IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 8 March 2024, accepted 26 March 2024, date of publication 1 April 2024, date of current version 10 April 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3383310

RESEARCH ARTICLE

Smart Healthcare: A Dynamic Blockchain-Based Trust Management Model Using Subarray Algorithm

MIMONAH AL QATHRADY[1], (Member, IEEE), MUHAMMAD SAEED[2], RASHID AMIN[2,3], MOHAMMED S. ALSHEHRI[4], ASMA ALSHEHRI[5], AND SAMAR M. ALQHTANI[1]

[1]Department of Information Systems, College of Computer Science and Information Systems, Najran University, Najran 61441, Saudi Arabia
[2]Department of Computer Science, University of Engineering and Technology, Taxila 47050, Pakistan
[3]Department of Computer Science, University of Chakwal, Chakwal 48800, Pakistan
[4]Department of Computer Science, College of Computer Science and Information Systems, Najran University, Najran 61441, Saudi Arabia
[5]Department of Computer Science, College of Computer Engineering and Science, Prince Sattam Bin Abdulaziz University, Al-Kharj 16273, Saudi Arabia

Corresponding author: Rashid Amin (rashid4nw@gmail.com)

Authors would like to acknowledge the support of the Deputy for Research and Innovation - Ministry of Education, Kingdom of Saudi Arabia for this research through a grant (NU/IFC/02/SERC/-/31) under the Institutional Funding Committee at Najran University, Kingdom of Saudi Arabia.

ABSTRACT A growing kind of communication, the Internet of Things (IoT), links all network-capable devices worldwide. The most recent phase of the Internet of Things (IoT), known as the Internet of Medical Things (IoMT), is one that is rapidly catching researchers' interest. The centralized storage system houses the substantial amount of medical data created by IoMT. However, centralizing sensitive patient data creates a single point of failure and raises privacy and security issues. To assure honesty, reliability, and safety while determining an entity's trustworthiness, trust information is required to be safely transmitted and preserved. We propose a safe trust management solution based on blockchain technology. The proposed solution gathers node trust data using both time- and event-driven methods that are used to compute the trust of a node based on the threshold value. We also confirm the validity of data by varying the threshold value during transmission and authentication and employing a membership mechanism for authentication. The trust scores for each node are securely stored in an array, and the Maximum subarray (Kadane) Algorithm is used to compute the threshold value. The blockchain network receives and stores the IoMT score in the trusted list. Due to its distributed structure, capacity to maintain safeguards, and resiliency against a variety of threats with low overhead. Our approach is viable, deployable, and appropriate and also includes safety features like tamper-proofing, attack resistance, dependability, and low capabilities for IoT in smart hospitals.

INDEX TERMS IoMT security, *blockchain*, smart hospital, trust management, medical sensors, 5G, temper proof, Kadane algorithm.

I. INTRODUCTION

This Internet of Medical Things (IoMT) is a software, hardware, network access, and sensor/actuator-based embedded system [1]. As these technologies become more complex and interfere with essential healthcare procedures, various security and privacy concerns have arisen. However, while IoMT technology moves faster, most devices are resource-constrained, prohibiting us from addressing multiple security and privacy mechanisms [2]. Even though IoMT ecosystems include numerous protocols and standards, they have security and privacy problems [3]. Furthermore, traditional cloud-based healthcare systems include limitations such as a single point of failure, lack of transparency, limited control over personal data, and excessive latency [4]. The healthcare industry cannot provide essential healthcare services to many patients during pandemic times due to a shortage of medical service personnel. With the help of the right combination of protocols, procedures, and increased system design, these technical problems can be overcome [5], [6]. Healthcare

The associate editor coordinating the review of this manuscript and approving it for publication was Zesong Fei.

practitioners may spend more time researching the patient's health concerns and less time on pointless professional consultations thanks to the remote patient monitoring system (RPMS) [7].

Data storage and transmission are encrypted and maintained to guarantee the data's correctness, validity, and, most importantly, authenticity [8]. Additionally, it ensures that only those with permission can access and edit data. Privacy protection is a crucial objective to take into account while building an SHS (PP) [9]. The open and unsafe route used to convey shared data largely determines how serious and sensitive it is. While content privacy can safeguard patient information against data theft, preserving patient privacy is challenging, as an attacker can deduce a patient's health status based on the identity of the attending doctor [10]. Contextual privacy refers to the protection of the communication's context [11].

Health professionals have made considerable use of EMRs, patient portals, and smartphone applications to manage electronic medical information. Interplanetary File Systems (IPFS) stores IoMT data blocks off-chain and records patient data as strings in blocks [12]. There are issues with bandwidth and data storage since every participating node on the blockchain network now has access to the whole patient's medical records. Intelligent healthcare networks with IoMT capabilities are vulnerable to serious attacks and security issues [13]. In a healthcare application, a key is used to securely convey alerts to trusted healthcare professionals based on health data [9]. According to the validity evaluation of digital identification, the patient's authentication is performed using blockchain-based electronic verification. It means that the technology used to verify an individual attempting to access a service is regulated [8]. The source of information is transformed into the entity's encrypted language using blockchain encryption of patient data [8]. This blockchain network involves safeguarding the integrity and privacy of digitally protected health information stored in health records, ensuring that unauthorized individuals cannot access or use information even if it is stored in a database or network [7].

The emergence of 5th Generation (5G) wireless technology offers never-before-seen bandwidth rates. 5G provides increased speed, capacity, and a cheap cost per bit. It has a vast broadcasting capacity of up to Gigabit and can sustain about 65,000 simultaneous connections [14]. In contrast to earlier advancements from 2G to 3G to 4G, the transition to 5G now opens up entirely new application domains, particularly in IoMT and the Tactile Internet. As a result, there are a variety of new research difficulties for both establishing networks and developing the hardware/software architecture to efficiently handle the vast range of demand in their implementation [15]. By pre-caching critical services in stationary edge nodes, edge computing (EC) becomes a significant model for achieving ultra-low latency for IoMT applications at the network edge. [16].

Blockchain was first created by Nakamoto in October 2008, and because of its collaborative network architecture, it currently holds the top spot on the internet. Blockchain originally belonged to the Bitcoin digital coin system. A characteristic of Blockchain is the public ledger that is maintained by all the nodes in the network. Due to Blockchain's collaborative structure, decentralized or third-party intervention is not essential for identifying or resolving cyberattacks. Blocks, another name for this continuously growing collection of documents, are connected by a secret hash. Data storage on the blockchain is anonymous and integrity-protected. Blockchain data cannot be readily modified once it has been recorded. Each block contains information about preceding nodes, and an intruder can take advantage of the network by using malicious nodes. Before being permitted to interact with other nodes, these nodes must go through verification [17].

Our suggested method uses blockchain technology to increase the reliability of devices using IoMT in smart hospitals. We calculate the minimum acceptable value using the subarray approach, then use the miner to send out its threshold score to the whole network while evaluating every node's trust score to the value of the threshold. Information about trustworthy devices is kept in a trusted list. The suggested model recalculates the trust score and threshold levels and broadcasts them at certain intervals or whenever a new event takes place. It is both time-dependent and event-driven.

To take advantage of blockchain technology's encryption techniques regarding dependability, traceability, and information integrity, our objective is to introduce a secure trust system based on this technology. By integrating blockchain technology with the trust concept, we can leverage its security features, including dependability, scalability, and data security.

A. RESEARCH CONTRIBUTION

IoMT devices commonly rely on cryptography and access control to ensure security. However, these methods have several limitations, such as the potential for fraudulent information and system hijacking. Additionally, the complexity and lack of uniformity of these techniques can compromise the nodes themselves, as cryptography may inadvertently authenticate bogus information, while access control can be circumvented by unauthorized users. To address these issues, trust computation can be used as a more effective alternative for IoMT security. Trust management allows devices to share trust with neighboring devices for communication, which can help mitigate the problems previously mentioned. The following are the primary contributions of this research.

- The proposed system employs reputation and trust-related data to create an immutable network for IoT, thereby gathering and disseminating information regarding credibility and trust through the Blockchain network.

- In the proposed IoMT scheme, each node requires membership authentication to communicate. For an IoMT device to communicate, it must possess authentic, rational, and trustworthy files regarding membership and transaction details.
- The connections and transactions are hybrid stored to acquire data concerning trust using both time-dependent and event-driven techniques. The ultimate trust score and level of trustworthiness are then tallied using a trust manager.
- The trust scores for each node are securely stored in an array, and the Maximum subarray (Kadane) Algorithm is used to compute the threshold value. These trust values from IOMT devices are stored in the Blockchain network. Due to its distributed structure, capacity to maintain safeguards, and resiliency against a variety of threats with low overhead.

The rest of this paper is broken up into several sections. The Related Work is described in Section II, and the Proposed System is described in Section III. The model's performance and evaluation summary are presented in Section V, and the study's conclusion is presented in Section VI.

II. RELATED WORK

In IoT systems trust computation is a vital task that affects the performance of the entire network. The research that has already been done on trust calculation in the IoT space is presented in this section. Egala et al. [18] proposed a ground-breaking blockchain-based architecture that offers a decentralized EHR and service automation based on smart contracts without endangering the system's security and privacy. The researchers address the limitations of blockchain-based IoMT healthcare systems that employ the cloud by combining the hybrid architecture with a distributed storage approach utilizing blockchain. To increase the security of the suggested system, a decentralized selective circle-based access control system, device authentication, and patient record privacy algorithms are developed. The suggested system evaluates the cost-effectiveness of data sharing and the latency of the blockchain.

