Contents lists available at ScienceDirect

Alexandria Engineering Journal

journal homepage: www.elsevier.com/locate/aej

Original Article

Accessibility and ensured quality of life for disabled people using trusted edge computing

Geetanjali Rathee[a], Sahil Garg[b,*], Georges Kaddoum[b,c], Samah M. Alzanin[d], Abdu Gumaei[d], Mohammad Mehedi Hassan[e,*]

[a] Department of Computer Science and Engineering, Netaji Subhas University of Technology, Dwarka Sector-3, New Delhi, India
[b] Electrical Engineering Department, École de technologie supérieure, Université du Québec, Montréal, QC H3C 1K3, Canada
[c] Cyber Security Systems and Applied AI Research Center, Lebanese American University, Beirut, Lebanon
[d] Department of Computer Science, College of Computer Engineering and Sciences, Prince Sattam bin Abdulaziz University, Al-Kharj 11942, Saudi Arabia
[e] Department of Information Systems, College of Computer and Information Sciences, King Saud University, and King Salman Centre for Disability Research, Riyadh 11543, Saudi Arabia

ARTICLE INFO

Keywords:
Artificial intelligence
Information communication technology
Edge devices
Smart home security
Industrial automation
Disabled persons
Trusted algorithms

ABSTRACT

Now a days, the revolution or advancements in Information Communication Technology (ICT) are changing the way of handling the situations in the present environment. In our society, several people are present who live with physical difficulties and can not complete their basic household tasks for their own. The disabled person is all alone at home and caring the house where intermediator may gain the benefit of the opportunity. Though the modern era is revolutionizing the whole communication and interaction process among environment and human. The disabled person who cannot walk, and is deaf completely unable to hear, run or handle the current situation, the automatic systems or alarm may be compromised by the intruder and can access the house with the mean of steal. The aim of this paper is to propose a secure and competent communication mechanism for AI and edge-computing based home automation in case of disabled persons handling the situation. The proposed mechanism integrates the distrust-based recommendation system along with Social Contact Similarity mechanism that improves the efficiency and quick action decision corresponding to the altered device that may cause severe harm at the edge-level or to the person. The proposed mechanism is simulated and substantiated against various existing scheme over several performance metrics such as delay, alteration rate, accuracy and response time.

1. Introduction

In industrialization countries, the care provision to the depend individuals is becoming a foremost priority for the government [1]. The increase in quality of life fosters an increase in life expectancy. In our society, millions of people are present who live with physical difficulties and can not complete their basic household tasks for their own. The disabled people are the one who are not able fully or partially dependent on others and their generic impairment do not thwart their participation in the society such as walking, hearing, seeing, mobility, communicating etc [2,3]. According to the report of united physical care and need, millions of people having disabilities are not able to gain the access of ICT and remain backward in the society. Now a days, the revolution or developments in ICT are changing the way of handling the situations in the present environment [4,5] such as Society 5.0, Smart homes, Smart cities, etc. The Artificial Intelligence (AI) and edge computing are the trending and emerging paradigm in order to fasten and strengthen by processing the information closer to the users in real time environments. The situations where it is necessary to process or provide an immediate response to the users, these technologies may benefit a great role.

1.1. Need of AI and edge computing

The AI technologies or methods can be used for surveillancing the nearby surroundings and responding without any intervention of human power [6]. The real time decisions and quick responses can be

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

https://doi.org/10.1016/j.aej.2023.09.046
Received 18 July 2023; Received in revised form 2 September 2023; Accepted 15 September 2023
Available online 29 September 2023

easily made through AI systems that is again a predefined necessity for the disabled individuals. In addition, to make it much faster, the responses can be fasten up by introducing the concept of edge computing with them [7]. There were cases where people with disabilities may move out from their homes and need a personal belonging or nurse to pursue their daily activities. Now a days, the revolution and involvement of ICT has made it possible where people with disabilities not only come out from their homes, but also performing best in their respective fields. Let us assume an example where along with so many advanced technologies where disabled people not only able to complete their tasks independently but also take good care of house, office, shop etc on their own without involvement of any other person. Here we have considered an example of AI-based home automation system where the home is fully automated starting from opening the door till washing dishes, cooking food, washing clothes, automatic lights and so on [8,9]. The disabled person is all alone at home and caring the house where intermediator may gain the benefit of the opportunity. The disabled person who cannot walk, and is deaf completely unable to hear, run or handle the current situation where automatic system or alarm is compromised by the intruder and can access the house with the aim of steal.

1.2. Problem statement

Though home automation is the greatest way for the disabled person who is all alone at home and can take good care of his/her house, however, any single mismanagement of non-working of device may completely harm the person. Though number of security alarms, automation alteration or cryptographic solutions have been proposed by various scientists, however, these schemes are can not be fully adopted by the disabled people and in case of emergency, the disabled person is helpless and, in a danger, to handle the situation [10,11]. The delay in processing by the systems may further add delays and various security threats in the network. Therefore, it is needed to propose an AI-based and edge-computing solutions in order to provide an immediate, automatic and efficient decision-making without any intervention of human power. The AI systems may take independent decisions along with real-time responses with the integration of edge-computing techniques. Therefore, it is further needed to propose some good solutions where the devices can be easily and regularly identifying itself or by their neighbouring devices for checking their legitimacy in the network at edge level (Fig. 1).

