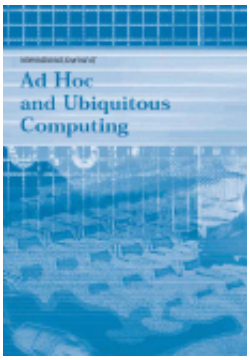


International Journal of Ad Hoc and Ubiquitous Computing

ISSN online: 1743-8233 - ISSN print: 1743-8225
https://www.inderscience.com/ijahuc

A trusted and adaptive security mechanism for wearable e-healthcare systems

Geetanjali Rathee, Hemraj Saini, Shishir K. Shandilya, S. Rajasoundaran

DOI: 10.1504/IJAHUC.2023.10052372

Article History:

Received:	23 July 2022
Accepted:	13 October 2022
Published online:	18 January 2024

A trusted and adaptive security mechanism for wearable e-healthcare systems

Geetanjali Rathee

Department of Computer Science and Engineering,
Netaji Subhas University of Technology,
Dwarka Sector-3, New Delhi, India
Email: geetanjali.rathee123@gmail.com

Hemraj Saini*

School of Computing,
DIT University,
Uttarakhand, 248009, India
Email: hemraj1977@yahoo.co.in
*Corresponding author

Shishir K. Shandilya

School of Data Science and Forecasting,
Devi Ahilya University,
Indore, Madhya Pradesh, India
Email: shishir.sam@gmail.com

S. Rajasoundaran

VIT Bhopal University,
Sehore, India
Email: rajasoundaransraja@gmail.com

Abstract: The wearable e-healthcare systems are a critical IoT mission having wearable sensors, wireless devices and intelligent monitoring of surroundings. The ultimate goal of e-healthcare systems is to identify or diagnose the patients by recognising their various features that are correlated among each other. The involvement of several malicious objects may try to hide the actual recognition of wearable objects for benefiting their own purposes. Though various researchers have proposed various security and efficient schemes, however, it may lead to several computations, management overhead. The aim of this paper is to propose a trusted and efficient e-healthcare communication mechanism while recognising the exact identification of wearable objects. In addition, the proposed mechanism is associated with blockchain mechanism to ensure the transparency and security inside the network while sharing the information. The proposed mechanism is further validated over several security threats against number of security parameters.

Keywords: wearable devices; AHP; security mechanism; analysis process; secure e-healthcare systems.

Reference to this paper should be made as follows: Rathee, G., Saini, H., Shandilya, S.K. and Rajasoundaran, S. (2024) 'A trusted and adaptive security mechanism for wearable e-healthcare systems', *Int. J. Ad Hoc and Ubiquitous Computing,* Vol. 45, No. 1, pp.3–10.

Biographical notes: Geetanjali Rathee is currently working as an Assistant Professor in the Department of Computer Science and Engineering of Netaji Subhas University of Technology (NSUT), Dwarka, New Delhi. She worked as an Assistant Professor (Senior Grade) in Jaypee University of Information Technology (JUIT), Waknaghat, Himachal Pradesh for four years. She has published around 06 national/international patents, around ten IEEE transactions research paper with highest impact factor of 9.1, 20 SCI papers, around 40 Scopus indexed papers. Her research interests include handoff security, cognitive networks, blockchain technology, resilience in wireless mesh networking, routing protocols, networking, and Industry 4.0.

Hemraj Saini is a Professor in the School of Computing, DIT University, Dehradun. His research interest includes information security, edge computing and cloud computing. His six PhD degrees have been awarded under his valuable guidance. Presently, he is providing his services in

various modes like, editor, member of editorial boards, member of different subject research committees, reviewer for international journals and conferences including Springer, Science Direct, IEEE, Wiley, IGI Global, Bentham Science, etc. and as a resource person for various workshops and conferences. He has published more than 150 research papers in international/national journals and conferences of repute.

Shishir K. Shandilya is the Deputy Director of SECURE – Centre of Excellence in Cyber Security and Division Head of Cyber Security and Digital Forensics at VIT Bhopal University. He is working as a Principal Consultant to the Government of India for Technology Development and Assessment in Cyber Security. He also holds the position of Executive Director of National Cyber Defense Research Centre, New Delhi. He is a visiting researcher at Liverpool Hope University, UK, a Cambridge University Certified Professional Teacher and Trainer, ACM distinguished speaker and a senior member of IEEE.

