Alexandria Engineering Journal (2023) 75, 605–614

Alexandria University

Alexandria Engineering Journal

www.elsevier.com/locate/aej
www.sciencedirect.com

ORIGINAL ARTICLE

A secure emotion aware intelligent system for Internet of healthcare

Geetanjali Rathee [a], **Sahil Garg** [b,*], **Georges Kaddoum** [c,d], **Mohammad Mehedi Hassan** [e]

[a] *Netaji Subhas University of Technology, Dwarka Sector-3, New Delhi 110078, India*
[b] *École de technologie supérieure, Montréal, QC H3C 1K3, Canada*
[c] *Electrical Engineering Department, École de technologie supérieure, Montréal, QC H3C 1K3, Canada*
[d] *Cyber Security Systems and Applied AI Research Center, Lebanese American University, Beirut, Lebanon*
[e] *Department of Information Systems, College of Computer and Information Sciences, King Saud University, Riyadh 11543, Saudi Arabia*

Received 18 March 2023; revised 3 May 2023; accepted 2 June 2023
Available online 15 June 2023

KEYWORDS

Intelligent systems;
Emotion aware;
Blockchain scheme;
Blockchain-based healthcare;
Security;
Trusted intelligent

Abstract Emotional aware intelligent healthcare mechanism is seen as one of the emergent techniques that can be used to overcome the traditional communication issues like storage overhead and delay in transmission process in healthcare systems. It is a smart technique primarily used to ensure faster connectivity and transmission as well as healthcare data processing through various heterogeneous networks by understanding human emotions. Researchers have focused on various processing and transmitting techniques of emotional aware intelligent systems. However, very few of them have focused on the need for security while transmitting or reading the patients' record. The aim of this paper is to propose a secure and transparent communication mechanism in intelligent emotional aware systems using Analytical Hierarchical Process (AHP), blockchain system and a mathematical model. AHP and the mathematical model are used to ensure accuracy during the data transmission process by analysing the legitimacy of each device. In addition, the identity based trust and blockchain mechanism is used to ensure the continuous analysis and transparency among network entities while transferring the information. The proposed framework is further analysed against existing models over various security matrices such as data alteration, report generation, accuracy etc. The out performance of proposed mechanism is approximate 89% as compare to existing mechanism.

1. Introduction

The intelligent wireless systems are being established in almost every field of networking for providing an efficient and

* Corresponding author.
E-mail addresses: geetanjali.rathee123@gmail.com (G. Rathee), sahil.garg@ieee.org (S. Garg), georges.kaddoum@etsmtl.ca (G. Kaddoum), mmhassan@ksu.edu.sa (M.M. Hassan).

Peer review under responsibility of Faculty of Engineering, Alexandria University.

https://doi.org/10.1016/j.aej.2023.06.002
1110-0168

effective communication mechanism. In recent years, e-healthcare practices are emerging on a rapid pace, in turn establishing stronger communication between patients and doctors. The diagnosis consultation and operation of a patient can be easily tackled while understanding their emotional status. The emotional-aware healthcare systems are playing an integral part to develop the same level of trust between patient and intelligent devices in a more efficient, and smooth manner. The emotional aware intelligent system is one of the most promising techniques nowadays to provide an efficient and fast communication in the network while using various Internet-of-Things (IoT) devices [1]. The intelligent medical systems is a type of IoT network that consists of wireless devices connected for the purpose of exchange and transmission of data from medical devices, software applications, health systems and services. The expansion of this technology is driven by the rise of demand in more efficient healthcare systems which are connected and provide a better organization of data and information. The growth of emotional aware intelligent computing has fuelled the drifting of healthcare technologies away from the local clinics to monitor the patients remotely who need it the most, especially during the pandemic scenario. The generation and consumption of data by the healthcare systems from physician's notebooks, nurses' smartphones, sensor-based patient-monitoring tools and other healthcare technologies is made much easier and efficient by intelligent architecture.

Emotional aware computing has also accelerated the advancements in forthcoming accessibility for remote healthcare facilities [2]. Emotional aware systems have blended the high-speed wireless technologies of intelligent computing with real time remote monitoring and analysis, thus providing the capability of improving health outcomes of the patients by boosting accessibility, efficiency and streamlining of communication [3]. However, the IoT-based healthcare faces number of security concerns related to cost ad accuracy while ensuring the security and privacy of information that is being recorded and stored via intelligent devices. In addition, the interoperability scarcity along with multidimensional and heterogeneous e-healthcare data is critical to be maintained in the network.

The issue of security is a major problem faced during wireless communication and transfer of data as various intruders may try to steal a patient's information or may hack into a network to affect its speed, efficiency and security [4]. Further, the communication sensors may be altered by the intruders from legitimate to malicious for degrading the network performance, increasing the congestion or slowing down the information transmission in the network.

1.1. Need of security

The involvement of IoT devices along with the ability of understanding every patient's emotions may further enhance the scope of adopting intelligent healthcare mechanisms in e-healthcare sectors. However, the risk and security perspectives might deter organizations from fully adopting this technique. While adopting any technique, it is a prerequisite for organizations that trust is established and security is provided to their clients in every aspects. The type of risks and security breach such as disclosure of patients' records, stealing and misuse of patients' data or providing patients' information to any third party like insurance providers may further decrease the benefits of e-healthcare sectors. In addition, the involvement of malicious devices while remote monitoring of patients through intelligent devices can be considered as another major issue. How trust can be established among entities while transferring the information on the network is considered as the main focus of this paper.

The below section determines the need for trust based mechanisms in emotional aware healthcare systems.