1.3. Contribution

The goal of this paper is to propose a secure and efficient communication mechanism for home automation in case of disabled persons handling the situation at edge-level. In other case, where AI or automatic devices used by disabled persons can be immediately altered by the intruders for not taking any action at that amount of time. The proposed mechanism integrates the distrust-based recommendation system [13] along with Social Contact Similarity (SCS) mechanism [14] that improves the efficiency and quick action decision corresponding to the altered device that may cause severe harm in the edge computing network or to the person. The point-wise contribution of the paper is illustrated as follows:

- The identification of trusted and legitimate devices used by the disabled person for completion of their tasks using intelligent devices.
- The detection of legitimacy using distrust-based recommendation system for computing the trust of each communicating node that are recommended by its neighbouring device at edge level.
- The proposed mechanism is integrated with SCS mechanism for further improving the efficiency and accuracy in the edge computing network.

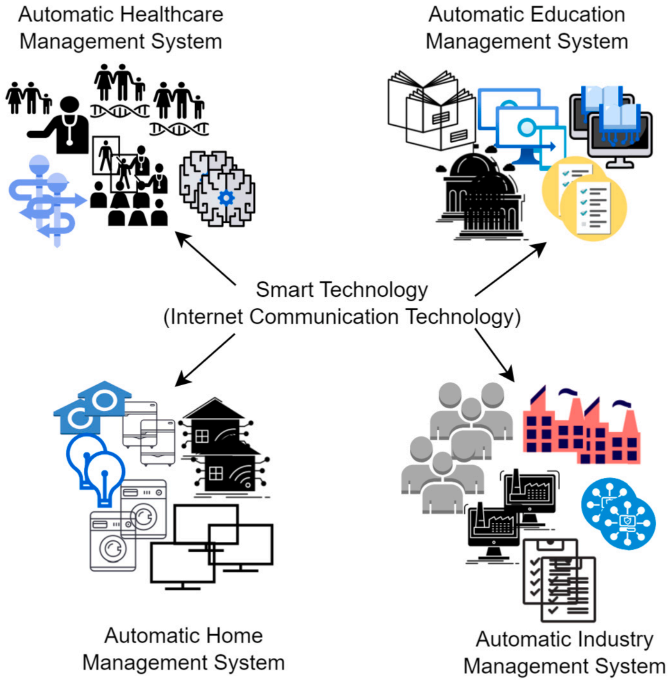

Fig. 1. Accessing of Information while Maintaining Quality for Disabled People in Healthcare [12].

- The proposed mechanism is simulated and verified against various existing scheme over several performance metrics such as delay, alteration rate, accuracy and response time.

The proposed mechanism used the Social Contact Similarity (SCS) technique for identifying the accurate decision making through AI by legitimate devices while transmitting the information. In addition, the recommendation system is used to distinguish among legitimate and malicious behaviour of communicating devices in the network. The proposed mechanism is verified and validated against various security measures over existing schemes. The remaining contribution of the paper is structured as follows. The literature survey of secure and efficient communication mechanism for disabled persons is discussed in section 2. Section 3 proposes an efficient and secure transmission and communication method using trust-based approaches based upon quality of life for ensuring smooth conduction of activities. Section 4 illustrates the verification and validation communication process against existing mechanism over several performance metrics. Finally, section 5 concludes and discusses the future scope of the paper.

2. Survey of literature

This section illustrates the number of AI and edge based secure and quality life communication approaches for the disabled persons for ensuring better survival in the society. The number of approaches proposed by various researchers/scientists/engineers and authors are listed in the below text. In addition, a table is illustrated as Table 1 for highlighting the limitations of existing works proposed by the several authors. The proposed mechanism resolves the existing limitations by improving the overall efficiency of the communication process.

Birajdar [15] and More have proposed security system for disabled and elderly people using ARM microcontroller by attaching biomedical sensors to sense the body temperature of patient. The proposed device is very useful for the disabled, children and elderly people with continuous sending and monitoring the behaviour of patient through android phone. The authors have used camera for emergency situation for capturing the images. Dimaunahan et al. [16] have proposed fingerprinting and voice recognition system involving feature extraction,

Table 1
Literature survey of existing schemes proposed by sever authors.

Authors	Proposed Mechanisms	Technologies Used	Drawback
Birajdar and More [15]	Security system for disabled and elderly people using ARM microcontroller	Useful for the disabled, children and elderly people	Increases communication delay
Dimaunahan et al. [16]	Fingerprinting and voice recognition system	Biometric recognition method for authenticating the patient and fingerprinting	excessive key management
Ragot [17]	Outlined two projects such as COALAS and SYSIASS	Meet the requirements and empowering the mobility enhancement	Discussed the future aspects of the project
Ziefle et al. [18]	Investigating the users willingness to accept the medical technologies	Examined the privacy and trust issues for medical technology	Need to focus on delay and error while transmitting the information
Priyadharshini and Umamakeswari [19]	Surveyed the number of technologies	Identification of humans for smart homes	Focused on future directions
Uzunay and Bicakci [20]	Presented secure hash algorithm	Incorporate home architecture and integrated framework	Increases communication overhead
Waynet et al. [21]	Addressed two main categories of the requirements	Construction and designing for non-standard shapes of user's body	Increase the storage delay and overhead
Faroom et al. [22]	Focused on the review and studies of multiple automation	Helpful for disabled people in order to search usable and efficient system	Mobility delay and communication delays
Rifon et al. [23]	Proposal of home automation for disabled people	Monitoring and remote surveillance the vital signs	Long decision making while action
Buzi et al. [24]	Blind user's interaction	Usability and accessibility of the transactions	storage and communication delays in the network
Pandey et al. [25]	proposed a structured design for assisting the disabled people's	have introduced the deployment using blockchain and cloud computing	Computation overhead for deploying and analysis of devices
Ahmed and Rasheed [26]	real time-based face recognition detection system	suggested the working model using Raspberry Pi and open CV	delays while recognizing the movement of face