Fang et al. [19] work on the analysis of the cybersecurity in ICN and also analyze the attack activity and defense schemes. The author used a fast and efficient trust management system for acute attacks. The acute attack is on-off. This system can notice and eliminate attacks in a very short period. Singh et al. [20] presents an approach for scalable trust management in IoT. They focused on bad-mouthing. They overcome the issues related to practical and pressing difficulties that belong to IoT, such as IoT clustering, which belongs to trust management, countering bad-mouthing attacks on the trust system through an intelligent method, and memory efficiency related to IoT trust computations.

Das et al. [21] The technique introduced in this paper relies on four key concepts: Self-trust, Green Trust, Social trust, and QoS trust. Self-trust is calculated within the node through the following means: trust in processing IoT data, trust in maintaining IoT data privacy, and trust in transmitting IoT data. Green trust pertains to the network's attributes, specifically its longevity and responsiveness. Social trust was responsible for evaluating device performance in its environment. Finally, QoS trust was used to verify trust on the node.

Arul et al. [9] MMSDDF, a multi-model confidential information distribution mechanism built on blockchain, was created to protect patient data in IOMT against unauthorized access and administration. The proposed architecture was intended to provide the highest levels of security and secrecy for the context of healthcare data in IoMT devices. The public blockchain keys have been implemented in a network of medical services where patient health data may be utilized to provide crucial alerts for licensed healthcare professionals. In comparison to other current approaches, their proposed method achieved 95.8% accuracy level, latency ranges of 0.5-0.8, and a response time of 1.5 %.

Khan et al. [22] presented a technique for detecting brain tumors based on their degree, ranging from degree I to degree IV. They employed Partial Tree (PART), an enhanced feature set association rule learner. The proposed model was compared against existing approaches, i.e., Random Forest, CART, Naive Bayes (NB), and Random Tree using 10-fold cross-validation. The results show that a partial tree implementation with an enhanced feature set selection can outperform the other strategies [23]. The performance measures used for evaluation include precision, recall, and F-measure.

Vaiyauri et al. [24] analyzed the security measure of IoMT and introduced a technique intending to secure the network from most of the attacks. About safety, confidentiality, guarding, verification, and approval, as well as the usage of blockchain for safe data flow between various nodes, SHS protects IoMT using the most advanced, cutting-edge techniques. Finally, the review's conclusions were summarised, demonstrating not only the advantages and disadvantages of present-day confidentiality and safety techniques but also the possibilities and probable directions for future study that may motivate researchers to organize their studies better based on the secure implementation of IoMT to SHS in the next ten years.

Lin et al. [17] The NR signal signature and Markov chain were used in a novel approach termed LNM that had been suggested for usage in smart buildings. Despite interface variety and changing environmental conditions, the offered technique for creating and localizing radio fingerprints integrated a neighbor's relationship strategy, resulting in stable and precise localization. The findings of the many studies the researchers ran on various cell phones showed that LNM was simultaneously practical and dependable, delivering ideal precision for localization with a standard error of about 1.5 m. While trust is a broad concept that may apply to nearly any situation, existing studies have not fully examined its management in the IoMT domain. Moreover, existing proposed trust models typically consider

only a limited number of parameters to analyze reliability, focusing on QoS, social, or reputation factors without addressing security mechanisms that validate the authenticity and privacy of trust evidence throughout their acquisition, distribution, and interaction among IoMT nodes. Another challenge faced by trust management systems is linking identification to a single node and preventing a single node from being associated with multiple identities. However, the emergence of Blockchain technology has provided a potential solution to these challenges and can address nearly all of the aforementioned issues. Advancements in attack robustness, cryptography, access control, and distributed computer networks have led to the emergence of various new security services, including data sharing, data storage, and reputation systems.

III. PROPOSED SYSTEM

The proposed system consists of a two-layered model, i.e., the IoMT layer and the Blockchain layer. in IoMT layer network devices, i.e., sensors, and nodes, of a smart hospital are contained. In the Blockchain layer, the miner, blockchain network to store trust information and trusted node information is presented. Our primary goal is to provide innovative trust management using blockchain. Transparency, integrity, authenticity, and permission are all guaranteed by our technology, which creates and analyses a trust score for each device before securely storing and transferring these ratings throughout the IoMT network. The following sections will provide an overview of our proposed scheme's architecture. To calculate trust values effectively, store them securely, and distribute them throughout the blockchain network, we must first accurately understand the precise composition of our system. Additionally, a quick rundown of the necessary interactions will be provided. Two additional components, which store the trust parameters used to gauge trust, are further separated into the IoMT devices. The first component is knowledge, which builds knowledge among nodes using compatibility, integrity, and feedback. The second component is used to hold the other nodes' identity mechanism for interaction and data sharing next time. The experience component also contains the recommendation. It helps the node to gather suggestions about particular nodes. The collection of suggestions is beneficial for trust evaluation. The data in the experience component is used to connect the devices only for the first time.

Figure 1 smart hospital is a 5G network cell, and smart hospital floors are 5G network sectors. All IoMT devices on a single floor are connected through wired media, and all floors are connected wirelessly. All floors in a 5G network are connected via radio waves.

Figure 2 illustrates the layers used in the proposed framework for trust management. The first layer is IoMT, while the second is the Blockchain layer. In the IoMT layer of the system, there are IoMT devices and trust managers. The Trust manager manages the calculated trust of each device in

FIGURE 1. IoMT devices connected through 5G networks.

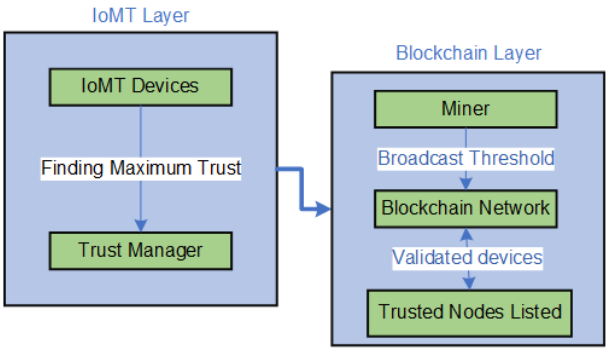


FIGURE 2. A layered model in which IoMT layers and Blockchain layers communicate with each other.

the network. The Blockchain layer has a miner server used to broadcast the threshold values, while trusted devices, after the validation based on threshold values, are stored in a "Trusted nodes list" list. The proposed system is time-based and event-based. It updates trust after a specific time when some event occurs.

A. TRUST MANAGER

The Internet of Medical Things (IoMT) is a critical component of the hospital's digital transformation, which will result in a new hospital ecosystem and healthcare model. The intelligence of the IoMT can be improved with the use of edge computing, and the IoMT can take root in a variety of vertical structures. Mobile phones, robots, digital sensing devices, smart bands, and home automation devices are examples of personal edge computing. As a result, in our case, we used personal edge services. The trust manager and miner use the personal edge services in the presented strategy. These two servers perform the data processing tasks. The service edge is where data from IoMT devices is gathered.

Such devices could be used in a smart hospital to help with information exchange and processing. The synchronization of different cloud platforms is required for a complicated IoMT application. The main purpose of a cloud at the edge often referred to as edge computing, is to bring computational resources, storage, and data processing closer to the source of data generation. Various data processing jobs should be used in a system of information processing activities. Application data analysis tasks take inputs from multiple computing devices, and the system distributes the bandwidth of the network enabling transmission among data nodes for application information processing tasks. The processing logic integrated with numerous data sources may be required to assess the information flows; the same system must handle it. A computer node generates an application data stream, transmitted to the associated data processing job via an edge computing network. Figure 3 shows that the trust manager server acts as an edge computing node in our strategy. In the trust manager, all calculations are completed, and the full trust and threshold values are determined. The threshold value is sent to the edge mining and the miner. This system unit is primarily responsible for monitoring the authenticity and integrity of the devices. Based on the credentials, IoMT in Smart hospital devices and smart objects are authenticated. Then, the trust manager permits any new node to enter the network. It uses the trust value for this purpose. For this purpose, the trust manager computes the trust value of every new node and, after every new time quantum, stores the calculated trust's copy to the cloud. The article uses the round-robin technique for adding the time quantum specified by the system. After the authentication, the trust manager allows the device to be part of the network, but it does not allow it to make any transaction. To enable the machine to make transactions in the network, the trust manager sends the device's trust value to the miner.

In this scenario, a trust may be described as a relationship among many parties, such as the trustee, the assessor, and the beneficiary of the trust who is the subject of the evaluation. The strength of this relationship depends on the time value at which a node is being evaluated. The following variables are used to define the relationship at a given time ''n'' between the trustor ''tr'' and trustee ''ti.'' The variable T represents the trust (tr→ti)t, which is a value assigned to this relationship. T ri(t) is used to indicate the trust worth of any hardware r for any other device j. The possible values of this trust score are -5 to $+10$, with -5 denoting complete mistrust and $+10$ denoting total trust.