1.2. Trusted schemes

For ensuring trusted and accurate report generation by various sensors and IoT devices, it is needed to propose some secure methods, schemes and models for healthcare systems [5]. The intruders may alter the generated reports and modify the various consultations and routine care for their own benefits. The altered reports can be further sent to various other organizations or third parties like insurance providers for fulfilling their own interests [6,7]. An efficient and innovative solution is needed in intelligent computing with enabled healthcare systems to tackle various issues such as heterogeneity, e-healthcare and interoperability scarcity issues. In addition, to ensure the accuracy and trust of healthcare data along with faster connectivity while communicating, it is necessary to propose such trust-based models [8–10]. Numbers of security schemes have been proposed by various researchers/scientists in order to ensure secure communication via intelligent sensor nodes. Trust-based cryptographic, encrypted and probabilistic schemes have been proposed by various researchers [11]. However, each technique has its own benefits and limitations while implementing in the network. The existing security schemes lead to additional security costs and management/storage overhead of keys and computational/communicational steps etc [12,13].

1.3. Motivation

Nowadays, blockchain has been emerged as one of the latest and highly secure and transparent smart techniques that ensures the security, accuracy and privacy of data and the system [14]. Blockchain-based mechanisms in intelligent systems are still at their early stages and in healthcare systems they are yet to be fully explored. The blockchain-based intelligent mechanism in healthcare systems can be considered as one of the most accurate trust-based schemes to provide a fast, efficient and secure system while communicating, recording and transmitting various healthcare related information through various heterogenous networks [15]. Fig. 1 depicts the blockchain-based intelligent framework where along with ensuring a fast and efficient connectivity during transmission of messages and texts, blockchain technique also ensures a secure and transparent mechanism for communication and identification of legitimate entities in the network. The intelligent communication system integrated with blockchain mechanism ensures a secure and transparent communication and transmission of patients' record in healthcare management. The depicted Fig. 1 details the overall model of proposed phenomenon where blockchain-based edge-computing mechanism has been used to provide a secure and transparent system in healthcare systems.

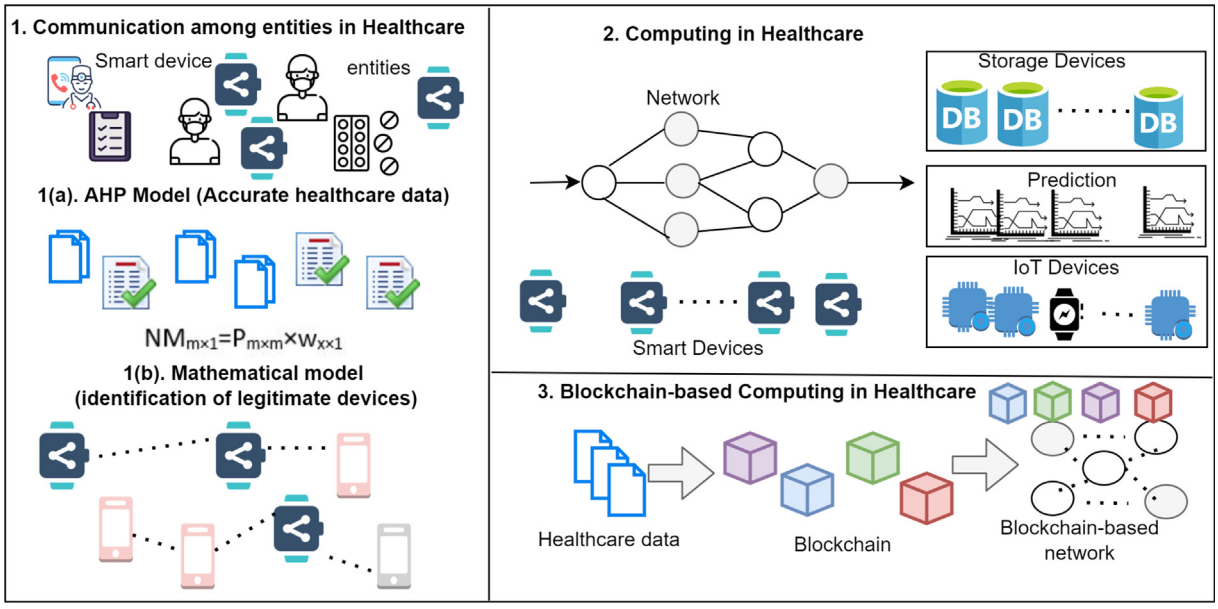

Fig. 1 Blockchain-based Emotion Aware Framework in healthcare systems.

1.4. Contribution

The aim of this paper is to propose a blockchain-based computing system in emotion aware healthcare systems for ensuring secure and trusted data transmission. The Analytical Hierarchical Process (AHP) model is used to provide an accurate transmission of healthcare information between patients and doctors while a mathematical model is used to analyse the legitimacy of each device that is involved in transmitting the information [16,17]. In addition, an identity based trust model and blockchain system is used to ensure the transparency and privacy among communicating entities by continuously verifying or analysing the generated reports by legitimate devices. Any alteration in healthcare data and involvement of malicious devices may immediately be known by other sensors and can be traced to tackle the issue at once.

The remaining organization of the entire manuscript is detected as follows. The number of trust-based intelligent scheme for healthcare systems discussed by several authors are detailed in Section 2. The proposed AHP, mathematical model along with blockchain mechanism is explained in Section 3. In addition, Section 4 determines the results and performance analysis of proposed phenomenon along with the comparison of existing schemes. Finally, Section 5 concludes and redirects the future scope of the paper.

2. Related work

Number of authors have proposed various security related approaches such as cryptographic, encrypted, artificial intelligence and blockchain based mechanism in wireless systems. The number of security approaches for edge-based computation specific to healthcare systems using blockchain technique is still at its early stages. This section describes the number of security schemes proposed by various scientists/engineers using blockchain or any other security methods for ensuring a secure healthcare information and identifying the legitimate communicating entities in the network using edge-based computing in healthcare systems.

Zhang et al. [18] have proposed a novel medical platform that monitored and provided decision making by considering emotions. The authors have experimented the results against various mainstream models. The authors claim that the proposed cognitive-based dynamic mechanism can be accommodated for various applications like COVID-19. Chiu et al. [19] have proposed a deep neural network by introducing a Chinese word embedding system. The authors have classified the input using convolutional neural network by converting the input into spectrogram. The proposed phenomenon provided the voice response interface presented through App mode.