S. Rajasoundaran is working as an Assistant Professor in VIT Bhopal University, Bhopal. He has completed his PhD in College of Engineering Guindy, Anna University, Chennai in 2017. His research areas are wireless sensor networks, computer networks and security. He has 42 publications in various reputed journals and conferences. In addition, he has filed three patents and has 13 years of teaching experience in various institutions.

1 Introduction

In the recent era of modern communications where intelligent devices are emerging at tremendous rate are benefiting the society in various areas or fields. The smart devices or internet of things are defined as the emergent technique where number of devices as the emergent technique controlling the heterogeneous information received from various servers or internet (Yang et al., 2019). Based upon the recorded data, structural information is generated by realising their connections in real-time scenarios. The wearable e-healthcare systems is defined as the critical IoT mission where patients wearing intelligent objects senses, analysis smart or control their healthcare by recognising the pulse rate, blood pressure, diabetes, etc. through images, recording and audios (Li et al., 2020; Hard et al., 2018). The e-healthcare consists of visual sensors, smart phones and digital cameras to capture the patient's health for identifying the exact information of each wearable object as depicted in Figure 1. The depicted Figure 1 represents the hybrid architecture of e-healthcare system where smart devices are collaborated and communicating among each other by providing the services accordingly. The e-healthcare systems can be further improved by providing the services via intelligent devices. Nowadays, digital cameras and visual sensors are placed at each place such as shopping malls, banks, vehicular automation and security surveillance areas where instead of analysing the data recorded from various sensors, the images are data recorded from various sensors, the images are captured to identify the exact position, identity and name of an object (Rathee et al., 2019a, 2020a; Tran et al., 2019).

1.1 Research significance

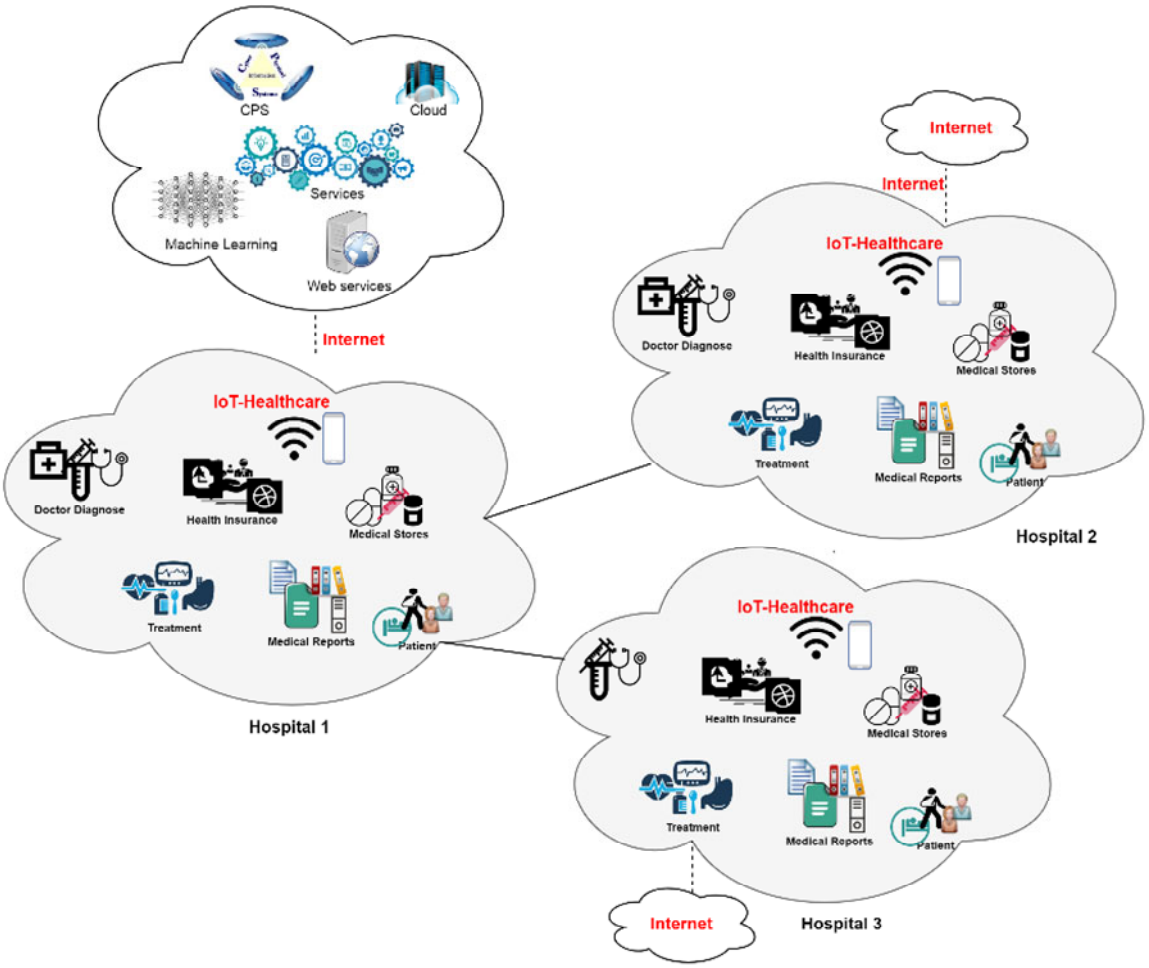
The e-healthcare is generally used in a variety of fields to recognise the objects, however, there is always a threat to compromise these sensors. The intruders may compromise number of visual sensors from highly secure regions such as airports, banks and prohibited areas in order to make their own benefits (Rathee et al., 2019b; Mavropoulos et al., 2019).