The following processes are included in the proposed model in a cyclic order:

- Inspections of packet delivery behaviour and advice from nearby entities are used to acquire data on trust.
- The trustworthiness of each participant was assessed, with a particular emphasis on Direct and Indirect trust. The calculation of each type of trust focuses on different characteristics and factors, such as the entities' cooperativeness, expertise, and interests. Indirect trust is evaluated based on the entities' integrity about the recommendations they have made.
- We used two techniques for inserting a new device into the system: 1. Device registration 2. Authentication and authorization The proposed system used an identification and authentication system to add a new device to the IoMT network. In this system, IoMT devices are authenticated through trust or threshold value. The proposed system utilizes the two aforementioned methods to identify a new device. This identification is based on authentication through a threshold value and is further used to verify the device to obtain trust information. In the device registration process, the proposed system calculates trust based on previous experiences and the recommendation system. After calculating the trust score, it is compared with a threshold value. If the trust score meets the threshold value, the proposed system allows the device to proceed with transactions and join the system. Verification and integrity checks were used by our system when updating the firmware. Using this method, a device updates its firmware and verifies its validity and correctness by performing verification and integrity checks. There might be a system in place to roll back updates that are unsuccessful or incomplete. This allows the device to go back to the prior firmware version to preserve functioning and prevent any problems.
- By combining these attributes and previous trust assessments over time, a composite trust score is generated to maximize security within the considered framework reliably and simply. The combined weighted average of the two components–the most recent trust assessment and those conducted throughout the time period ''t''–leads to the ultimate trust score, as is seen in the graph below.

$$Txy = tri1 * (Txy)(t-1) + tri2 * (\Delta t) \qquad (1)$$

The values tri1 and tri2 correspond to a time difference of t and satisfy the equation tri1 + tri2 = $+10$, with tri1 ranging from -5 to $+10$ and tri2 also ranging from -5 to $+10$. The behaviour of an entity is subject to frequent changes over time, but the entity consistently monitors its trust-related attributes regarding its neighbors, including their cooperativeness, capabilities, and attention group. For the system to operate as intended, entity e's level of cooperation, as assessed by item exy through act monitoring throughout the interval [0..t], is crucial, according to equation 1. The Throughput measurement, which determines the proportion of successfully sent bits to the entirety of packets delivered by the sender, is used to gauge this level. Another critical attribute is the aptitude property, which reflects the entity's ability to execute proposed functions and is assessed based on its energy and computing capabilities. The interest factor community, which is defined as the proportion of their shared principles of community compared to their overall common

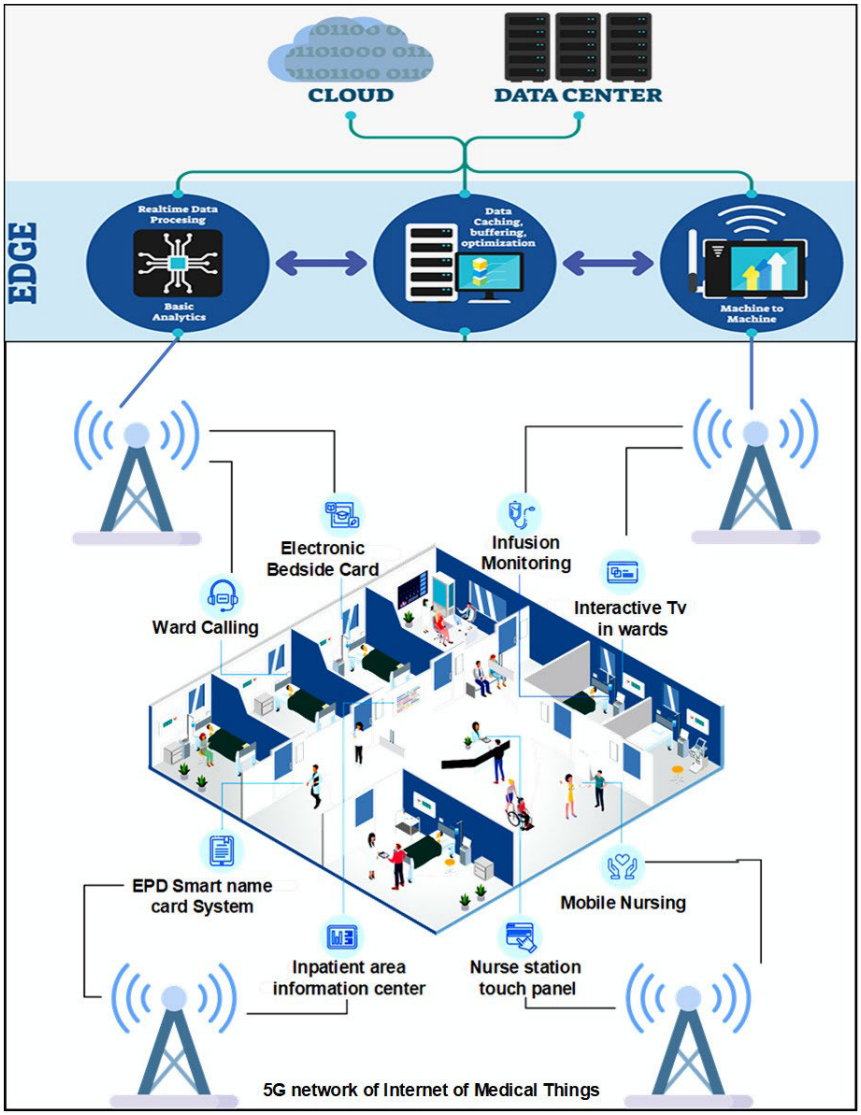


FIGURE 3. IoMT framework with edge computing architecture.

interests, defines the level of cooperation or shared interests between entities.

After the trust calculation, we store all nodes' trust in the array. To identify the largest subarray of trust values, the Kadane method is used with a dynamic programming approach. Bentley introduces Kadane's approach, which has an O(n) time complexity and is used to explore the whole subarray sum in linear time. following the compilation of all subarray components. The greatest number of the subarray is divided by two to determine a threshold value once trust has been calculated and the trust array has been used with a subarray technique. This value is used as a checkpoint. If the trust value matches it, the corresponding node is authorized otherwise unauthorized for communication. The following algorithm is used for finding the maximum subarray.

A robust technique for quickly determining the largest subarray sum in a numerical array is Kadane's Algorithm. It is beneficial in many fields, including computer science, finance, and other fields because of its simplicity, adaptability, and linear temporal complexity. It is essential to look at how changes to the submatrix are tracked as it only displays the maximum sum of the submatrix and not the submatrix itself. The subarray problem can be solved using unordered arrays, but it might not be the most efficient approach. The subarray problem typically involves finding a contiguous subarray within a given one-dimensional array that has the largest sum or meets certain criteria. Using unordered arrays (often referred to as sets or hash sets), we can still solve this problem by iterating through all possible subarrays and calculating their sums or checking their properties. Instead, traditional arrays or lists are often used because they allow direct access to elements by index and facilitate iteration in a linear order. This makes it easier to implement efficient algorithms for solving the subarray problem, such as

Kadane Algorithm for Finding Maximum Subarray

Input: 3,2,-2,5,-3,1,-4,-5,4,-1,0
Output: Find maximum trust value
Initialisation:

```
int max_trustsubarary=integer min-value
int sum-nodes=0;
for int i=0; i<a.length; i++ do
    sum-nodes = sum-nodes + a[i];
    if (max-trustsubarray<sum-nodes) then
        max-trustsubarray = sum-nodes;
    end if
    if (sum-nodes<=0) then
        sum-nodes=0;
    end if
end for
```

Kadane's algorithm for finding the maximum sum subarray. The primary idea of the Kadane algorithm involves maintaining variables that store the maximum sum of a contiguous subarray ending at the current index and the maximum contiguous subarray found thus far. Any subarray with a negative sum is disregarded by setting the variable sum-node to 0 in the code. We continue extending the subarray as long as it yields a positive sum. The current element of the iteration is denoted as representing the iteration's current element. Utilizing the previously derived equation, we compute a value for Max_arr at each index. This process aids in deciding whether to incorporate the current element in the subarray or commence a new subarray at this index. The highest subarray sum achieved during the iteration is preserved in another variable namedmax-arr. Upon completion of iteration over the last index, the total of the maximum subarray is stored in Max _ind. The greatest number of the subarray is divided by two to determine a threshold value. We find the threshold value using the maximum subarray. Figure 5 represents the complete working of the subarray problem (Kadane algorithm). If the sum of the current subarray goes negative, the algorithm resets it to 0, effectively removing any negative subarrays.

Figure 4 represents the flowchart for the subarray process. Initially, the array contains the trust of all IoMT nodes in the network. In the first algorithm, the trust values ''a[i]'' are used as input, and contiguous subarray values (sum_nodes) are used to find the maximum subarray. The total sum of the contiguous subarray is stored in a variable (max_trustsubarray). Every time variable ''sum_nodes'' is compared with max_trustsubarray and updates the max_trustsubarray. If sum_nodes are greater than max_trustsubarray, then the sum_nodes are saved in max_trustsubarray; otherwise, it creates a new sub-array. This algorithm maintains the initial position of the subarray and frequently checks the next element.