Meng et al. [20] have proposed a blockchain based trust management system for medical applications by exploring various insider attacks. The authors have explored the healthcare system by demonstrating the blockchain mechanism identifying malicious devices having workloads. Akkaoui [21] has proposed a contract-based authentication mechanism for identifying the legitimate IoT devices in medical systems. The author has explored various security threats including denial of service, anonymity and confidentiality including blockchain mechanism. The author has implemented the proposed framework using Ethereum by evaluating communication and computation costs. Du et al. [22] have proposed an optimized blockchain mechanism for sharing the information among various entities in medical systems. By exploring the benefits of blockchain mechanism, the authors have improved the security while sharing and recording various information among several users in the network. In addition, Lockl et al. [23] have proposed a trust-based ecosystem using blockchain mechanism where the authors have improved the availability and integrity of data for monitoring the data. Gao et al. [24] have proposed blockchain based intelligent framework to ensure the confidentiality of healthcare data processing. The blockchain based scenario provided the authenticity among cloud services and healthcare systems devices for accessing or managing the data.

Table 1 Related work discussion.

Author	Approach	Technical Contribution	Limitation
Meng et al. [20]	blockchain based trust management system for medical applications	The authors have explored the healthcare system by demonstrating the blockchain mechanism for identifying malicious devices having workloads	The proposed scheme causes delay while transmission the information
Akkaoui et al.[21]	Contract based authentication mechanism	The author has implemented the proposed framework using Ethereum by evaluating communication and computation costs	The proposed mechanism may delay the data encryption and increased data computation
Du et al. [22]	Optimized blockchain scheme	The authors have proposed an optimized blockchain mechanism for sharing the information among various entities in medical systems	The proposed scheme has not considered the malicious devices
Lockl et al. [23]	Trusted ecosystem	The authors have proposed a trust-based ecosystem using blockchain mechanism where the authors have improved the availability and integrity of data for monitoring the data	The proposed scheme delayed the data transmission process
Gao et al. [24]	Blockchain based intelligent framework	The proposed framework used the Hyperledger and SGX technology for predicting the analysis of the proposed framework performance	The author has not focused on the malicious devices for ensuring a secure communication
Sun et al. [25]	Timely analysis and processing of the healthcare data	The authors have discussed the future possibilities and challenges of combining the artificial intelligence and edge-cloud computing in healthcare systems	The proposed mechanism may lead to computational overhead
Nandy et al. [26]	Swarm-Neural network scheme	The proposed mechanism is analyzed over real-time data dataset by classifying the various performance models and their metrics	The proposed phenomenon may lead to analysis delay while transmitting the communication

Further, the proposed framework used the Hyperledger and SGX technology for predicting the analysis of the proposed framework performance. Sun et al. [25] have surveyed the need of timely analysis and processing of the healthcare data under the constraints of traditional healthcare equipment's and environments. The authors have focused on various benefits of combining intelligent, cloud computing and artificial intelligent techniques in healthcare systems. In addition, the authors have also explored the privacy and security of the healthcare data while providing high quality services to the patients. Further the authors have discussed the future possibilities and challenges of combining the artificial intelligence and edge-cloud computing in healthcare systems.

Nandy et al. [26] have proposed a secure Swarm-Neural network scheme for identifying the threats during analysis and transmission among devices in the network. The proposed mechanism is analyzed over real-time data dataset by classifying the various performance models and their metrics. The authors claimed the 99.5% accuracy using Swarm-neural strategy against Traditional neural network datasets. Nguyen et al. [27] have proposed a decentralized blockchain based intelligent framework for ensuring a secured data sharing and collection in distributed networks. The authors have designed a data sharing scheme for exchanging the healthcare information by interplanetary and leveraging the file systems. In addition, the authors have used a contract-based authentication scheme for verifying the users without any central authority. The proposed mechanism is analyzed against security, privacy and quality of service metrics against existing methods. Parah et al. [28] have proposed an encryption mechanism using left data mapping and check computation schemes. The RC4 algorithm is used to chunk the larger data into 3-bits by converting them into decimal devices. In addition, the decimal digits are analyzed through checksums for localization and detection of diagonal pixels. The experimental results of proposed framework are analyzed in terms of computational complexity, payload, capability to localize and identify the tampered data and so on. Further, the proposed scheme claimed the potential improvement in authentication and security of healthcare systems data over traditional schemes.

Rahman et al. [29] have developed a deep learning based diversified health-related information for identifying the COVID19 generated symptoms and reports for the support of accurate medical decisions. Number of COVID19 based applications have been proposed, tested, developed and deployed in order to support clinical trials. The authors have designed a framework and detailed explanation of proposed framework with various accurate results in terms of verifying the suitability of health management systems during this pandemic. Lin et al. [30] have proposed a resource allocation and computational offloading processing system to resist various malevolent threats. In order to reduce the virtual devices and computational loading service, the authors have formulated a Markov decision issue by involving the content, block consensus and learning schemes to allocate the suitable number of resources. The proposed framework is simulated against convergence rate, stalling rates and energy consumption by demonstrating the efficiency and effectiveness of proposed phenomenon. Table 1 describes the number of secure and trust based approach for healthcare and healthcare systems mechanisms along with their limitations.

2.1. Research gap

Though number of security mechanisms and approaches have been proposed by various scientists and researchers, however, the existing mechanisms leads to various security and privacy issues. The transmission delay, storage overhead, data de-duplication, increased computation leads to huge loss in the overall performance of the network. In order to overcome

the above-mentioned limitations. The aim of this paper is to highlight the research significance by proposing a transparent and secure transmission mechanism using blockchain networks. In addition, the AHP model is integrated in order to further analyze the legitimacy and trust of the communicated devices.