pre-processing and images at the time of account opening. The authors have used biometric recognition method for authenticating the patient and fingerprinting for checking and opening the account for further transactions. Ragot et al. [17] outlined two projects such as COALAS and SYSIASS with the aim of developing the technologies set to meet the requirements and empowering the mobility enhancement and communication. Ziefle at al. [18] have focused on investigating the users willingness to accept the medical technologies with continuous monitoring their homes. The authors have examined the privacy and trust issues for medical technology by concerning the insensitive age and gender. The proposed mechanism revealed the patients requirement and acceptance issues in order to successfully identifying and designing the new medical schemes. Priyadharshini and Umamakeswari [19] have surveyed the number of technologies used in identification of humans for smart homes while identifying the malicious behaviour in the network. The used have used support vector machine and component analysis model for broadly classifying and mitigating the negative ideas along with addressing the accuracy and privacy among devices. The authors have addressed the potential performance improvements and people's trust towards smart technologies. Uzunay and Bicakci [20] have presented secure hash algorithm for providing a secure voice activated home device for quadriplegia patients. The contribution of proposed system is to incorporate home architecture and integrated framework for assisting the monitoring the remote healthcare system. Buzzi et al. [24] have investigated the blind user's interaction with the commercial services such as eBay by focusing on the usability and accessibility of transactions securely navigating via screen reader. Waynet et al. [21] have addressed two main categories of the requirements such as clothing with the users who have issues with undressing and dressing and clothing with improved construction and designing for non-standard shapes of user's body. Faroom et al. [22] have focused on the review and studies of multiple automation of home designed for disabled patients. The proposed research was helpful for disabled people in order to search usable and efficient system with respect to various categories. Rifon et al. [23] have discussed the proposal of home automation for disabled people for improving their life quality using automation and tele-assistance. The home theatre personal computer connected through monitoring and remote surveillance the vital signs, interfaces and type of disability by centrally controlling the automatic system installed at home. In addition, Pandey et al. [25] have proposed a secure and efficient home communication mechanism based upon smart devices technology. The authors have proposed a structured design for assisting the disabled people's to health, housing and other necessities. The authors have introduced the development and deployment of such applications with smart technologies using blockchain, cloud computing, sensors and so on for computing and processing the health and home aspects for disabled people. Ahmed and Rasheed [26] have proposed a real time-based face recognition detection system using raspberry PI software. The aim of their paper is to recognise the moving face towards several levels using RFI-cards and passwords for accessing the security systems. The authors have suggested the working model using Raspberry Pi and open CV by providing extra scenarios of face recognition in combination with efficient and cheap machinery systems.

2.1. Problem statement

Though number of security based and accessibility methods have been projected by various researchers/scientists/authors [27–30], however, very few of them have focused on the quality life for disabled people using AI. The disabled persons who are surviving to get a better life using technologies may further affect their standard of living in the society. The malicious or disrupted devices may further harm them drastically. Therefore, it is needed to focus on the AI based security aspects of intelligent devices using by disabled people in any specific area of application. This paper proposes two trust-based schemes such as Social Contact Similarity and Fuzzy Trust-Distrust Recommendation system for ensuring a better secure accessibility and quality of life for disabled people.

3. Proposed framework

3.1. System model

The system model of proposed phenomenon is depicted in Fig. 2 having number of devices incorporated in the environment where disabled persons can easily track and move freely with any hurdle in the

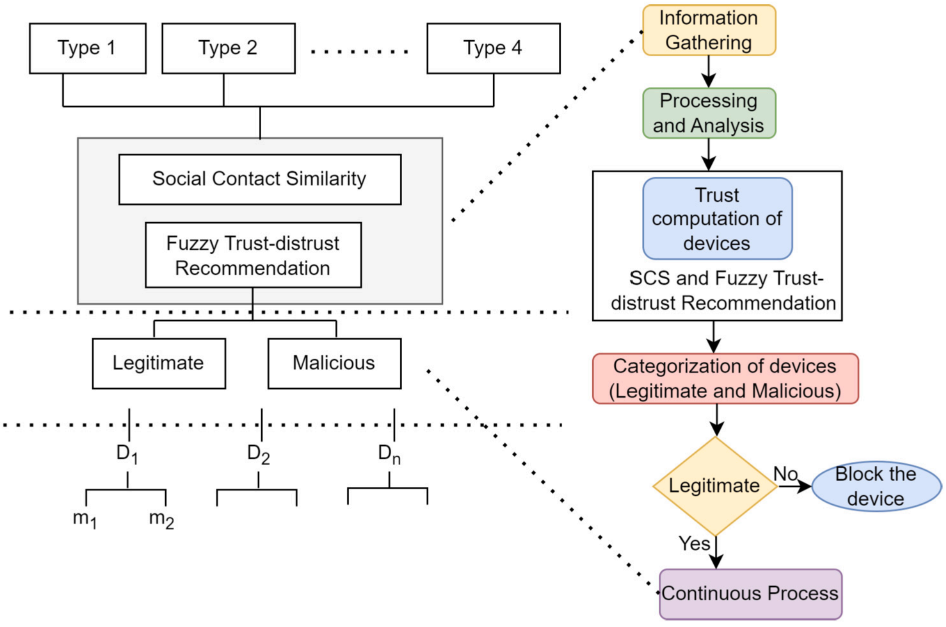
Type 1
Type 2
Type 4
Social Contact Similarity
Fuzzy Trust-distrust Recommendation
Legitimate
Malicious
D1
D2
Dn
m1
m2
Information Gathering
Processing and Analysis
Trust computation of devices
SCS and Fuzzy Trust-distrust Recommendation
Categorization of devices (Legitimate and Malicious)
Legitimate
No
Block the device
Yes
Continuous Process

Fig. 2. Proposed Framework to Ensure Secure Communication through Intelligent Devices on AI-based Edge Computing Network.