The compromised sensors may always generate or record the same pattern of objects so that intruders may perform their malicious actions from the given surroundings. The aim of malicious wearable sensors is not only to generate similar pattern of records but also may affects the decision of neighbouring nodes by generating the altered output (Rathee et al., 2020b; Mejri et al., 2019). They may also affect the overall performance of the network by consuming the network resources, and dropping of information received from their preceding nodes.

1.2 Security methods

Numbers of security schemes have been proposed by various researchers/scientists in order to ensure a secure communication mechanism via wearable sensor nodes. Trust-based cryptographic, encrypted and probabilistic schemes have been proposed by various researchers (Rathee et al., 2020c). However, each technique has their own benefit and limitation to implement a security scheme in the network. The existing security scheme leads to additional security costs, management/storage overhead of keys, computational and communicational steps, etc. The existing schemes provide the security by leading to same extra security charges in the network. In addition, blockchain has been emerged as of the latest technique to provide security and transparency while communicating among entities in the network. Number of organisations has used blockchain techniques in various applications such as industry, healthcare, smart cities, etc. (Rathee et al., 2019c; Zhang et al., 2019). However, the security and transparent mechanism along while communicating or transmitting the information in the network is still at its early stages.

Figure 1 Hybrid e-healthcare architecture (see online version for colours)



Source: Rathee et al. (2020a)

1.3 Paper contribution

The aim of this paper is to propose a secure and efficient e-healthcare communication mechanism where without involving the much security cost, the security is provided by recognising the behaviours of each node. The proposed mechanism uses AHP model to generate the ideal decision while providing a centralised authority system in the network. The AHP mechanism is used to provide an efficient and secure communication mechanism by generating ideal and accurate decisions while recognising the systems (Chan and Chan, 2010). Further, the proposed model is associated with blockchain mechanism in order to ensure the transparency among network while communicating or transmitting the information. The potential contribution of the paper is discussed as follows:

- An accurate and ideal AHP decision making model is used to exploit the unstructured behaviour of malicious objects in the network.
- The continuous analysis of legitimate devices and detecting the malicious number of nodes in order to remove them from the network is maintained through blockchain technique.
- The proposed e-healthcare mechanism is analysed and verified over synthesised dataset consisting of ideal and altered records over probability of false alarm and altered records.

The remaining organisation of paper is structured as follows. The number of schemes proposed by various researchers and scientists will be discussed in Section 2. A security e-healthcare framework using AHP decision model will be illustrated in Section 3. The validation and verification of proposed framework over various number of security parameters will be discussed in Section 4. Finally, Section 5 concludes the paper and discusses the future directions of the paper.