3. Proposed framework

3.1. System/state model

The surveillance analysis may facilitate the management of trust in healthcare. The proposed mechanism elaborates a secure designing architecture/framework by applying trusted decision schemes and mathematical models. The proposed system model consists of three different layers: (1) The visual representation of various objects such as person, house, road etc. (2) The security protocols applied in sensors such as mathematical modelling for identifying the legitimacy of ideal nodes and decision scheme (AHP) to take appropriate decision during run time exchange of information (3) The cloud servers having blockchain network such as databases for storing the online record of each activity. Every object is analysed and sensed by several smart IoT devices where legitimacy is identified by defining the trust of each such device. There exist n numbers of IoT sensors which all are assumed to be trusted at the time of network deployment. In addition, the legitimacy of each IoT sensor is decided or analyzed depending upon its trust value. The trust of each IoT device is measured using a mathematical model whereas the decision for allowing further communications/ transmissions in the network is taken via an AHP.

3.2. Mathematical model for identifying the trust of each IoT device

For generating a mathematical model and validating the proposed phenomenon, some randomly generated malicious IoT devices (MID's) are deployed in the network. The main aim of randomly generated MID's is to (1) forge the ideal device legitimacy or (2) to create the illegal activities inside the network by providing huge number of false messages/requests. The intruder may perform active attacks such as denial of service, network congestion, network delay or passive threats such as address forging, network traffic recognition, data falsification and so on.

The generation of any passive/active threats inside the network leads to less trusted value by the authority to that IoT sensor. In addition, each New IoT Sensors (NIS) added inside the network needs to prove the authenticity to the centralized authority (CA). If new IoT sensor is ideal then it may perform ideal number of activated having acceptable Trust Values (TV) inside the network, however the malicious NIS is easily identified whenever a sensor node starts generating huge number of requests and identified less TV in the network. The computed TV based upon their internal communication behaviour, there exist four different networking scenarios for both MID and Legitimate IoT devices (LID) in the network such as i) H_{a0} that states the absence of both MID and LID means none of them approaches centralized authority to prove their authenticity. ii) H_{a1} where LID becomes active inside the network and needs authenticity approval from CA. iii) H_{a2} where the MID tried to replicate LID with the aim of network performance degradation and at last iv) H_{a3} where both MID and LID tried to prove their legitimacy inside the network. The number of equations generated by above stated conditions is written in equation as (1):

$$\begin{aligned} H_{a0} &= \text{neither LID nor MID}, \\ H_{a1} &= \text{LID, contact to CA}, \\ H_{a2} &= \text{MID, contact to CA only}, \\ H_{a3} &= \text{Both MID and LID contact to CA}. \end{aligned} \tag{1}$$

In addition, the absence and presence of MID is denoted through MID^{off} and MID^{on} respectively where the probability of each hypothesis H_{γ_k} is represented through γ_k as defined in Eq. (2):

$$\begin{aligned} \gamma_0 &= P(H_{a0}) = P(H_0), MID^{off} = P(MID^{off}/H_0)P_{H0,} \\ \gamma_1 &= P(H_{a1}) = P(H_1), MID^{off} = P(MID^{off}/H_1)P_{H1,} \\ \gamma_2 &= P(H_{a2}) = P(H_0), MID^{on} = P(MID^{on}/H_0)P_{H0,} \\ \gamma_3 &= P(H_{a3}) = P(H_1), MID^{on} = P(MID^{on}/H_1)P_{H1} \end{aligned} \tag{2}$$

Moreover, the respective attacking strategies mathematical model upon presence and absence of MID using an attacking metrics and are defined as: $\delta = P\frac{MID_{on}}{H_1}$ and $\delta = P\frac{MID_{on}}{H_0}$. The above stated equations according to previously defined equations are rewritten as Eq. (3):

$$\begin{aligned} \gamma_0 &= (1-\theta)P(H_0), \\ \gamma_1 &= (1-\delta)P(H_1), \\ \gamma_2 &= \theta P(H_0), \\ \gamma_3 &= \delta P(H_1). \end{aligned} \tag{3}$$

Further, if α_m and α_f represents the non-identification and false legitimate probabilities at CA respectively, then it can be again rewritten in the form of $\alpha_m = P(D_{off/MID^{on}}, \alpha_f = P(D_{on/MID^{off}}$, where D_{on} and D_{off} where D_{off} and D_{on} are the CA's decision based upon the absence and presence of MID in the network.

3.3. Decision Making Model (AHP)

An analytical hypothetical process is used while identifying the trusted nature of each IoT sensor upon visualizing the mobility of each device. The AHP approach is applied after mathematical modeling of proposed phenomenon in order to improve the decision-making process while computing the trust of each sensor. Initially, a random weight is assigned to each device that is further increased depending upon certain measuring criteria. The below steps determine the further weights evaluation strategy using AHP.1. Start with generating a pair-wise matrix comparison through relative importance of P_m measuring parameters. While there are P_m measuring parameter and $P_{(mm)}$ will be defined as the pair-wise comparison of x^{th} alternative with y^{th} criteria. However, P_{xy} determines the relative importance of alternative x with respect to y criteria.

In addition, weights W_x are determined upon analyzing the mean of x^{th} rows (systematically and normalized).

The W_x is further validated from step (2) by computing normalized metric (NM) matrix as:

$$NM_{m\times 1} = P_{m\times m} \times W_{x\times 1} \tag{4}$$

Further, the relative NM matrix as $RNMP_{(m1)} = NM_{(m1)}/W_{(m1)}$.

Moreover, the maximum eigen values EV_{max} is identified as the average of $RNMP_{(m1)}$ as consistency Index (CI) as $(EV_{max-m})/(m-1)$.

Finally, the RI (random index) is computed as the ratio of CI/RI.