B. BLOCK CHAIN

The second layer of the proposed model uses blockchain for the authentication of new nodes. In this layer, a miner uses a round-robin technique to verify the authenticity and integrity of trusted nodes and transactions. The most current miner value is then published on a blockchain system where trust data is transmitted across network devices and verified in a decentralized way. The system generates authenticity and transaction-related keys that are used to verify the reliability of networked devices and digitally sign operations based on reputation and trust metrics. The integrity of the system is greatly enhanced by these keys. There are two ways to calculate the solution for any element at index ''i''. Either add to the solution found till ''i-1''the index OR start a new sum from the index ''i''.

$$max\_trustsubarray = sum - nodes + a[i] \quad (2)$$

Figure 5 represents the iteration's current element. We'll use the equation we derived before to determine a value

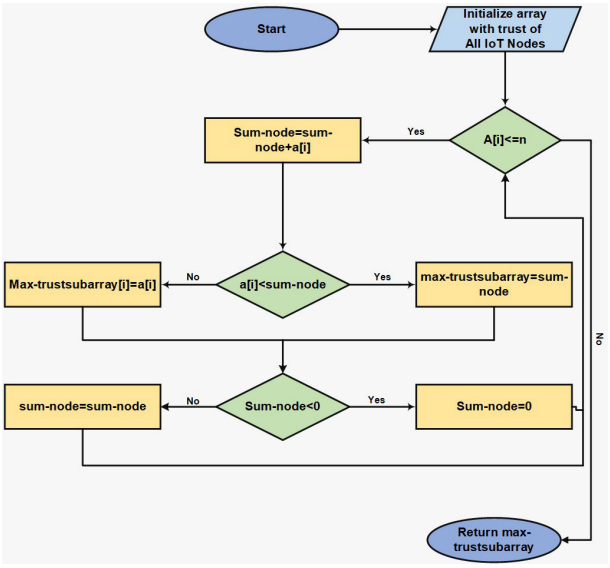


FIGURE 4. Flow model for maximum subarray calculation.

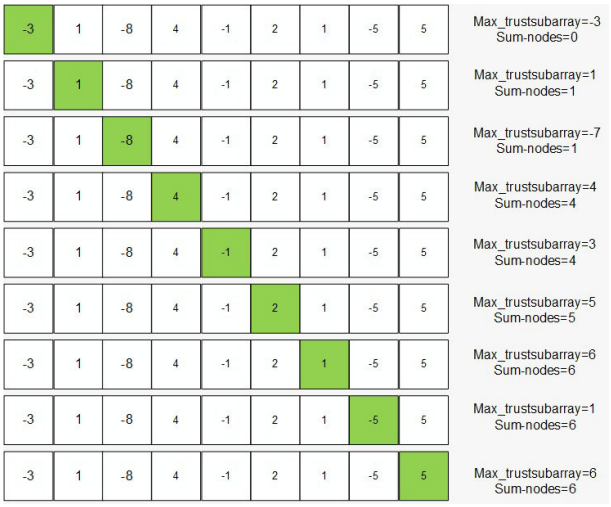


FIGURE 5. Maximum subarray computation for trust values taken from different nodes.

for Max_trustsubarray at each index. This allows us to determine whether the current element should be included in the subarray or if a new subarray should be started at this index. The maximum subarray sum obtained throughout the iteration is stored in another sum-nodes variable. Max so far will store the total of the maximum subarray once we've iterated over the last index.

Our approach used Blockchain for trust management. A miner server is used to broadcast the threshold values. The round-robin technique is used for authenticating a new device, checking integrity, and producing authenticity and transaction-related keys in this consensus. POW ensures distributed verification of trusted data in network devices and improves system integrity. The necessity for honesty, reliability, authenticity, and permission to provide creative trust management for IoMT devices that are used in a smart hospital is what motivates the adoption of Blockchain consensus in the solution. The primary motivations for incorporating Blockchain into our system are its transparency and immutability. These attributes enhance the security and efficiency of our system compared to traditional trust management in IoMT networks. Blockchain imposes penalties on a malicious node should its trust score fall below the threshold value. However, if the node resumes responsible behavior, it can sustain a score around the threshold value, utilizing a feature offered by Blockchain technology. Transparency fosters trust among participants, particularly in complex IoMT applications involving multiple entities. The threshold values are disseminated via a miner server. In this consensus, the round-robin method is employed to produce authenticity and transaction-related keys, verify integrity, and authenticate new devices. POW enhances system integrity and provides distributed verification of reliable data in network devices. The implementation of Blockchain consensus in the solution is driven by the need for permission, honesty, reliability, and authenticity to provide innovative trust management for IoMT devices used in a smart hospital. The primary characteristics of Blockchain aid in trust management. The entity is responsible for handling and verifying transaction information as well as the legitimacy, integrity, and authenticity of trust records. After being received, this data is disseminated to the network of miners, who confirm its accuracy and incorporate it into a block that is added to the ledger. It is important to note that every miner entity keeps a current, comprehensive copy of the ledger. To organize the blocks in the Blockchain for broadcasting the threshold value, we implement the gossip protocol within the network. When new nodes join or at specific time intervals, miners broadcast the threshold value across the network through the protocol. The gossip protocol is utilized to provide a distributed and robust method for broadcasting information/threshold values within the Blockchain network. In Blockchain, files are arranged into collections known as blocks. Each block in the Blockchain contains its own set of transactions. The number of transactions in each block depends on the available space.

Blockchain has main features that help trust management.

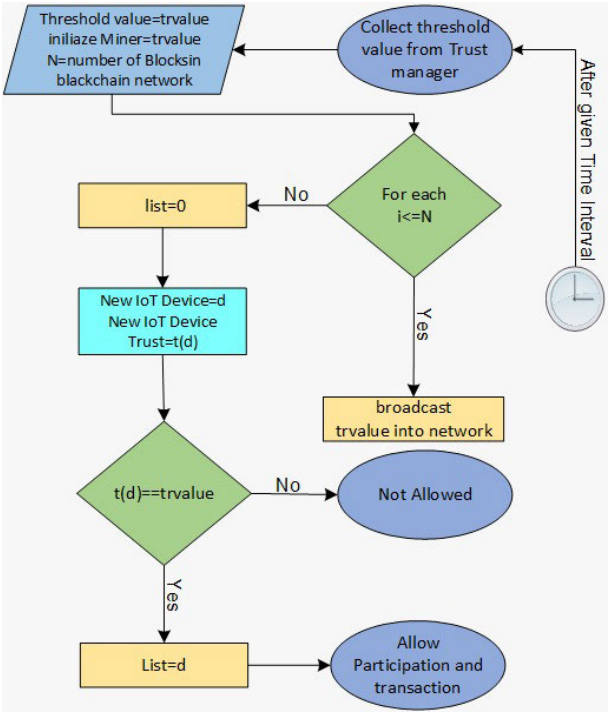


FIGURE 6. Blockchain flow model for the proposed system.

Decentralization: Blockchain uses the main idea of storage, distributed and decentralized computing. Blockchain has no centralized database and each node of the Blockchain has its charge of storing.

Security: Blockchain security features consist of accessibility, privacy, and honesty. Blockchain provides authenticity and consistency by chain blocks using hash functions, which prevents data within blocks from being changed once they are joined.

Traceability: Blockchain achieves very high degrees of data transfer and accountability harmony. This system provides efficient historical information sharing while ensuring transaction transparency and traceability. When it comes to the Internet of Medical Things applications like smart manufacturing, tracing backward in time is essential.

We take into account Multichain Blockchain technology in our framework, which is a secure Blockchain protocol that controls block access employing a list of registered users. The only people who can read and write in the ledger are those who have already registered. The consensus mechanism used by Multichain. The mechanism known as the round-robin (RR) algorithm is used to approve transactions. The rationale behind our selection of Multichain primarily alludes to the reality that the last meets the majority of our required characteristics. The reason for using the POW consensus is the selection of a miner for the next block.

Figure 6 illustrates the flow model for the proposed blockchain technique for edge computing nodes (trust management). The trust value of each node is computed first, and then the threshold value is defined. After that, the

threshold value is broadcasted by the miner into the whole network. Initially, the trust is empty; when a new node enters the network, its trust is computed. If the trust value of the new node is equal to the threshold value, then it is added to the list. If the new node trust value is less than the threshold value, it cannot enter the network and can not do any transactions. The trust value is transferred to the miner by the trust manager of IoMT in the Smart hospital network. The miner has a list of all previously registered nodes with the network. The new node after authentication is added to the list for transactions. The value of the list is updated in which the new node is added and broadcasted into the blockchain environment so that the new node can communicate with other trusted nodes or devices.

This layer of the proposed system is responsible for checking the devices' accuracy, legitimacy, and integrity and allowing new machines to make transactions. It collects trust values for trust management, and after verification of trust, it broadcasts the trust of the device in the blockchain network. The trust of the last device is broadcasted in the blockchain network, where it is verified for its validity. After broadcasting the trust, it includes the new device in the trusted devices list. The trusted devices list contains the IDs and trust values of all authorized devices. The proposed model uses a round-robin technique that uses a time limit for the update cycle of trust computation. In this process, after a specified time, the trust of every connected device is computed and compared with the threshold value to retain it in the network. If the trust value of any device is less than the threshold value, the device is excluded from the web and the trusted device list.