Table 2
Definition and Abbreviations.

Symbol	Description
SCS	Social Contact Similarity
FTD	Fuzzy Trust-Distrust
d_i, d_j	device i and device j in the network
$SCS(d_i, d_j)$	social contact similarity among device i and device j
P, Q, R	Number of devices
$L_i and L_j$	location of devices in the network
O	Outlier
W and CF	Variants to measure trust of a device
$PredictionCF$	Prediction using context fuzzy scheme
S'	set of malicious devices
$N - S'$	Set of legitimate devices
w_p	weight of a device p during communication in the network
$r_{\vec{p}_k}$	Vector of device r over device
$S - o$	set of legitimate surroundings

surroundings. The proposed mechanism consists of N number of edge computing devices as $D_i, D_j, , , D_n$ that communicates among each other in order to guide the person to take their corresponding action. The SCS and fuzzy trust-distrust AI recommendation system is used to ensure the accuracy and effectiveness in the device while interaction and responding to the patients at edge level. The SCS method is adopted by the devices at the initial stage in order to analyze the social contact similarity among devices in the network. The SCS method is integrated with fuzzy distrust method in order to analyze the effectiveness of ensuring the security and trustworthiness of communicated devices. The SCS and fuzzy trust-distrust recommendation systems will process and generate the category of devices at AI edge levels for real-time responses.

Table 2 lists the number of symbols and abbreviations that are used in the paper.

3.2. AI and edge computing in SCS and recommendation system

The AI and edge-based systems where automative decisions and processing in entirely dependent on smart devices. It is needed to provide a secure and efficient communication system at edge level only before processing and generating the further information at upper level of the network. The proposed framework is depicted in Fig. 2 consisting of n number of edge devices having n type such as type 1 (completely malicious), type 2 (red zone devices), type 3 (yellow zone devices), and type 4 (legitimate devices). Now in order to ensure a secure communication mechanism where disabled people are completely rely on the AI decisions and action of the intelligent devices. It must be ensured that devices are legitimate and provide immediate and accurate response to their respondents. For ensuring an accurate decision making and reliable communication mechanism, the proposed phenomenon has integrate two trust-based approaches such as social contact similarity and fuzzy trust-distrust recommendation system in the back end. All the devices at the AI edge-level are weighted with some trust value that keeps on changing depending upon their communication behaviour. Whenever a device is compromised by the intruder, its trust value will keep on reducing that can't be further allowed for any future communication and transaction in the AI edge network. The integration of SCS and fuzzy trust-distrust is to provide a secure and accurate categorization of devices such as legitimate or malicious. The malicious devices are further categorized into other types such as type 1, type 2, and type 3. The surroundings information is processed and analyzed by the AI edge devices that are categorized by the approaches into two category and depending upon their type, the devices are either blocked or termed as legitimate in the network. The detailed explanation of both the approaches is described below.

3.3. Social contact similarity (SCS) method

The trust-distrust recommendation mechanism is further integrated with social contact similarity (SCS) where devices having same services and sentiments. Devices D_i are partitioned into IDs of record by visiting their location L_i for their social contacts. The SCS of two devices d_i and d_j during exchange of information L_i and L_j are followed as:

$$SCS(d_i, d_j) = \frac{|L_i \bigcap L_j|}{|L_i|.|L_j|} \quad (1)$$

3.4. Fuzzy trust-distrust recommendation

In order to utilize the computational model for belief-disbelief concepts, we can use a fuzzy-based recommendation system for identifying

Table 3
Complexity Comparison.

Complexity to be considered	Baseline Approach 1 (Existing Method)	Baseline Approach 2 (Existing Method)	Proposed Approach
Computational Complexity	(n-1)log n	(n-1) log n	log(n)
Communication Complexity	(n-1)	(n-1)	log n
Overall Complexity	n × log (n-1)	n × log (n-1)	log(log(n))

the legitimate or trusted devices while transmitting the information among each other. If a device P trusts highly on device Q, Q highly trusts on device R and P distrusts R completely then the recommendation or decisions about identifying the legitimacy of a device is completely infeasible. This is a type of outlier that must be avoided while examining the legitimacy of a device. The fuzzy trust-distrust recommendation method along with the integration of SCS method is defined as:

$$PredictionW(P_k, d_j) = \frac{\sum_{p\epsilon(s-o)} w_p \times r_p, d_j}{\sum_{p\epsilon(s-o)w_p}} +$$

$$SCS(d_i, d_j) = \frac{|L_i \bigcap L_j|}{|L_i|.|L_j|}$$

$$PredictionCF(p_k, d_j) = r\vec{pk} + \frac{\sum_{p\epsilon(s-o)} w_p \times (r_p, d_j - r\vec{p}}{\sum_{p\epsilon(s-o)w_p}}$$

$$+SCS(d_i, d_j) = \frac{|L_i \bigcap L_j|}{|L_i|.|L_j|}$$

$$++SCS(d_i, d_j) = \frac{|L_i \bigcap L_j|}{|L_i|.|L_j|}$$

Where O is set of outlier's type in the mechanism, and S is the set of legitimate neighbours along with their weights. The W and CF are the two variants to measure the trustworthiness of a device. Number of schemes can be used to ensure the trust effectiveness in the system in order to further enhance the accuracy of computation of each communicating device.

$$Prediction(p_k, dj) = r\vec{p}_k + \frac{\sum_{p\epsilon(N-s')} sim(p, p_k) \times (r_p, d_j - r\vec{p})}{\sum_{p\epsilon(N-S')} |sim(p, p_k)| + \sum_{p\epsilon S' w_p}}$$

$$+ \frac{\sum_{p\epsilon s' w_p} \times (r_p, d_j - r\vec{p})}{\sum_{p\epsilon(N-S')|sim(p,p_k)}|}$$

$$+SCS(d_i, d_j) = \frac{|L_i \bigcap L_j|}{|L_i|.|L_j|}$$

The below Algorithm 1 illustrates the brief methods and equations to be followed in order propose a secure communication method. The disabled people may fully rely on the proposed trusted method that is further verified by comparing it with existing mechanisms.