3.4. Identity based trust

The trust should be maintained while transmitting or sharing the information among various entities in the network. The blockchain based system ensures transparency, however, to fasten the validation mechanism, trust can be further analyzed or evaluated of every authenticated/verified entity. The validation score VS (V_i) is used to quantify the trustworthiness/legitimacy of devices. The source node S_i that wishes to start communication has high trust values (i.e. set to 1) and the devices from where the message transmitted may have any random trust values. Now, the newly created devices that joined intentionally and registered disseminate trust information to degrade the network performance. The registered age of S_i can not be modified artificially and is relatively very difficult to mold by intruders. The older the registration age, the more trustable a device is. The trust can be now computed as registered age score as:

$$RAS_{S_i} = \frac{R_{S_i} - \mu_R}{\sigma_R} \tag{5}$$

where R_{S_i} is registration age of score S_i, μ_R is average registration age of all devices and σ_R defines standard deviation of registration age of all the devices. The larger number of historical transaction of a source S_i reflects its trustworthiness and popularity. A large number of transaction history of a source commonly implies more users trust. The transaction history of S_i denoted as $TH(S_i)$ can be evaluated as:

$$TH(S_I) = \frac{log(TransH(S_i)+1)}{log(max_{s_i \epsilon (TransH(S_i))+1)}} \tag{6}$$

Further, the verification score of source S_i according to page rank algorithm can be evaluated as:

$$VS(S_i) = d \times \sum_{S_j(i)} \frac{VS(S_j)}{TransH(S_j)} + \frac{1-T}{N} \tag{7}$$

Where, $TransH(S_i)$ is set of information source S_i and $TransH(S_j)$ is number of source S_j entities. N is the total number of devices and $T \epsilon (0,1)$. The below Algorithm 1 determines the identity based trust along with blockchain mechanism. The presented Algorithm 1 illustrates the communication among legitimate devices along with providing the transparency while transmitting the information among each other.

Algorithm 1. Identity based Trusted Blockchain Algorithm

Algorithm 1: Identity based Trusted Blockchain Algorithm

Require: Device 'D', network 'N', set of source's profile information
Ensure: Source's based trust
Input Value: (1) Number of smart devices sd, (2) category of devices (altered and ideal)
Output: Device is either ideal or malicious
Step 2: Every smart device sd having their own identity known as $Trust$ value.
Step 3: The identity based trust values and blockchain mechanisms are used to ensure the legitimacy of the communicating (source) device
for $each S_i \epsilon S$ **do**
  if $S_i is validated and part of blockchain$ **then**
    $VS(S_i) = 1$
  else
    $VS(S_i) \epsilon (0 - 0.9)$
  end
  Cal. $RAS(S_i)$ using Eq. (3)
  cal. $TransH(S_i)$ using Eq. (4)
  Cal. validation score (VS_I) using Eq. (5)
  $IT_i =$
   $VS(S_i) + RAS(S_i) + TransH(S_i) + VS(S_i)/4$
end

3.5. Blockchain-based intelligent Framework

The decision making and mathematical model are further used to ensure the security and legitimacy of each and every communicating entity in the network that can be further traced using blockchain network.

The Analytical Hierarchical Model (AHP) model is used to provide an accurate transmission of healthcare information among patient, doctors and other staff while mathematical model is used to analyses the legitimacy of each device that is involved while transmitting the information. In addition, blockchain system is used to ensure the transparency and privacy among communicating entities by continuously verifying or analyzing the generated reports by legitimate devices. Any alteration in healthcare data and involvement of malicious devices may immediately know by other sensors and can be traced and tackle the issue at once. The flow of the proposed mechanism is represented through Fig. 2 which presents a blockchain-based computing scenario where each and every block contains the smart devices which are being traced regu-

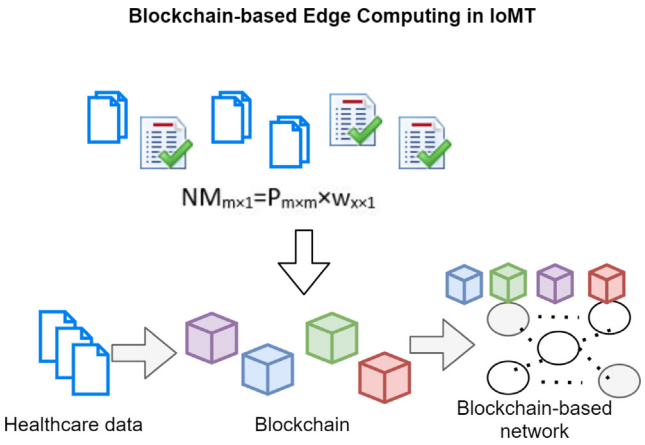

Fig. 2 Proposed Blockchain-based intelligent Framework in healthcare systems.

larly in order to ensure a transparent and legitimate communication mechanism in the network. The depicted Fig. 2 integrates the healthcare system with blockchain mechanism where each and every record of patient, doctors prescription, tests, and medical history is kept secret and transparent among doctor and patient using blockchain network. A single alteration in any block can be immediately known by the remaining entities and blocked for future communications in the network. In order to validate the proposed mechanism, the ideal and adversary model is considered where number of malicious objects are included during the communication process in the network.

3.6. Ideal model

An ideal model as depicted in Fig. 3 (a) having legitimate number of IoT sensors are present inside the network for performing message transmission and sharing of information among each other. The number of nodes that considered for analyzing, sensing and monitoring the visual objects is defined as ideal IoT sensors and has a sufficient TV above a specified threshold value in the network.

3.7. Adversary model

In the adversary environment as depicted in Fig. 3 (b), malicious IoT sensors are present inside the network to further validate the communication process inside the network. Upon transmission, sensing, monitoring and controlling of information from several IoT sensor, intruders have deployed various types of threats such as data falsification, denial of service, black hole threat by compromising few IoT sensors. In order to further validate the proposed phenomenon over both ideal and adversarial nature, the compromised IoT sensors are deployed at a rate of 0–5% upon increasing the network size in the environment. Further, the number of objects is moving from one place to another that are sensed and controlled by many ideal and adversarial number of sensor nodes and are analysed through mathematical modelling and AHP decision rules.

