energy management system for smart homes based on Internet of Things and blockchain technology," *Journal of Network and Computer Applications*, vol. 185, pp. 102966, 2021.

[19] C. B. Sivaparthipan, B. A. Muthu, G. Manogaran, B. Maram, R. Sundarasekar, S. Krishnamoorthy, and K. Chandran, "Innovative and efficient method of robotics for helping the Parkinson's disease patient using IoT in big data analytics," *Transactions on Emerging Telecommunications Technologies*, vol. 31, no. 12, e3838, 2020.

[20] X. Zhang, G. Manogaran, and B. Muthu, "IoT enabled integrated system for green energy into smart cities," *Sustainable Energy Technologies and Assessments*, vol. 46, pp. 101208, 2021.

[21] N. Gunasekaran and G. Zhai, "Stability analysis for uncertain switched delayed complex-valued neural networks," *Neurocomputing*, vol. 367, pp. 198-206, 2019.

[22] W. Li, T. Logenthiran, V. T. Phan, and W. L. Woo, "A novel smart energy theft system (SETS) for IoT-based smart home," *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 5531-5539, 2019.

[23] A. Bissoli, D. Lavino-Junior, M. Sime, L. Encarnação, and T. Bastos-Filho, "A human–machine interface based on eye tracking for controlling and monitoring a smart home using the internet of things," *Sensors*, vol. 19, no. 4, pp. 859, 2019.

[24] M. Alshahrani and I. Traore, "Secure mutual authentication and automated access control for IoT smart home using cumulative keyed-hash chain," *Journal of Information Security and Applications*, vol. 45, pp. 156-175, 2019.

[25] P. Gupta, R. McClatchey, and P. Caleb-Solly, "Tracking changes in user activity from unlabelled smart home sensor data using unsupervised learning methods," *Neural Computing and Applications*, vol. 32, no. 16, pp. 12351-12362, 2020.

[26] S. Bhattacharyya, S. Athithan, S. Pal, B. Sarkar, D. Akila, S. Chowdhury, and S. Gurusamy, "[Retracted] An IoT-Enabled Intelligent and Secure Manufacturing Model Using Blockchain in Hybrid Cloud Communication System," *Security and Communication Networks*, vol. 2023, no. 1, pp. 7556728, 2023.

[27] S. J. Rajawat, M. Kaushik, and S. K. Yadav, "Cloud Enabled e-Banking Payment Security Implementation using Blockchain Technology," *Journal of Electrical Systems*, vol. 20, no. 7s, pp. 1445-1455, 2024.

[28] Y. Luo, W. You, C. Shang, X. Ren, J. Cao, and H. Li, "A Cloud-Fog Enabled and Privacy-Preserving IoT Data Market Platform Based on Blockchain," *CMES-Computer Modeling in Engineering & Sciences*, vol. 139, no. 2, 2024.

[29] A. A. Khan, A. A. Laghari, A. Kumar, Z. A. Shaikh, U. Baig, and A. A. Abro, "Cloud forensics-enabled chain of custody: a novel and secure modular architecture using Blockchain Hyperledger Sawtooth," *International Journal of Electronic Security and Digital Forensics*, vol. 15, no. 4, pp. 413-423, 2023.

[30] R. A. Abutaleb, S. S. Alqahtany, and T. A. Syed, "Integrity and privacy-aware, patient-centric health record access control framework using a blockchain," *Applied Sciences*, vol. 13, no. 2, pp. 1028, 2023.