2 Related work

Various research studies have been carried out to propose security methods/models network through trusted, probabilistic and cryptographic algorithms illustrates the number of approaches/security schemes proposed by various authors.

Table 1 Literature survey on security schemes in healthcare SDNs

Authors	*Technique*	*Mechanism*
Zhang et al. (2019)	Visualising and managing	The authors have emphasised on various systematically analysis by using dynamic or static UML models.
Liu et al. (2003)	Zero-watermarking scheme	The blind extraction and zero-embedding ensured the protection of original image by diagnosing the special requirements.
Sherif et al. (2016)	Ride sharing and privacy issues	The servers measured the similarity score of finding the shares without revealing their information.
Jiang et al. (2018)	Multi-objective estimations	The authors have applied a shortest path scheme to find 3D groups.
Gao et al. (2020)	Co-saliency identification technique	Contributed by enabling multistage perception method to extract the data from various sizes of image.
Rathee et al. (2020d)	Lightweight adaptive boosting model	The authors have improved the logarithm and sharing exponentiation functions by expanding the input range.
Gheisari et al. (2019)	Privacy preserving model	The authors have initially proposed a privacy informative device by providing a dynamic environment.
Qi et al. (2021)	Blockchain-based secure traffic classification	The authors have proposed a learning-based hash method to build the coding tress and generating the hash tables using l-nearest classification algorithm.
Huang et al. (2019)	Credit-based consensus in IIoT	The authors have conducted a case study using directed acyclic graph to demonstrating the analysis and evaluation of proposed phenomenon.
Liu et al. (2019)	Reputation-based retail marketing	The authors have proposed reputation systems for retail marketing the PoS blockchain method.

Liu et al. (2003) have proposed watermarking security scheme through hyper chaos for enhancing the security. The authors have ensured bling extraction with protection of original objects by identifying their special features. The simulated results verified the resistance and secure information transmission for a medical data record with 46.67% of improvement as compare to conventional methods. In addition, Zhang et al. have used re-identification feature to correlate the different objects by utilising the regional metric of structured information. The authors have proposed a new similarity score scheme to differentiate the images through their weights. Sherif et al. (2016) have proposed an organised scheme to ensure the privacy and ride sharing issue for vehicular environments. The servers analysed similarity score of each observed image for revealing the information. Further, Jiang et al. (2018) have focused on multi-objective criteria's for observing study generated the efficient validation and verification of proposed scenarios. Similarly, Gao et al. (2020) have proposed a co-salience mechanism to recognise the communication and silent regions in surveillance systems. The authors have implemented a perception-based scheme to extract the variable size data from the network. Further, Rathee et al. (2020d) have proposed a cognitive automation mechanism for IIoT systems for providing a secure and accuracy decision-making phenomenon while transmitting the information among network. Furthermore, Gheisari et al. (2019) have proposed a privacy model for preserving the communication process secured via IoT systems. The authors have provided a dynamic informative device to determine the privacy of each IoT node. Qi et al. (2021) have proposed blockchain-based traffic classification mechanism for IIoT. The authors have proposed a learning-based hash method to build the coding tress and generating the hash tables using l-nearest classification algorithm. The proposed mechanism was simulated using various datasets through accuracy. Huang et al. (2019) have proposed a credit-based proof of work method to protecting the sensitive information among nodes. The authors have conducted a case study using directed acyclic graph to demonstrating the analysis and evaluation of proposed phenomenon. Liu et al. (2019) have proposed reputation systems for retail marketing the PoS blockchain method. The implementation and architecture of the systems is measured using Ethereum and demonstrated the off/on chain and scalability performance in the system.

Though, numbers of schemes have been proposed by various researchers/authors using various preserving, multi-objective and resilient schemes. However, the existing mechanisms are further leads to several computational and communicational overhead in the network. Further, the present security schemes lead to various accurate decision-making issues while collaborating among each other. The aim of this paper is to propose a secure an efficient decision-making scheme via number of collaborative visual sensors using AHP model.

3 Proposed approach

AHP is an analytical hierarchical process that is multi-attribute decision making scheme that categorises the objects depending upon their various internal behaviours and attributes. The AHP is used to provide an appropriate decision model based on multiple attributes. This paper presents a secure F-learning mechanism where visual sensors that are responsible to recognise or identify the objects using AHP scheme. The number of visual sensors during recognition of objects may take collaborative

decision recognition of objects decided to determine the final object.