4. Performance analysis

4.1. Baseline method

The proposed mechanism is validated over a heterogeneous network against Gao et al. [24] and Sun et al. [25] where they tried to propose a trustworthy VIoT by enabling multistage perception scheme to extract the contextual data. Gao et al. [24] have constructed 2-path data propagation from difference and similarity of group images and finally projected a stage-wise refinement for learning the semantic information. In addition, Sun et al. [25] have surveyed the need of timely analysis and processing of the healthcare data under the constraints of traditional healthcare equipment's and environments. The authors have focused on various benefits of combining intelligent, cloud computing and artificial intelligent techniques in healthcare systems. In addition, the authors have also explored the privacy and security of the healthcare data while providing high quality services to the patients.

4.2. Implementation setup

It is very crucial to identify the trust based IoT sensors in visual-IoT environment, therefore, to validate the proposed

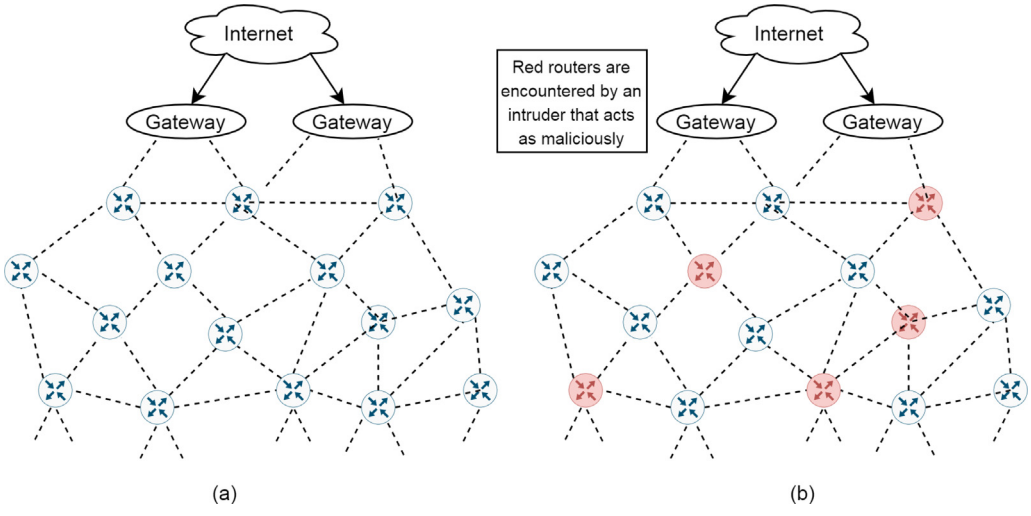

Fig. 3 Ideal Vs Adversary Network Model.

trust-based phenomenon we have simulated the results over synthesized data. Table 2 represents the abstract view of the test bed having major links and components. The numbers of nodes are running over NS2 simulator with predefined trust values and IoT devices.

4.3. Performance metrics

Initially, 1000 devices are deployed in the network that is further updated by adding more devices in the network after every minute. Along with that various malicious device are inserted

Table 2 Simulation environment.

Nodes	Edges Devices	Levels	Activity	Threat Possibility
50	5	15	Malicious devices insertion	15
100	10	25	Handoff Process	10
150	15	45	Conversion of malicious during handoff	15

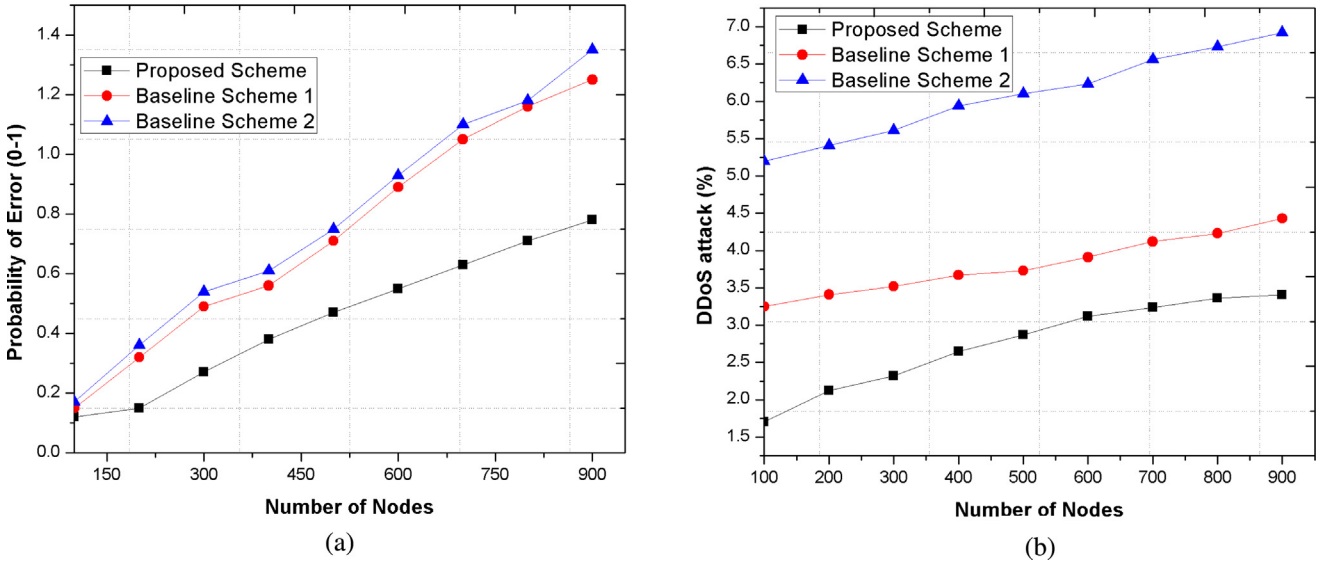

Fig. 4 a. Probability of Error, b. DDoS Attack.