Blockchain Authentication and Allocation

Input: threshold value and new node trust

Output: Listed nodes and allow participation and transaction

Initialisation:

```
Collect threshold value from server(trust manager)
threshold value=trvalue
Initialize Miner(server)=trvalue.
for int n=Node1; n<=NodeN; n++ do
    n=trvalue;
    initialize list=0;
end for
m=new node;
New node trust=t(m)
if (t(m)==trvalue) then
    List=m;
end if
for step1 to step 4 do
    if (t(n)== trvalue) then
        Allow new nodes for transactions.;
    end if
end for
```

Figure 7 illustrates the complete proposed framework. We collect the trust of every 5G network of the IoMT device in Smart hospital devices and store it in an edge computing node(trust manager server) and the cloud. The trust manager maintains an array of trust values for all devices. Using this array, a maximum subarray is created and its value is computed. The threshold value is then calculated by halving the resultant subarray value, saved in the trust manager, and sent to a server known as the miner for dissemination throughout the blockchain network. The trust management calculates a node's trust value whenever another node enters the network and compares it to the threshold amount. The miner receives a fresh node's trust value if it satisfies the threshold and distributes it throughout the blockchain system for additional validation versus the threshold value. If the node's trust value is accepted, it is added to the list of trusted devices. At predetermined intervals, the trust values of all IoMT nodes already in the Smart hospital network are evaluated and stored in the trust manager, and a new threshold value is calculated. This threshold value is then broadcasted to the blockchain network via the miner. Whenever a new threshold value is broadcasted, all listed nodes re-evaluate their trust against the new threshold value, and only those that meet the threshold are allowed to transact within the system. Figure 8 shows The proposed methodology presents a trust management system for secure trust transmission across various floors of smart hospitals using IOMT devices. The system comprises six key components, namely IOMT devices, Trust manager, Miner, Blockchain nodes, Trusted node list, and Key. Patient health data is collected and collated using various IoMT devices, and the trust of these devices is computed and stored in the trust manager and cloud. The trust manager, miner, and blockchain elements compute trust and determine threshold values, while the trusted list stores the data on trustworthy devices. In smart hospitals, the trust limit for IOMT devices is thought to be between -5 and $+10$. The trust data for every IOMT item in the smart healthcare network is first gathered and kept in the server and cloud of the trust management. The trust manager maintains an array of the trust scores of all systems, and a maximum subarray is built from this list to determine the subarray value. The threshold value is then calculated by halving the subarray value, kept in the trust manager, and sent to a miner server for dissemination throughout the blockchain network.

The trust manager system determines a new node's trust value when it enters the network and compares it to the threshold amount. The miner receives the data and distributes it into the network of blockchain nodes for additional verification versus the threshold value if the newly added node's trust value meets the threshold value. The node is added to the group of trustworthy devices if its trust value is approved. The system also generates transaction-related keys for authentication and verification of device legitimacy and digital activity signing based on trust rankings and reputation. These keys enhance the overall security of the system.

At predetermined intervals, the trust values of all IOMT devices in the smart hospital network are evaluated and stored in the trust manager, and a new threshold value is computed.

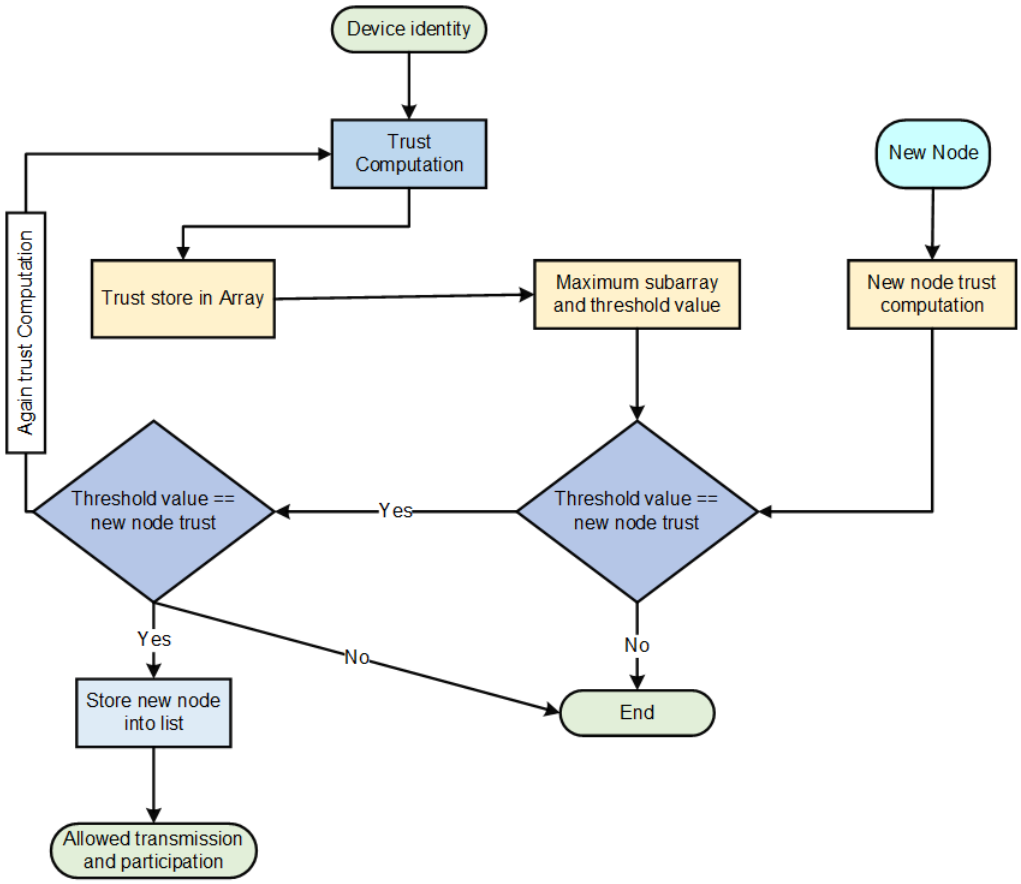


FIGURE 7. Proposed model flow chart.

TABLE 1. Simulation parameter.

Parameters	Values
Simulator	NS 3.29
Simulation Run Time	2.5 hours
Distribution of Nodes	Random topology
Count of all nodes	20 ….100
Compromise Nodes in number	25% to 40 %
Update Period	500s
starting trustworthiness	1.0
Interval of trust	0..1

This threshold value is then broadcasted to the blockchain network via the miner. Whenever a new threshold value is broadcasted, all listed nodes re-evaluate their trust against the new threshold value, and only those that meet the threshold are allowed to transact within the system.

IV. PERFORMANCE EVALUATION

To evaluate the performance of the proposed system, we used a Linux-based OS, Ubuntu 16.04, on an HP Envoy machine core i5 6th generation with 12 GB RAM. We used the famous discrete event network simulator, "NS3" to develop and simulate the proposed solution. Using NS3 and other supporting tools, we developed a smart hospital scenario in which different network devices are connected and the central server. An IoMT in a Smart hospital environment is considered with various Smart network devices ranging from 50, 60, 80,90, and 100. The system randomly spreads the trust in the blockchain network, as the devices are in the same category with shared values or perform the same tasks and operations. Each device is given a number between 0 and 10. These values represent a device's membership in ten established communities of interest within the network. Furthermore, one, two, or three societies can exist simultaneously. The insecure model also contains a range of malicious devices, 20% of all network devices. The behaviour of these devices begins with the start network's lifetime. The suggested model focused on three different types of attacks, which are outlined below:

A. ON-OFF ATTACK IN IoMT

As its name suggests, the malicious node behaves in this situation in a mixed mode of good and harmful. The node can theoretically start an attack using this strategy up until the trust system notices it.