3.5. Complexity

In order to recognize the legitimacy of devices, the interaction among them will be at least $(n-1)$ times in the entire network. That means $(n-1)$ trails will be conducted by the proposed phenomenon while computing their trust in order to recognise or prove the legitimacy of a device. Therefore, the overall complexity of AI device would be $O(\log(n-1))$.

However, along with identification of legitimate devices that takes at least $O(\log(n-1))$ time, some addition computational storage, key management and overheads will be there that will further increase the overall complexity of baseline approach such as $O(n \times (\log(n-1)))$ that is more than the proposed approach. The computational and communicational cost of both baseline schemes and proposed mechanism is presented in Table 3.

Algorithm 1: Algorithm: SCS and Fuzzy trust-distrust recommendation model.

```
Require: Considering two types of smart devices such as altered and ideal
  (legitimate).
Input: (1) Device $D$ consists of n numbers such as $D = d_i, d_j ... d_n$
Output: The device is acting accurately on disabled person
For t = 1→ 250 do
Step 1: Compute the trust values of each device by categorizing them into
  various categories using SCS and fuzzy based trust methods
Step 2: Compute SCS
    $SCS(d_i, d_j) = \frac{|L_i \bigcap L_j|}{|L_i|.|L_j|}$    (2)
Step 3: Accurate decision
End For
    $PredictionW(P_k, d_j) = \frac{\sum_{p\epsilon(s-o)} w_p \times r_p, d_j}{\sum_{p\epsilon(s-o)w_p}} +$    (3)
    $SCS(d_i, d_j) = \frac{|L_i \bigcap L_j|}{|L_i|.|L_j|}$    (4)
Step 3: Altered decision
Step 4: Select the device $d_i, d_j \dots d_n$ having TV ≥ 0.95
[accuracy, decision value, latency, response time] = altered and legitimate $(d_i)$
```

Table 4
Setup Parameters.

Metrics	Description
People	10k
Regions	Three
datasize	100k
1	Completely disagreement
2	Average
3	Above average
4	Good state
Metrics	5, 6
Devices	Altered, Legitimate

4. Performance analysis

In order to evaluate and analyse the recommended trust and distrust by strategizing the behaviour of each device, number of AI and edge based experiments have been conducted on the dataset data.world at (https://data.world/datasets/health). The dataset is of size 100k having data where number of people are living with disabilities by regions. The aim of this experimentation is to present a comprehensive survey on proposed recommendations utilizing SCS and fuzzy trust-distrust methods at AI edge devices.

The setup of parameter is further mentioned in Table 4.

4.1. Setup

The dataset consists of $10k$ people separated with different regions and districts based upon their disability rates. The categories of disabled people are scaled as follows: 1: completely disabled, 2: average, 3: above moderate, 4: good state. Each people have rated at least 5,6 metrices to analyse their disabilities. Now, all the disabilities are carried

Table 5
Simulation metrics for verification of proposed approach.

Metrics	Value
Total no. of communicating devices	250
Total no. of interaction in the network	1026
Compromised devices rate in the network	[5, 10]%
Trusted values to be considered	[0, 1]
Power of transmission	[15, 20] dBm
Communities	Ideal = 999, Altered = 27
Computational resources	10^2 CPU cycle/unit time

out through intelligent devices that needs to be trusted and identifying their legitimacy on a regular basis. The ratings and trust values in test data are considered as behavioural activity of people. The trust-distrust and SCS methods are applied over smart devices that takes an accurate and immediate response to the disabled person in case of any dispensary.

4.2. Performance evaluation

In order to validate the recommended strategies, the proposed mechanism is measured in two evaluation metrics such as mean absolute error (MAE) and data alteration rate (DAR) at AI and edge network. The MEA identifies the deviation of predictions generated by the devices according to their computed trust values in a specific interval of time. On the other hand, DAR measures the alteration in predicted and accurate or absolute trust values measured after identifying the behaviour of each device. The simulation parameters of framework is listed in Table 5.

MEA for a device d_i is identified as follows:

$$MEA(d_i) = \frac{1}{|T_i|} \sum_{p=1}^{|T_i|} |prod_{i,p} - d_{i,p}| \tag{5}$$

Whereas, the DAR is measured as number of devices altered to act maliciously by the intruders in the network.

$$DAR(d_i) = \frac{\sum_{i=1}^{N_d} Pr_i}{\sum_{i=1}^{N_d} T_i} \tag{6}$$

4.3. Role of AI and edge-computing

In order to demonstrate the effectiveness and feasibility of proposed and existing methods, the computation of devices trust are considered for analyzing the number of graphs over mentioned categories for healthcare applications having disabled people. The immediate response along with accurate decisions in real-time situations can be easily feasible using AI edge-computing devices. In addition, the AI-based decision making scheme can be further used to improve and fasten up the communication process. In our proposed approach, the presented results provide relative performance of categories for both worst (malicious) and best (legitimate) cases by computing the trust of each device at AI edge-level. The experimentation is done over 250 devices evaluated over 10 runs against delay, alteration rate, accuracy and response time in comparison of existing work.