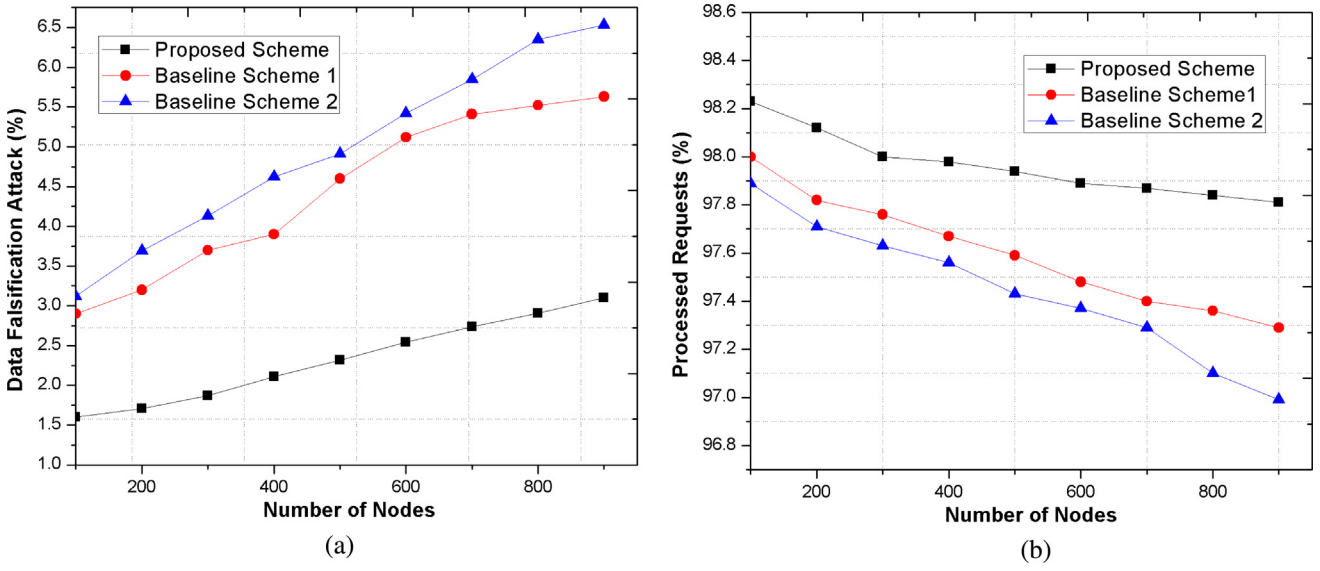

Fig. 5 a. Data Falsification Attack, b. Processed Request.

to analyze or validate the further results. The simulation environment table is further added as Table 2 in performance analysis section where total number of nodes including edge devices, levels, activity and threat possibility detailed the overall structure of the paper. The below Fig. 4 (a) depicts the probability of error occurred from each environment using probability distribution as represented in Table II. The probability of error in case of proposed mechanism as represented in Fig. 4 (a) can be well identified because of mathematical model that detects the involvement of malicious number of nodes involved during communication in the network. The shown Fig. 4 (b) elaborates that MID can't be fully identified and removed from the system upon increasing the number of nodes in the network. However, the proposed mechanism may successfully identify the various numbers of malicious nodes in the network that leads to improved resource utilization.

Further, Fig. 5 (c), Fig. 5 (d) represents the data falsification threat and number of processed requests of proposed and baseline mechanism. It can be predicted from depicted figures where as the number of nodes are increasing, the proposed mechanism performs better as compare to conventional schemes. The mathematical model along with blockchain mechanism ensures a secure and transparent identification and continuous surveillance of proposed framework as compare to existing schemes.

4.4. Discussion of results

The proposed trusted mechanism using decision making and mathematical model is evaluated against various edge and sensor nodes by customizing a synthesized test bed. The evaluation of experimental conduction is successful by recording variety of measuring parameters. The system state along with implementation set up and performance results are defined in section B and section C. The evaluated simulated results were generating positive impact against all the mentioned parameters. In addition, around 87% accuracy in proposed scheme improvement has been recorded with the presence of various malicious numbers of nodes. The two-stage based analysis of trusted results using mathematical and decision modelling results based upon removal and identification of MID in blockchain-based intelligent environment. Overall, the proposed mechanism achieves better and desired results over several numbers of nodes in the network.

5. Conclusion

This paper has proposed a secure, transparent and trusted blockchain-based computing scheme for ensuring secure transmission and communication in emotional aware healthcare systems. The proposed framework used AHP, a mathematical model, identity based trust model and blockchain mechanism to ensure a transparent and secure system. The proposed phenomenon efficiently provides faster, accurate, transparent and more secure communication by understanding human emotional behavior. The generated results are compared against existing schemes over various security metrics such as data alteration, report generation, accuracy etc to show the outperformance of the proposed scheme. The proposed mechanism presents 89% improvement as compare to existing mechanism over various security metrics.

The number of dynamic generated attacks while analysing the data alteration through heterogeneous networks may be considered as the future scope of this paper.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgement

This work was supported by the King Saud University, Riyadh, Saudi Arabia, through the Researchers Supporting Project under Grant RSP2023R18.