B. BAD MOUTHING ATTACK IN IoMT

A special type of attack is launched by untrusted or compromised nodes that attempt to undermine the reliability of trustworthy devices by issuing false recommendations

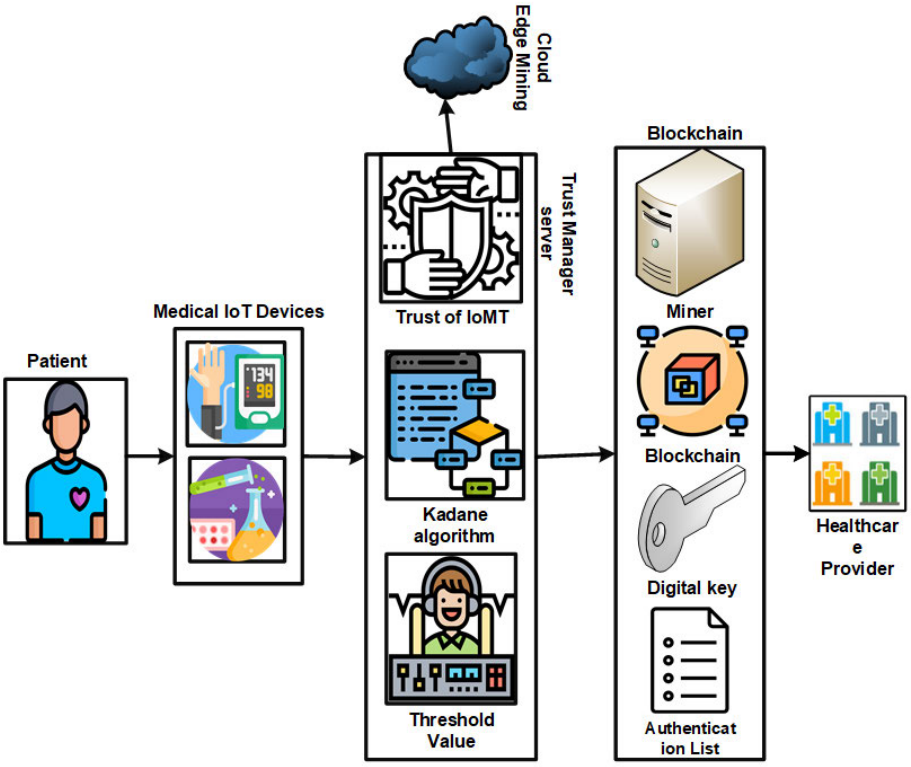


FIGURE 8. Entire system model with all modules and proposed trust management.

against them. This exploit reduces the credibility of trustworthy nodes within an IoMT system implemented in a smart healthcare facility. In one instance, the attackers work together to disparage the target to harm or ruin its reputation. This assault, sometimes referred to as a ''bad-mouthing attack,'' may seriously impair the network's functionality.

C. BALLOT STUFFING ATTACK IN IoMT

By providing them with positive feedback about themselves and raising the likelihood that they would be believed, this strategy, like the previous attack, fosters the growth of further bad nodes.

D. ON-OFF ATTACK IN IoMT

As its name suggests, the malicious node behaves in this situation in a mixed mode of good and harmful. The node can theoretically start an attack using this strategy up until the trust system notices it.

The multi-chain system incorporates miners' functionalities within the blockchain network. The suggested system is tested against different assaults in this part to determine its reliability and efficacy. Three categories are used to categorize the study's findings. First, a test is done to determine how resistant the recommended model is to compromise measures. The efficiency of our blockchain technology data storage and sharing method is then assessed by keeping track of the total transactions, the total number of answers, and the amount of computing resources each mining group employed.

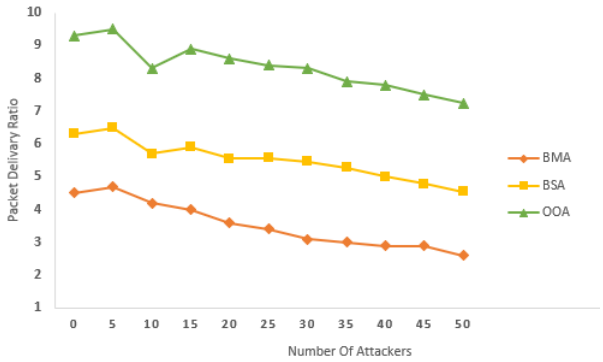


FIGURE 9. Attacks and packet delivery ratio.

E. RESILIENCE IN THE FACE OF ATTACKS

This section investigates how vulnerable our proposed architecture is to attack launches from various IoMT devices against the wireless networks of smart buildings. Figure 9 represents the number of attackers and the packet delivery ratio for all strategies. When the number of attackers grows, more packets are discarded, resulting in a lower packet delivery ratio. Then, by altering the total quantity of infected nodes that launch defamation assaults, we determine the system's overall trust value.

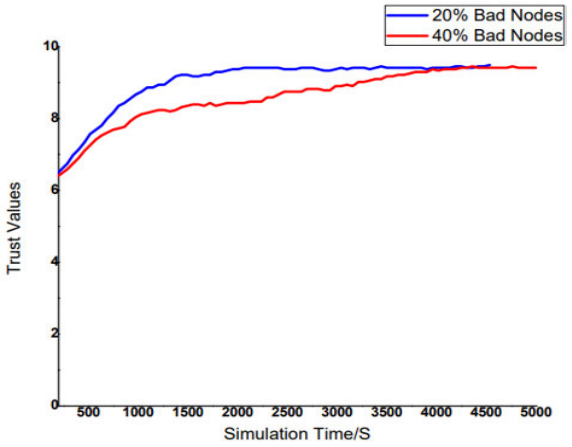


FIGURE 10. Analysis of Well-behaved node trust evolution in IoMT.

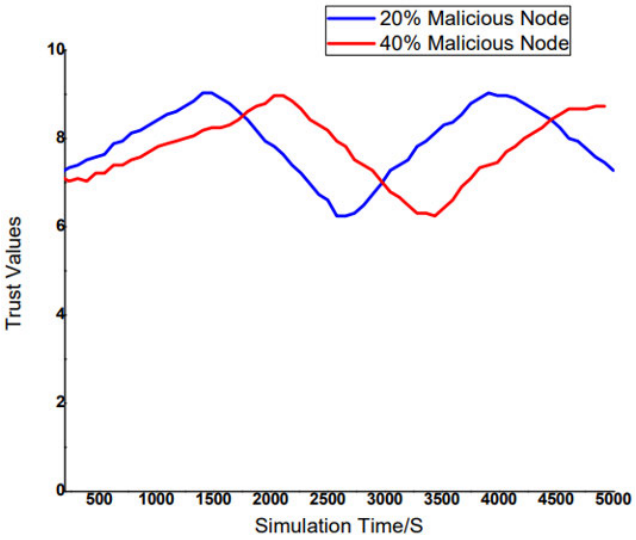


FIGURE 11. Effectiveness of Malicious node trust evolution in IOMT.

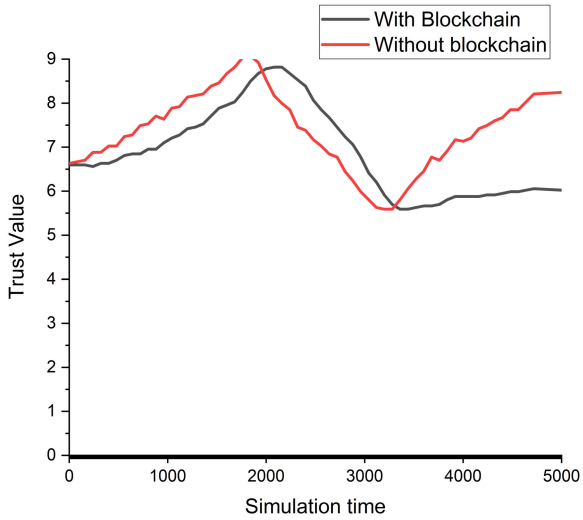


FIGURE 12. Malicious node trust evolution.

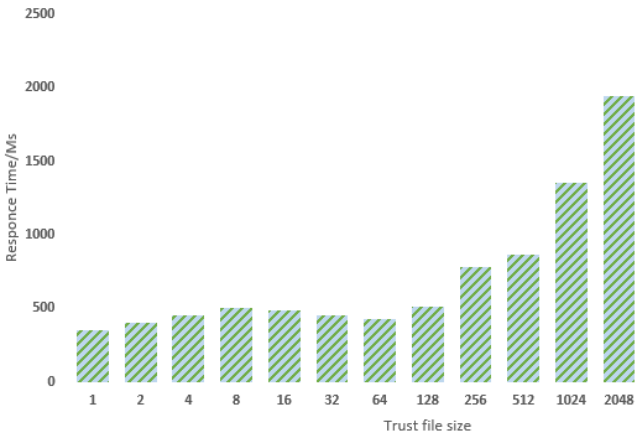


FIGURE 13. Average response time.

Figure 10 examines how a malicious node's trustworthiness is impacted by the proportion of bad nodes that together start On-Off Attacks and ballot stuffing attacks. In an on-off assault, the attacking node switches between efficient and ineffective packet delivery.

To be more specific, the malicious node strives to attain high trust ratings by sending packets at the required intervals. Once its score surpasses 9, it starts to behave poorly, and when it falls below 7, it improves its behavior to increase its trust score. We find that when the ratio rises, trust levels vary, suggesting that more infected nodes work together to support the incorrect node and quickly raise the trust level. This finding relates to the effect of the number of malicious nodes in figure 11.

The findings of accuracy are illustrated in figure 12, Suppose that each node determines a new value based on its preceding and previous trust assessments beginning at time t = the 1800s. The graph demonstrates how blockchain technology might improve a network's reliability and accuracy in the face of On-Off assaults. The traceability function of the blockchain secures, timestamps, and saves trust data within the database for later use. For instance, by keeping an eye on and examining previous trust ratings, we may spot any more harmful behaviour, punish the malicious node, and deter it from obtaining excellent trust values in the future. Additionally, the blockchain penalizes the malicious node if its trust score falls below 7 and it starts acting responsibly again, keeping its score value near 6, thanks to a feature offered by blockchain technology. The percentage of the active store of transactions in the multichain system depends on the amount of trust information. By calculating the ratio of the total quantity of known activities to the total amount of operations that were successfully executed, this was assessed. With an efficient storage transmission rate of 97.55 percent, the suggested method performs well. By changing the file size holding trust information and ratings for each analyzed device in the network, from 1 kilobyte to 2 gigabytes, the response time was evaluated. As illustrated in figure 13, With

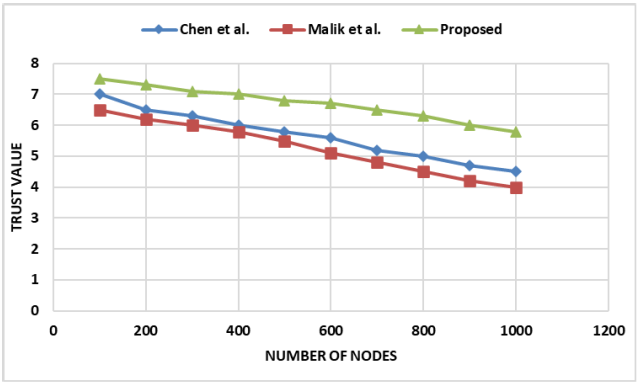


FIGURE 14. Trust computation with nodes.