4.4. Baseline approaches

The proposed mechanism is validated against two existing (baseline) approaches Pandey et al. [25] and Ahmed and Rasheed [26] as baseline approach 1 and baseline approach 2. While the proposed approach is mentioned as proposed approach. All the graphs are represented in these manner in order to maintain the consistency in validating and comparing the results in the entire paper. Pandey et al. [25] have proposed a secure and efficient home communication mechanism based upon smart devices technology. The authors have proposed a structured design for assisting the disabled people's to health, housing and other necessities. The authors have introduced the development and deployment of such applications with smart technologies using blockchain, cloud computing, sensors and so on for computing and processing the health and home aspects for disabled people. Ahmed and Rasheed [26] have proposed a real time-based face recognition detection system using raspberry PI software. The aim of their paper is to recognise the moving face towards several levels using RFI-cards and passwords for accessing the security systems. The authors have suggested the working model using Raspberry Pi and open CV by providing extra scenarios of face recognition in combination with efficient and cheap machinery systems. Though both the approaches are mentioned for the disabled people while analyzing their surroundings using intelligent devices. However, the real time behaviour and immediate response by including legitimate devices further adds on the accuracy in the system. The proposed framework is maintained and simulated against these two baseline approaches after analyzing the trust or identifying the legitimate device before communicating in the network.

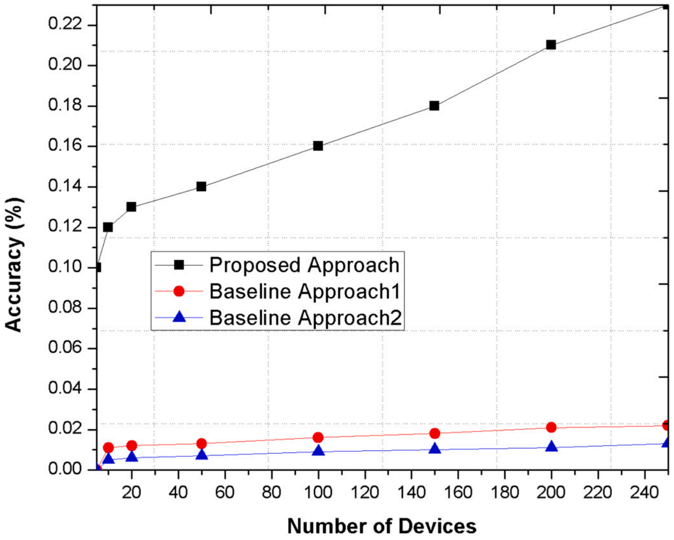

Fig. 3. Accuracy Comparison of Baseline Approaches over Proposed Approach.

4.5. Results and discussion

The results are verified and validated against baseline mechanisms where the proposed approach is tested at AI edge devices for identifying the legitimacy of devices. The proposed framework validates and verifies the accuracy and immediate response according to the surroundings to the disabled people by involving intelligent systems. The proposed scheme successfully analyzed against various security measuring metrics in comparison of baseline approaches. The below text illustrates the detailed explanation of proposed phenomenon out performance as compare to existing approaches through their graphs. Fig. 3 illustrates the accuracy of device analysis using SCS and recommended methods for analysing the trustworthiness of the device. The presented Fig. 3 determines the effectiveness of proposed mechanism as compare to existing mechanism because of their recommendation process that allows multiple verification that leads to accuracy in the system. The computed trust values are further processed and increased and decreased during the transmission process in order to evaluate the legitimacy of each AI device in the network.

Fig. 4 presents the alteration rate where intruders tried to compromise the communicated devices in order to gain their own benefits. The disabled person is unable to move or react immediate upon occurrence

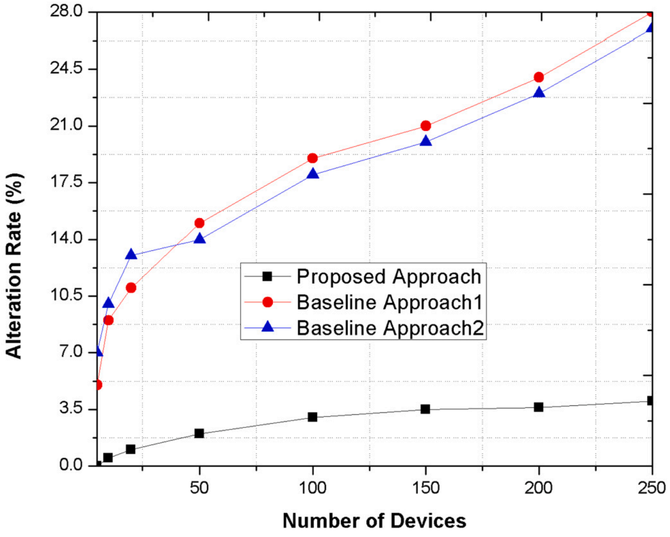

Fig. 4. Alteration Rate Comparison of Proposed Approach over Baseline Approaches.

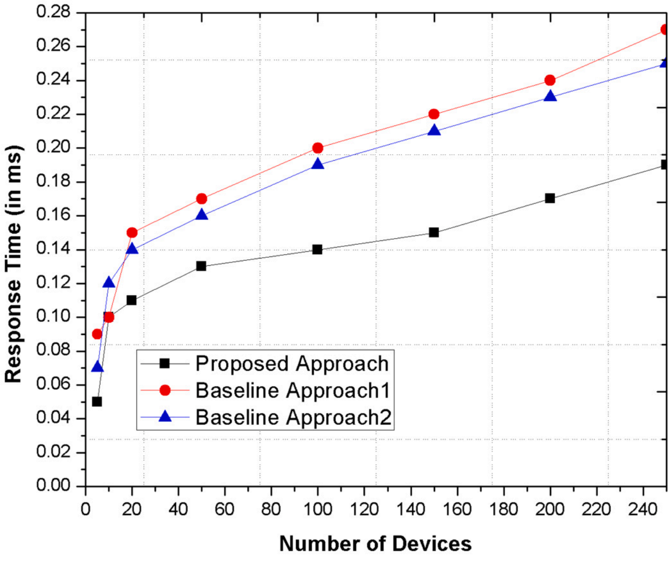

Fig. 5. Response Time Comparison of Proposed Approach over Baseline Mechanisms.

of any mishap. Therefore, it is needed for the devices to be real and accurate while providing any alarm or sending any message to others. The recommended mechanism along with the combination of SCS leads to reduce the data alteration process in proposed phenomenon.