3.1 System model

The system model of proposed mechanism is depicted in Figure 1 consist of three main layers such as

1 The visual sensors such as vehicles, roads, individuals, etc. that visualises the correct identification using various features.

2 AHP layer where it is necessary to take final decision for identifying the object from the surroundings. The AHP models ensure an accurate detection of scheme among visual sensors to identify any object.

3 Server layer where finally the identified objects are passed to higher layer for further processing and analysis.

In a network size of 'n' visual sensors, initially all the nodes are identified to be ideal and trusted where in order to identify the accurate identification of objects, some compromised visual sensors are involved in the network. The collaborative and accurate decision by multiple sensors to recognise the objects through AHP model is explained in further detail.

3.2 AHP model

An analytical hypothetical process ensures a secure, accurate and efficient visualisation of objects by visual sensors. The legitimacy of objects by visual sensor is computed through various communicating behaviours. The multi-attributes are analysed to generate a trust rate of each communicating sensor where the node having high trust rate is assumed to be legitimate. The initial weights are distributed between 0–1 that are further increased or decreased depending upon their internal behaviours or communicating entities. The step-wise process to recognise further trust rates through AHP is discussed as below:

Step 1 A pair-wise matrix comparison having q number of parameters p_q as $p_{q\times q}$ are defined as the pair-wise comparison of u^{th} alternative with v^{th} criterions. The p_{uv} illustrates the relative significance of alternatives u over v criteria.

$$p_{q\times q} = \begin{vmatrix} 1 & p_2 & \cdots & \cdots & p_{1n} \\ p_{21} & 1 & \cdots & \cdots & p_{2n} \end{vmatrix}$$

Step 2 The weights w_u of each visual sensor are recognised by analysing the u^{th} row.

Step 3 The w_u weights are further analysed from previous steps to compute normalised metric MN or M as:

$$N \text{ or } M_{q\times 1} = p_{q\times q} \times w_{u\times 1}$$

Step 4 The relative N or M is defined as:

$$RN \text{ or } M_{q\times 1} = NM_{u\times 1} / w_{u\times 1}$$

Step 5 Further, the maximised eigenvalues as $EV_{\max}$ is determined as an average of RN or $MP_{q\times 1}$ as consistency index (CI) as:

$$(EV_{\max} - q)/(q-1)$$

Step 6 Finally, the random index is analysed as the ratio of CI/RI.

3.3 Blockchain-based AHP model

The trust rate and their distribution among nodes are analysed using AHP model. However, the continuous analysis of trust values and weights to ensuring or maintaining the security and transparency among nodes are further maintained through a blockchain mechanism. The trust and weight of each node is maintained in a block where each and every node's value is changed depending upon their internal behaviour. In case any kind of node value alteration by the malicious devices, or altering of legitimate node into malicious nodes by the attackers can be easily detected or intimated immediately to the entire network. The trust and weight of a node block maintains the transparency in the network.

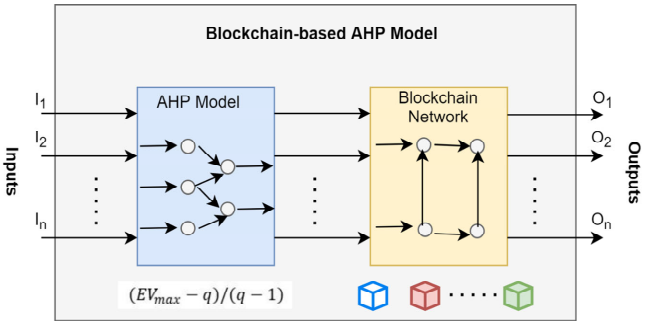
The working of proposed blockchain-based AHP model is detailed in further subsection while ensuring a secure and transparent communication among the nodes in the network.