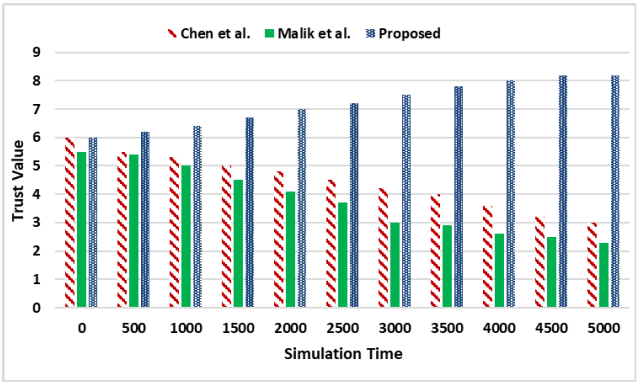


FIGURE 15. Malicious node evaluation.

the length of the trust data list, the blockchain network's average waiting time tends to grow. This is because the blockchain's security features result in a 1937ms latency in a 2Mb trust document. In order to evaluate the efficiency, relevance, and application of the suggested technique in IoMT scenarios.

Figure 14 demonstrates the relationship between the trust value and the number of IoMT nodes. Assume that each node creates a new score based on previous and previous trust ratings. This illustrates how, as compared to older techniques, Blockchain technology may increase a network's reliability and integrity. Trust information may be timestamped and securely stored inside the database for future use thanks to the Blockchain's traceability function.

In Figure 15, the malevolent node's trust value is determined by aggregating the fraction of bad nodes that engage in On-Off Attacks and ballot stuffing attacks. Attacking nodes engage in on-off attacks by alternating between efficient and ineffective packet delivery. To put it more simply, the negative node sends packets for the required amount of time to get high trust ratings.

F. COMPARISON

The data presented in Figure 16 demonstrates that our method outperforms the existing studies by Chen et al. [25],

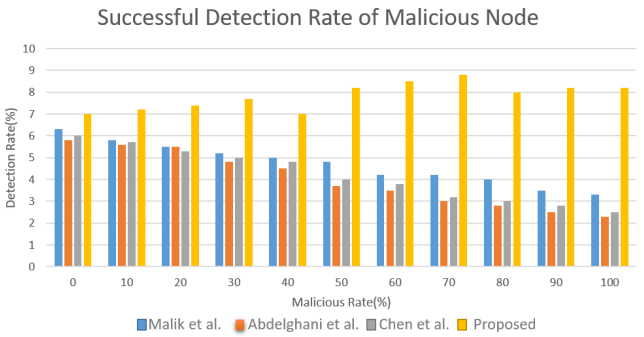


FIGURE 16. Successful detection rate.

Abdelghani et al. [26], and Malik et al. [27] in detecting malicious nodes, even in scenarios where all nodes are malicious. When the malicious rate is 20% or below, the blockchain's trust mechanism operates brilliantly, with a detection rate of 90% and a rate of 99%, respectively. Our two-layer design accomplishes these goals by giving a thorough picture of trustworthiness throughout the network with little communication, allowing it to successfully manage extremely dynamic contexts.

G. LIMITATION

The proposed system utilizes a static threshold value for trust calculation, but it does not mention the disadvantages of using a static threshold value. It may encounter issues in a dynamic environment where trust requirements may change, rendering the static threshold value ineffective. If the number of devices increases, the system may encounter challenges related to scalability, storage, and transactions during network communication. The proposed system does not specifically address the potential scalability challenges. The methodology operates on a hybrid-driven system, incorporating both time-driven and event-driven components. However, it does not specify the time interval in the given study and does not investigate certain criteria related to updates. In the proposed system, the discussion revolves around simple trust management, but it does not explain the concepts of edge and edge state, potentially leading to issues in the proposed system.

H. DISCUSSION

In this part, we evaluated the effectiveness of our suggested solution in terms of reaction time, resilience to on-off and ballet stuffing attacks, and computing power for transaction processing. According to our investigation, our strategy is more resistant to assaults than conventional ones that do not use blockchain. This is because blockchain technology's traceability feature permanently preserves confirmed transactions and trust data within the ledger. Our system can provide a thorough perspective of an entity's past behaviour thanks to this functionality, which can help forecast the future behaviour of malevolent entities launching assaults.

Additionally, we evaluated the response time required to process storage and transactions to demonstrate the usefulness of blockchain technology in this context while upholding our initial architectural objectives. We also demonstrated that this metric remained low even with larger file sizes, confirming the real-time evaluation goal. Although blockchain has not yet been widely used in smart building security, it has been employed to enhance the security of intelligent equipment in buildings. Therefore, our proposed framework contributes to improving the security of the IoMT network in general.

V. CONCLUSION

In IoMT, several medical devices, i.e., ECG, BP, sugar level, and pulse reader are working coherently. These Medical devices are becoming a frequent target for attackers to poison the actual information of the patient. If one device is hacked, the attacker can also pledge to other connecting devices for malicious activities. We just use one blockchain functionality in our example. We must work on several blockchain consensus techniques, such as proof of stake and proof of work. For all the processes, our job takes a little longer. This paper presents the concept and implementation of a robust trust management mechanism that uses Blockchain technologies to gather trust evidence and safely store it in the respective Blockchain nodes. The suggested system offered a more dependable way to compute trust, keep information private, and verify someone's reliability. It also used Blockchain to store and exchange trust data and create a time-stamped record of all transactions and behavior from all entities. Because it is decentralized, maintains security and resistance to diverse threats, and has minimal overhead, the suggested framework is practical, deployable, and appropriate in IoMT contexts.

REFERENCES

[1] Q. Sun, K. Lin, C. Si, Y. Xu, S. Li, and P. Gope, "A secure and anonymous communicate scheme over the Internet of Things," *ACM Trans. Sensor Netw.*, vol. 18, no. 3, pp. 1–21, Aug. 2022.

[2] D. Koundal, B. Sharma, and Y. Guo, "Intuitionistic based segmentation of thyroid nodules in ultrasound images," *Comput. Biol. Med.*, vol. 121, Jun. 2020, Art. no. 103776.

[3] W. Meng, W. Li, and L. Zhu, "Enhancing medical smartphone networks via blockchain-based trust management against insider attacks," *IEEE Trans. Eng. Manag.*, vol. 67, no. 4, pp. 1377–1386, Nov. 2020.

[4] B. Sharma and M. S. Obaidat, "Comparative analysis of IoT based products, technology and integration of IoT with cloud computing," *IET Netw.*, vol. 9, no. 2, pp. 43–47, Mar. 2020.

[5] F. Kamalov, B. Pourghebleh, M. Gheisari, Y. Liu, and S. Moussa, "Internet of Medical Things privacy and security: Challenges, solutions, and future trends from a new perspective," *Sustainability*, vol. 15, no. 4, p. 3317, Feb. 2023.

[6] F. Jamil, M. A. Iqbal, R. Amin, and D. Kim, "Adaptive thermal-aware routing protocol for wireless body area network," *Electronics*, vol. 8, no. 1, p. 47, Jan. 2019.

[7] A. Abbas, R. Alroobaea, M. Krichen, S. Rubaiee, S. Vimal, and F. M. Almansour, "Blockchain-assisted secured data management framework for health information analysis based on Internet of Medical Things," *Pers. Ubiquitous Comput.*, vol. 28, no. 1, pp. 59–72, Feb. 2024.

[8] M. Saeed, R. Amin, M. Aftab, and N. Ahmed, "Trust management technique using blockchain in smart building," *Eng. Proc.*, vol. 20, no. 1, p. 24, 2022.

[9] R. Arul, Y. D. Al-Otaibi, W. S. Alnumay, U. Tariq, U. Shoaib, and M. D. J. Piran, "Multi-modal secure healthcare data dissemination framework using blockchain in IoMT," *Pers. Ubiquitous Comput.*, vol. 28, no. 1, pp. 3–15, Feb. 2024.

[10] M. Ammar, G. Russello, and B. Crispo, "Internet of Things: A survey on the security of IoT frameworks," *J. Inf. Secur. Appl.*, vol. 38, pp. 8–27, Feb. 2018. [Online]. Available: https://lirias.kuleuven.be/retrieve/489458DIoTFrameworksSurvey.pdf

[11] R. Kumar and R. Tripathi, "Towards design and implementation of security and privacy framework for Internet of Medical Things (IoMT) by leveraging blockchain and IPFS technology," *J. Supercomput.*, vol. 77, no. 8, pp. 7916–7955, Aug. 2021.