Further, Fig. 5 response time where upon demand the disabled person needs any kind of immediate help or guidance in the system. The legitimated devices who are involved in providing the communication will ensure an immediate response to the person. The presented figure depicts the outperformance of proposed phenomenon as compare to existing one because of their continuous surveillance and management of records in the network. The response time from the legitimate devices are always less than malicious or altered devices.

Furthermore, the latency graph is presented in Fig. 6 that represents the amount of time required to validate the legitimacy of a device in the network. The device is continuously transmitting the information and get involved in the communication mechanism. The proposed mechanism performs better as the legitimacy and alteration behaviour of each communicating device is regularly analysed by the system and does not take extra storage, overhead or delay while proving the legitimacy of a device. The accuracy rates of baselines and proposed algorithms is further presented in Table 6.

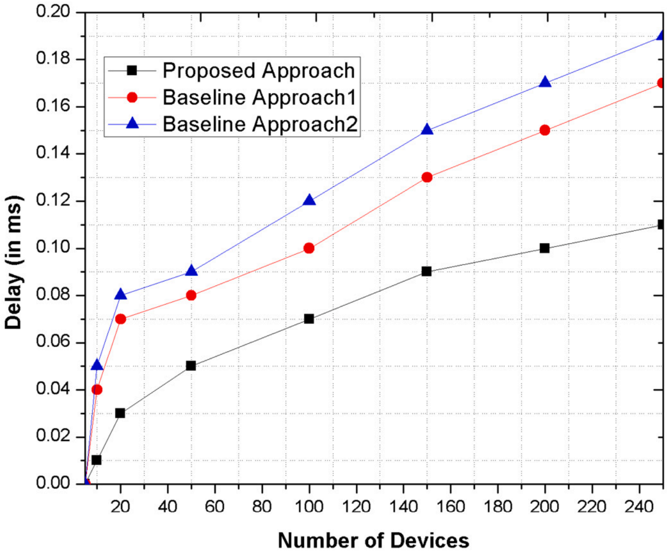

Fig. 6. Delay Comparison of Baseline Approaches over Proposed Approach.

Table 6
Accuracy Rates among Proposed approach and Baseline Approaches.

Algorithms	Accuracy
Quantitative and statistical Analysis	87%
Smart tick utilization system	89%
Social Contact Similarity and Recommendation system	92%

4.6. Summary

Though number of cryptographic or algorithmic based security systems have been proposed by several researchers. Trust-based systems are considered as one of the efficient and significant way of ensuring the security. The AI and edge based trusted mechanisms do not provide additional security cost, storage or key management for providing the security to the system. In this paper, we have proposed two trust-based approaches for immediate and accurate decision making in the network. The SCS and distrust-based recommendation system are considered as one of significant way of identifying the legitimacy of a device while communicating in the network. The proposed phenomenon is simulated and verified against various security metrics for improving and overcoming the existing approaches limitations in terms of quick response, and accuracy. The proposed mechanism also provided an improvement rate of 88% as compare to existing baseline approaches.

5. Conclusion

Though AI-based home automation is the greatest way for the disabled person who is all alone at home and can take good care of his/her house, however, any single mismanagement of non-working of device may completely harm the person. In addition, number of security alarms, automation alteration or cryptographic solutions have been proposed by various scientists, however, these schemes are cannot be fully adopted by the disabled people and in case of emergency, the disabled person is helpless and, in a danger, to handle the situation. The proposed mechanism integrated the distrust-based recommendation system along with SCS mechanism at edge-levels that improved the efficiency and quick action decision corresponding to the altered device that may cause severe harm in the network or to the person.

The proposed mechanism is simulated and verified against various existing scheme over several performance metrics such as delay, alteration rate, accuracy and response time. The proposed mechanism outperforms existing mechanisms that can be further analysed along with their dynamic interactions in the future work.

The proposed framework can be further analyzed over various performance criterion's by discussing data injection, falsification, and accuracy measurement rates in the future direction 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

The authors extend their appreciation to the King Salman Center for Disability Research for funding this work through Research Group no KSRG-2023-118.