3.4 Working of proposed blockchain-AHP model

The working of AHP-based blockchain mechanism is explained through a diagram where number of nodes in network having randomly weight and trust allocation to the entire network. The random trust and weights of each node is inputted in the AHP model during the establishment of the network. In addition, the AHP model is used to assign or change the weight and trust of each node by analysing their internal behaviours. After the computation of trust and weights of each node, the transparency and security among nodes is maintained through blockchain mechanism. The nodes act as a block having the weight and trust that may be changed automatically in the network while communicating among each other. In case any nodes explicitly want to change the trust value or weight of a node or want to alter the legitimate node into malicious node, then, it can be easily analysed and intimated by the other nodes in the network. The legitimate nodes are identified having less weight and more trust value (among 0.7–1.0) that is continuously computed through AHP model in the network. In addition, the weight and trust of each node or block is changed while communicating or transmitting the information to other nodes in the network.

The depicted Figure 2 details the proper working of blockchain-based AHP model while distributing the weight and trust value of each node using AHP model. In addition, the transparency and security of each node is maintained using blockchain mechanism.

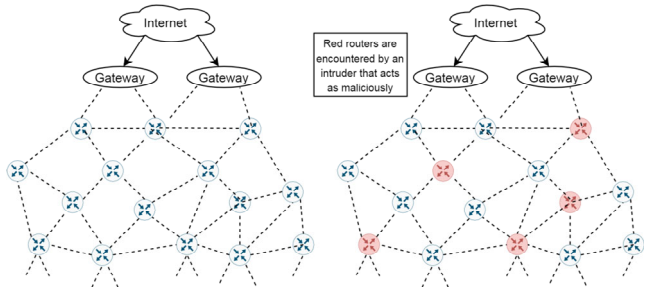
Figure 2 A secured blockchain-based AHP framework (see online version for colours)



4 Performance evaluation

The proposed AHP-based mechanism is analysed over ideal and altered network model as depicted in Figure 3.

Figure 3 Ideal vs. adversary network model (see online version for colours)



(a) (b)

4.1 Ideal network

The depicted Figure 3(a) represents the ideal network where all number of nodes are categorised as trusted/legitimate. The network is complete ideal and is ideally communicated and trusted among each. The visual sensors that are responsible to identify, monitor and sense objects are trusted and ideal.

4.2 Adversary network

Figure 3(b) represents the adversary model having number of malicious devices involved during object identification. In the proposed model, the initial network consists of number of nodes where 5% of nodes are acted as malicious. Similarly, the malicious nodes rate is increases with 5% upon increasing the network scalability.

The proposed phenomenon determines the analysis and identification of validated number of nodes during recognition of objects through visual sensors.

4.3 Baseline approach (existing approach)

The proposed mechanism is compared and validated against Tran et al. where the authors have formulated an optimised federated learning mechanism by exploiting the transmission and decomposition of problems into three sub problems. The authors have also categorised the optimal solution of all the subproblems in a closed form. The approach is validated against extensive theoretical and numerical results. The proposed approach is simulated and validated against Tran et al. by introducing an adversary and ideal network model. In addition, the proposed framework is analysed against various security metrics.

4.4 Setup

For identifying the validation and verification of proposed network, the proposed model is simulated over MATLAB having 20 numbers of nodes at the initial and 100 number of nodes at maximum count. Table 2 represents an abstract view several parameters as an input of threat sources.

Table 2 Measuring parameters

Category	*% of threat request*	*Severity level*	*No. of sources*
1	Number of nodes	100	
2	Network area	500 × 500	
3	Node's behaviour	Ideal, malicious	
6	Algorithm	BP, ANN	

Figure 4 Run time (see online version for colours)