[12] S. Shivani, S. C. Patel, V. Arora, B. Sharma, A. Jolfaei, and G. Srivastava, "Real-time cheating immune secret sharing for remote sensing images," *J. Real-Time Image Process.*, vol. 18, no. 5, pp. 1493–1508, Oct. 2021.

[13] H. Aldabbas, D. Albashish, K. Khatatneh, and R. Amin, "An architecture of IoT-aware healthcare smart system by leveraging machine learning," *Int. Arab J. Inf. Technol.*, vol. 19, no. 2, pp. 160–172, 2022.

[14] J. M. Khurpade, D. Rao, and P. D. Sanghavi, "A survey on IoT and 5G network," in *Proc. Int. Conf. Smart City Emerg. Technol. (ICSCET)*, 2018, pp. 1–3.

[15] R. U. Rasool, H. F. Ahmad, W. Rafique, A. Qayyum, and J. Qadir, "Security and privacy of Internet of Medical Things: A contemporary review in the age of surveillance, botnets, and adversarial ML," *J. Netw. Comput. Appl.*, vol. 201, May 2022, Art. no. 103332.

[16] D. Guo, S. Gu, J. Xie, L. Luo, X. Luo, and Y. Chen, "A mobile-assisted edge computing framework for emerging IoT applications," *ACM Trans. Sensor Netw.*, vol. 17, no. 4, pp. 1–24, Nov. 2021.

[17] J. Lin, Z. Shen, and C. Miao, "Using blockchain technology to build trust in sharing lorawan IoT," in *Proc. 2nd Int. Conf. Crowd Sci. Eng.*, 2017, pp. 38–43.

[18] B. S. Egala, A. K. Pradhan, V. Badarla, and S. P. Mohanty, "Fortified-chain: A blockchain-based framework for security and privacy-assured Internet of Medical Things with effective access control," *IEEE Internet Things J.*, vol. 8, no. 14, pp. 11717–11731, Jul. 2021.

[19] W. Fang, M. Xu, C. Zhu, W. Han, W. Zhang, and J. J. P. C. Rodrigues, "FETMS: Fast and efficient trust management scheme for information-centric networking in Internet of Things," *IEEE Access*, vol. 7, pp. 13476–13485, 2019.

[20] K. Singh, B. Sharma, J. Singh, G. Srivastava, S. Sharma, A. Aggarwal, and X. Cheng, "Local statistics-based speckle reducing bilateral filter for medical ultrasound images," *Mobile Netw. Appl.*, vol. 25, no. 6, pp. 2367–2389, Dec. 2020.

[21] R. Das, M. Singh, and K. Majumder, "SGSQoT: A community-based trust management scheme in Internet of Things," in *Proc. Int. Ethical Hacking Conf.* Singapore: Springer, 2019, pp. 209–222.

[22] S. R. Khan, M. Sikandar, A. Almogren, I. U. Din, A. Guerrieri, and G. Fortino, "IoMT-based computational approach for detecting brain tumor," *Future Gener. Comput. Syst.*, vol. 109, pp. 360–367, Aug. 2020.

[23] D. Koundal and B. Sharma, "Challenges and future directions in neutrosophic set-based medical image analysis," in *Neutrosophic Set in Medical Image Analysis*. Amsterdam, The Netherlands: Elsevier, 2019, pp. 313–343.

[24] T. Vaiyapuri, A. Binbusayyis, and V. Varadarajan, "Security, privacy and trust in IoMT enabled smart healthcare system: A systematic review of current and future trends," *Int. J. Adv. Comput. Sci. Appl.*, vol. 12, no. 2, pp. 731–737, 2021.

[25] G. Chen, F. Zeng, J. Zhang, T. Lu, J. Shen, and W. Shu, "An adaptive trust model based on recommendation filtering algorithm for the Internet of Things systems," *Comput. Netw.*, vol. 190, May 2021, Art. no. 107952.

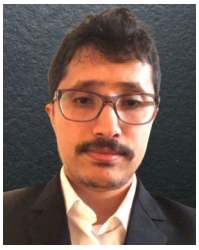
[26] W. Abdelghani, I. Amous, C. A. Zayani, F. Sèdes, and G. Roman-Jimenez, "Dynamic and scalable multi-level trust management model for social Internet of Things," *J. Supercomput.*, vol. 78, no. 6, pp. 8137–8193, Apr. 2022.

[27] S. Malik, V. Dedeoglu, S. S. Kanhere, and R. Jurdak, "TrustChain: Trust management in blockchain and IoT supported supply chains," in *Proc. IEEE Int. Conf. Blockchain*, Jul. 2019, pp. 184–193.

MIMONAH AL QATHRADY (Member, IEEE) received the B.S. degree information systems from King Khalid University, Abha, Saudi Arabia, in 2007, and the M.Sc. and Ph.D. degrees in computer engineering (CE) from the University of Florida (UF), Gainesville, USA, in 2013 and 2020, respectively. Since 2020, she has been working as an Assistant Professor at the Computer Science and Information Systems College, Najran University. Her research interests focuses on the IoT data analysis and modeling, with applications in mobility, encounter and infection tracing, and security, as well as data-driven systems integrating machine and deep learning. She is a member of ACM. She has contributed to various projects, including MobiBench, i-Hospital, and Applying AI in IoT. She was the coordinator of the NOMADS laboratory at UF, and a recipient of the Gartner Group Grad Fellowship award.

MUHAMMAD SAEED received the Graduate degree in computer science from the University of Haripur, Haripur, Pakistan, in 2015, and the M.S. degree in computer science from the University of Engineering and Technology, Taxila, in 2021. He is a Computer Scientist from Pakistan, who has a strong academic background and expertise in a variety of computer science fields. Since January 2019, he has been a Teacher with the Elementary and Secondary Education Department, Khyber Pakhtunkhwa, Pakistan. His research interests include machine learning, the IoMT, and the IoT.

RASHID AMIN received the M.S.C.S. and M.C.S. degrees from International Islamic University, Islamabad, and the Ph.D. degree from COMSATS University Islamabad, Wah Campus. He has been an Assistant Professor with the Department of Computer Science, University of Chakwal, Pakistan. Before this, he was a Lecturer with the Department of Computer Science, University of Engineering and Technology, Taxila, Pakistan, for more than seven years, and the University of Wah, Wah Cantt, Pakistan, for four years. His area of research was hybrid software defined networking. He has supervised many M.S.-level students and five Ph.D. students are working under his supervision. He has published several research papers on hybrid SDN, SDN, clouds, the IoT, and machine learning in well-reputed venues (such as IEEE COMMUNICATION SURVEYS AND TUTORIAL, IEEE ACCESS, IEEE TRANSACTIONS ON ENGINEERING MANAGEMENT, *Sensors*, *Electronics*, AIHC, and CIN). His current research interests include SDN, HSDN, distributed systems, P2P, machine learning, and network security. He has been serving as a Reviewer for international journals (e.g., NetSoft, LCN, Globecom, Fit, IEEE WIRELESS COMMUNICATIONS, IEEE INTERNET OF THINGS JOURNAL, IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, IEEE ACCESS, and IEEE SYSTEMS JOURNAL.



MOHAMMED S. ALSHEHRI received the B.S. degree in computer science from King Khalid University, Abha, Saudi Arabia, in 2010, the M.S. degree in computer science from the University of Colorado at Denver, Denver, USA, in 2014, and the Ph.D. degree in computer science with concentration on information security from the University of Arkansas, Fayetteville, USA, in 2021. He received a Graduate Certificate in cybersecurity from the University of Arkansas, in 2020. His areas of interests include cybersecurity, computer networks, blockchain, machine learning, and deep learning.

ASMA ALSHEHRI received the B.S. degree in computer science from Princess Nourah bint Abdulrahman University, Riyadh, Saudi Arabia, and the M.S. and Ph.D. degrees in computer science from The University of Texas at San Antonio (UTSA). It was her honor to be the first Arabian woman to work and graduate from the Institute for Cyber Security (ICS), UTSA. She is an Assistant Professor of computer science with Prince Sattam Bin Abdulaziz University, Al-Kharj, Saudi Arabia. Her primary area of research includes security and privacy in cyberspace focused on studying foundational aspects of access control and their application in technologies, including cloud computing, the IoT, and big data. She has worked in developing novel security mechanisms, models, and architectures for IoT smart cities, cars, and homes. She is also interested in malware analysis and AI-assisted cybersecurity solutions.

SAMAR M. ALQHTANI received the Ph.D. degree in information technology from the University of Newcastle, Australia. She is currently an Associate Professor with Najran University, Saudi Arabia. She has lectured and developed curricula for courses in computer science and information systems and working to develop quality in the university sector. Recently, she has led and worked on various projects, including event detection applications in social media, medical applications, and applying artificial intelligence and machine learning algorithms to emerging technologies. Her research interest is in information technology and multimedia, including artificial intelligence, machine learning, deep learning, health informatics, data mining, image processing, computer vision, text processing, information security, and internet-oriented IT applications.