References

[1] M. Xu, J.M. David, S.H. Kim, et al., The fourth industrial revolution: opportunities and challenges, Int. J. Finan. Res. 9 (2) (2018) 90–95.
[2] M.D. Williams, R. Douglass, Ensuring the security of defense iot through automatic code generation, in: IoT for Defense and National Security, 2022, pp. 307–323.
[3] T. Higashino, H. Yamaguchi, A. Hiromori, A. Uchiyama, K. Yasumoto, Edge computing and iot based research for building safe smart cities resistant to disasters, in: 2017 IEEE 37th International Conference on Distributed Computing Systems (ICDCS), IEEE, 2017, pp. 1729–1737.
[4] S.S. Kaware, S.K. Sain, Ict application in education: an overview, Int. J. Multidiscipl. Approach Stud. 2 (1) (2015) 25–32.
[5] F. Biagi, Ict and Productivity: A Review of the Literature, 2013.
[6] M. Aazam, S. Zeadally, E.F. Flushing, Task offloading in edge computing for machine learning-based smart healthcare, Comput. Netw. 191 (2021) 108019.
[7] A. Pardos, A. Menychtas, I. Maglogiannis, On unifying deep learning and edge computing for human motion analysis in exergames development, Neural Comput. Appl. 34 (2) (2022) 951–967.
[8] L.W. Koay, Y. Hashim, A review on indoor smart energy managemet system, Int. J. Eng. Technol. Sci. 4 (1) (2017) 122–137.
[9] B. Daengneam, S. Deebhijarn, A. Saengnoree, Integrative medicine and health training for Thai general practitioners (GP): a sem analysis, J. High. Educ. Theory Pract. 23 (1) (2023) 76–89.
[10] M. Kumar, S. Shimi, Voice recognition based home automation system for paralyzed people, Int. J. Adv. Res. Electr. Commun. Eng. 4 (10) (2015).
[11] L.M. Gladence, V.M. Anu, R. Rathna, E. Brumancia, Recommender system for home automation using iot and artificial intelligence, J. Ambient Intell. Humaniz. Comput. (2020) 1–9.
[12] G. Rathee, A. Sharma, R. Kumar, R. Iqbal, A secure communicating things network framework for industrial iot using blockchain technology, Ad Hoc Netw. 94 (2019) 101933.
[13] V. Kant, K.K. Bharadwaj, Fuzzy computational models of trust and distrust for enhanced recommendations, Int. J. Intell. Syst. 28 (4) (2013) 332–365.
[14] R. Chen, J. Guo, F. Bao, Trust management for soa-based iot and its application to service composition, IEEE Trans. Serv. Comput. 9 (3) (2014) 482–495.
[15] A.K. Birajdar, P. More, Healthcare and security system for elderly and disabled people using arm microcontroller, in: 2018 International Conference on Information, Communication, Engineering and Technology (ICICET), IEEE, 2018, pp. 1–5.
[16] E.D. Dimaunahan, A.H. Ballado, F.R.G. Cruz, J.C.D. Cruz, Mfcc and vq voice recognition based atm security for the visually disabled, in: 2017IEEE 9th International Conference on Humanoid, Nanotechnology, Information Technology, Communication and Control, Environment and Management (HNICEM), IEEE, 2017, pp. 1–5.
[17] N. Ragot, F. Bouzbouz, R. Khemmar, J.-Y. Ertaud, A.-M. Kokosy, O. Labbani-Igbida, P. Sajous, E. Niyonsaba, D. Reguer, H. Hu, et al., Enhancing the autonomy of disabled persons: assistive technologies directed by user feedback, in: 2013 Fourth International Conference on Emerging Security Technologies, IEEE, 2013, pp. 71–74.
[18] M. Ziefle, C. Rocker, A. Holzinger, Medical technology in smart homes: exploring the user's perspective on privacy, intimacy and trust, in: 2011 IEEE 35th Annual Computer Software and Applications Conference Workshops, IEEE, 2011, pp. 410–415.
[19] S.S. Priyadharshini, A. Umamakeswari, A survey on various technologies used in human identification for smart home, in: 2018 3rd International Conference on Communication and Electronics Systems (ICCES), IEEE, 2018, pp. 70–77.
[20] Y. Uzunay, K. Bicakci, Sha: a secure voice activated smart home for quadriplegia patients, in: 2007 IEEE International Conference on Bioinformatics and Biomedicine Workshops, IEEE, 2007, pp. 151–158.
[21] L. Norton-Wayne, R. Harwood, J. Wyatt, Easytex-Improving the Quality of Life for the Disabled and the Elderly, 1997.
[22] S. Faroom, M.N. Ali, S. Yousaf, S.U. Deen, Literature review on home automation system for physically disabled peoples, in: 2018 International Conference on Computing, Mathematics and Engineering Technologies (iCoMET), IEEE, 2018, pp. 1–5.
[23] L.A. Rifon, C.R. Costa, M.G. Carballa, S.V. Rodriguez, M.F. Iglesias, Improving the quality of life of dependent and disabled people through home automation and teleassistance, in: 2013 8th International Conference on Computer Science & Education, IEEE, 2013, pp. 478–483.
[24] M.C. Buzzi, M. Buzzi, B. Leporini, F. Akhter, User trust in ecommerce services: perception via screen reader, in: 2009 International Conference on New Trends in Information and Service Science, IEEE, 2009, pp. 1166–1171.
[25] S. Pandey, A. Kumar Dixit, R. Singh, A. Gehlot, S. Kathuria, V. Pandey, Smart devices technology based homes for differently abled people, in: 2023 International Conference on Artificial Intelligence and Smart Communication (AISC), 2023, pp. 319–323.
[26] H.M. Ahmed, R.T. Rasheed, A raspberry pi real-time identification system on face recognition, in: 2020 1st. Information Technology to Enhance e-Learning and Other Application (IT-ELA, 2020, pp. 89–93.
[27] M. Zhang, Y. Liu, A commentary of tiktok recommendation algorithms in mit technology review 2021, Fund. Res. 1 (6) (2021) 846–847.
[28] V. Moscato, A. Picariello, G. Sperli, An emotional recommender system for music, IEEE Intell. Syst. 36 (5) (2020) 57–68.
[29] A.K. Sahoo, S. Mallik, C. Pradhan, B.S.P. Mishra, R.K. Barik, H. Das, Intelligence-based health recommendation system using big data analytics, in: Big Data Analytics for Intelligent Healthcare Management, Elsevier, 2019, pp. 227–246.
[30] A. Abu-Khadrah, M. Jarrah, H. Alrababah, Z.N. Alqattan, H. Akbar, Pervasive computing of adaptable recommendation system for head-up display in smart transportation, Comput. Electr. Eng. 102 (2022) 108204.