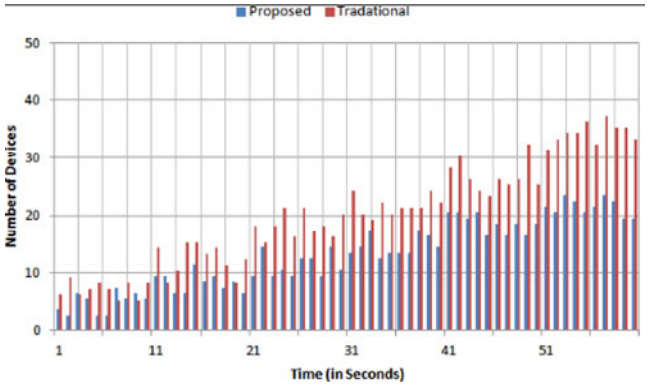
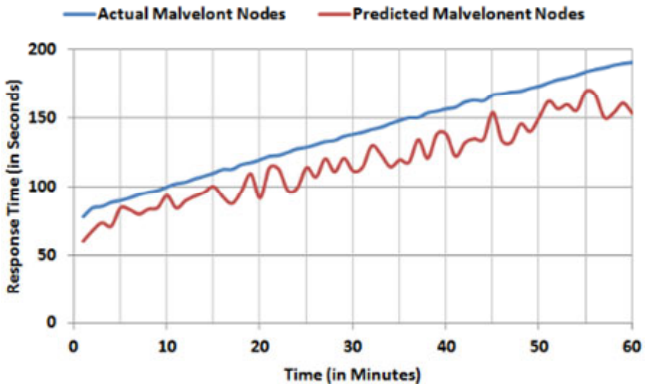


Figure 5 Response time (see online version for colours)



The graphs of simulation run time and processed requests are depicted in Figures 4 and 5.

The depicted Table 2 represents the addition of malicious number of nodes through a determined percentage upon increasing network size. The probability of handoff

process elaborates that around 5% number of nodes are moving from one place to another while 10% number of devices are changing from ideal to malicious upon each network size. In order to study the changing records of the environment, numbers of parameters are analysed. The depicted Figure 4 details the total devices during the 60 minutes course of simulated environment.

Several metrics were determined from proposed scheme performance based upon the created test bed. The depicted Figure 5 analyses the system accuracy to identify MID among large number of nodes connected to specific environment. The proposed mechanism leads to approximate 87% of predicted accuracy as compare to existing mechanisms in terms of data identification as depicted in Figure 5.

5 Conclusions

The security is considered as one of the emergent issues in e-healthcare systems where number of devices used to recognise the patients' health in various fields must be trusted. The proposed e-healthcare mechanism ensures a secure and reliable communication mechanism using AHP model to categorise the nodes into legitimate and malicious. The proposed mechanism is simulated over processed request and run time over existing mechanism. Further, the transparency and security are further analysed by maintain a blockchain of each node having trust and weights. The depicted results showed the efficient and reliable improvements as compare to conventional approach. Number of patterns used to categorise the devices through machine learning should be considered in future directions.

References

Chan, F.T. and Chan, H.K. (2010) 'An AHP model for selection of suppliers in the fast-changing fashion market', *The International Journal of Advanced Manufacturing Technology*, Vol. 51, No. 9, pp.1195–1207.

Gao, Z., Xu, C., Zhang, H., Li, S. and de Albuquerque, V.H.C. (2020) 'Trustful internet of surveillance things based on deeply represented visual co-saliency detection', *IEEE Internet of Things Journal*, Vol. 7, No. 5, pp.4092–4100.

Gheisari, M., Pham, Q.V., Alazab, M., Zhang, X., Fernández-Campusano, C. and Srivastava, G. (2019) 'ECA: an edge computing architecture for privacy-preserving in IoT-based smart city', *IEEE Access*, Vol. 7, pp.155779–155786.

Hard, A., Rao, K., Mathews, R., Ramaswamy, S., Beaufays, F., Augenstein, S. and Ramage, D. (2018) *Federated Learning for Mobile Keyboard Prediction*, arXiv preprint arXiv:1811. 03604.

Huang, J., Kong, L., Chen, G., Wu, M., Liu, X. and Zeng, P. (2019) 'Towards secure industrial IoT: blockchain system with credit-based consensus mechanism', *IEEE Transactions on Industrial Informatics*, June, Vol. 15, No. 6, pp.3680–3689, DOI: 10.1109/TII.2019.2903342.

Jiang, X., Fang, Z., Xiong, N.N., Gao, Y., Huang, B., Zhang, J. and Harrington, P. (2018) 'Data fusion-based multi-object tracking for unconstrained visual sensor networks', *IEEE Access*, Vol. 6, pp.13716–13728.

Li, T., Sahu, A.K., Talwalkar, A. and Smith, V.V. (2020) 'Federated learning: challenges, methods, and future directions', *IEEE Signal Processing Magazine*, Vol. 37, No. 3, pp.50–60.