References

[1] W.Z. Khan, E. Ahmed, S. Hakak, I. Yaqoob, A. Ahmed, intelligent: a survey, Future Gener. Comput. Syst. 97 (2019) 219–235.
[2] T. Han, L. Zhang, S. Pirbhulal, W. Wu, V.H.C. de Albuquerque, A novel cluster head selection technique for edge-computing based healthcare systems systems, Comput. Netw. 158 (2019) 114–122.
[3] G. Rathee, A. Sharma, H. Saini, R. Kumar, R. Iqbal, A hybrid framework for multimedia data processing in IoT-healthcare using blockchain technology, Multimedia Tools Appl. 79 (15) (2020) 9711–9733.
[4] G. Rathee, F. Ahmad, F. Kurugollu, M.A. Azad, R. Iqbal, M. Imran, CRT-BIoV: a cognitive radio technique for blockchain-enabled internet of vehicles, IEEE Trans. Intell. Transp. Syst. (2020).
[5] G. Rathee, N. Jaglan, R. Iqbal, S.P. Lal, V.G. Menon, A trust analysis scheme for vehicular networks within IoT-oriented green city, Environ. Technol. Innov. 20 (2020) 101144.
[6] Z. Zhu, T. Dumitras, Chainsmith: Automatically learning the semantics of malicious campaigns by mining threat intelligence reports, in: 2018 IEEE European Symposium on Security and Privacy (EuroS&P), IEEE, 2018, pp. 458–472. April.
[7] B.Z.H. Zhao, M. Ikram, H.J. Asghar, M.A. Kaafar, A. Chaabane, K. Thilakarathna, A decade of mal-activity reporting: A retrospective analysis of internet malicious activity blacklists, in: Proceedings of the 2019 ACM Asia Conference on Computer and Communications Security, 2019, July, pp. 193–205.
[8] A.H.M. Aman, W.H. Hassan, S. Sameen, Z.S. Attarbashi, M. Alizadeh, L.A. Latiff, healthcare systems amid COVID-19 pandemic: Application, architecture, technology, and security, J. Network Comput. Appl. 102886 (2020).
[9] A. Ghubaish, T. Salman, M. Zolanvari, D. Unal, A.K. Al-Ali, R. Jain, Recent advances in the internet of medical things (healthcare systems) systems security, IEEE Internet of Things Journal. (2020).
[10] M. Papaioannou, M. Karageorgou, G. Mantas, V. Sucasas, I. Essop, J. Rodriguez, D. Lymberopoulos, A survey on security threats and countermeasures in internet of medical things (healthcare systems), Transactions on Emerging Telecommunications Technologies e4049 (2020).
[11] X.A. Wang, J. Ma, F. Xhafa, M. Zhang, X. Luo, Cost-effective secure E-health cloud system using identity based cryptographic techniques, Future Generation Computer Systems 67 (2017) 242–254.
[12] E. Tromp, M. Pechenizkiy, M.M. Gaber, Expressive modeling for trusted big data analytics: techniques and applications in sentiment analysis, Big Data Analytics 2 (1) (2017) 1–28.

[13] G. Rathee, S. Garg, G. Kaddoum, B.J. Choi, Decision-making model for securing IoT devices in smart industries, IEEE Trans. Industr. Inf. 17 (6) (2020) 4270–4278.
[14] G. Rathee, M. Balasaraswathi, K.P. Chandran, S.D. Gupta, C. S. Boopathi, A secure IoT sensors communication in industry 4.0 using blockchain technology. Journal of Ambient Intelligence and Humanized, Computing 12 (1) (2021) 533–545.
[15] D. Efanov, P. Roschin, The all-pervasiveness of the blockchain technology, Procedia computer science 123 (2018) 116–121.
[16] M. Dağdeviren, İ. Yüksel, Developing a fuzzy analytic hierarchy process (AHP) model for behavior-based safety management, Information sciences 178 (6) (2008) 1717–1733.
[17] G. Rathee, S. Garg, G. Kaddoum, B.J. Choi, Decision-making model for securing IoT devices in smart industries, IEEE Trans. Industr. Inf. 17 (6) (2020) 4270–4278.
[18] T. Zhang, M. Liu, T. Yuan, N. Al-Nabhan, Emotion-Aware and Intelligent Internet of Medical Things Toward Emotion Recognition During COVID-19 Pandemic, IEEE Internet of Things Journal 8 (21) (2020) 16002–16013.
[19] P.S. Chiu, J.W. Chang, M.C. Lee, C.H. Chen, D.S. Lee, Enabling intelligent environment by the design of emotionally aware virtual assistant: A case of smart campus, IEEE Access 8 (2020) 62032–62041.
[20] W. Meng, W. Li, L. Zhu, Enhancing medical smartphone networks via blockchain-based trust management against insider attacks, IEEE Trans. Eng. Manage. 67 (4) (2019) 1377–1386.
[21] R. Akkaoui, Blockchain for the Management of Internet of Things Devices in the Medical Industry, IEEE Trans. Eng. Manage. (2021), https://doi.org/10.1109/TEM.2021.3097117.
[22] M. Du, Q. Chen, J. Chen, X. Ma, An optimized consortium blockchain for medical information sharing, IEEE Trans. Eng. Manage. (2020), https://doi.org/10.1109/TEM.2020.2966832.
[23] J. Lockl, V. Schlatt, A. Schweizer, N. Urbach, N. Harth, Toward trust in Internet of Things ecosystems: Design principles for blockchain-based IoT applications, IEEE Trans. Eng. Manage. 67 (4) (2020) 1256–1270.
[24] Y. Gao, H. Lin, Y. Chen, Y. Liu, Blockchain and SGX-enabled intelligent Empowered Secure healthcare systems Data Analysis, IEEE Internet of Things Journal. (2021).
[25] L. Sun, X. Jiang, H. Ren, Y. Guo, Edge-cloud computing and artificial intelligence in internet of medical things: Architecture, technology and application, IEEE Access 8 (2020) 101079–101092.
[26] S. Nandy, M. Adhikari, M.A. Khan, V.G. Menon, S. Verma, An Intrusion Detection Mechanism for Secured healthcare systems framework based on Swarm-Neural Network, IEEE Journal of Biomedical and Health Informatics. (2021).
[27] D.C. Nguyen, P.N. Pathirana, M. Ding, A. Seneviratne, BEdgeHealth: a decentralized architecture for edge-based healthcare systems networks using blockchain, IEEE Internet Things J. (2021).
[28] S.A. Parah, J.A. Kaw, P. Bellavista, N.A. Loan, G.M. Bhat, K. Muhammad, A. Victor, Efficient security and authentication for edge-based internet of medical things, IEEE Internet of Things Journal. (2020).
[29] M.A. Rahman, M.S. Hossain, An Internet of medical things-enabled intelligent framework for tackling COVID-19, IEEE Internet Things J. (2021).
[30] P. Lin, Q. Song, F.R. Yu, D. Wang, L. Guo, Task offloading for wireless VR-enabled medical treatment with blockchain security using collective reinforcement learning, IEEE Internet Things J. (2021).