Liu, D., Alahmadi, A., Ni, J., Lin, X. and Shen, X. (2019) 'Anonymous reputation system for IIoT-enabled retail marketing Atop PoS blockchain', *IEEE Transactions on Industrial Informatics*, June, Vol. 15, No. 6, pp.3527–3537, DOI: 10.1109/TII.2019.2898900.

Liu, J., Ma, J., Li, J., Huang, M., Sadiq, N. and Ai, Y. (2003) 'Robust watermarking algorithm for medical volume data in internet of medical things', *IEEE Access*, Vol. 8, pp.93939–93961.

Mavropoulos, O., Mouratidis, H., Fish, A. and Panaousis, E. (2019) 'Apparatus: a framework for security analysis in internet of things systems', *Ad Hoc Networks*, Vol. 92, pp.101735–101743.

Mejri, M.N., Ben-Othman, J. and Hamdi, M. (2019) 'Survey on VANET security challenges and possible cryptographic solutions', *Vehicular Communications*, Vol. 1, No. 2, pp.53–66.

Qi, H., Wang, J., Li, W., Wang, Y. and Qiu, T. (2021) 'A blockchain-driven IIoT traffic classification service for edge computing', *IEEE Internet of Things Journal*, 15 February, Vol. 8, No. 4, pp.2124–2134, DOI: 10.1109/JIOT.2020. 3035431.

Rathee, G., Sharma, A., Saini, H., Kumar, R. and Iqbal, R. (2020a) 'A hybrid framework for multimedia data processing in IoT-healthcare using blockchain technology', *Multimedia Tools and Applications*, Vol. 79, No. 15, pp.9711–9733.

Rathee, G., Garg, S., Kaddoum, G. and Choi, B.J. (2020b) 'A decision-making model for securing IoT devices in smart industries', *IEEE Transactions on Industrial Informatics,* accepted.

Rathee, G., Jaglan, N., Iqbal, R., Lal, S.P. and Menon, V.G. (2020c) 'A trust analysis scheme for vehicular networks within IoT-oriented green city', *Environmental Technology & Innovation*, Vol. 20, pp.101138–101144.

Rathee, G., Ahmad, F., Iqbal, R. and Mukherjee, M. (2020d) 'Cognitive automation for smart decision-making in industrial internet of things', *IEEE Transactions on Industrial Informatics*, Vol. 17, No. 3, pp.2152–2159.

Rathee, G., Sharma, A., Iqbal, R., Aloqaily, M., Jaglan, N. and Kumar, R. (2019a) 'A blockchain framework for securing connected and autonomous vehicles', *Sensors*, Vol. 19, No. 14, pp.3157–3165.

Rathee, G., Sharma, A., Kumar, R. and Iqbal, R. (2019b) 'A secure communicating things network framework for industrial IoT using blockchain technology', *Ad Hoc Networks*, Vol. 94, pp.101925–101933.

Rathee, G., Sharma, A., Saini, H., Kumar, R. and Iqbal, R. (2019c) 'A hybrid framework for multimedia data processing in IoT-healthcare using blockchain technology', *Multimedia Tools and Applications*, Vol. 79, pp.1–23.

Sherif, A.B., Rabieh, K., Mahmoud, M.M. and Liang, X. (2016) 'Privacy-preserving ride sharing scheme for autonomous vehicles in big data era', *IEEE Internet of Things Journal*, Vol. 4, No. 2, pp.611–618.

Tran, N.H., Bao, W., Zomaya, A., Nguyen, M.N. and Hong, C.S. (2019) 'Federated learning over wireless networks: optimization model design and analysis', in *IEEE INFOCOM 2019 – IEEE Conference on Computer Communications*, pp.1387–1395.

Yang, Q., Liu, Y., Cheng, Y., Kang, Y., Chen, T. and Yu, H.H. (2019) 'Federated learning', *Synthesis Lectures on Artificial Intelligence and Machine Learning*, Vol. 13, No. 3, pp.1–207.

Zhang, Y., Xu, X., Liu, A., Lu, Q., Xu, L. and Tao, F. (2019) 'Blockchain-based trust mechanism for IoT-based smart manufacturing system', *IEEE Transactions on Computational Social Systems*, Vol. 6, No. 6, pp.1386–1394.