Alexandria Engineering Journal 80 (2023) 425–432

Contents lists available at ScienceDirect

Alexandria Engineering Journal

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

ORIGINAL ARTICLE

Trusted and secure communication system using intelligent devices for individuals with disabilities

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:
Trusted schemes
Knowledge factor and friendship similarity approaches
Individuals with disability
Intelligent systems
Trust-based communication

ABSTRACT

Disability has traditionally posed a significant barrier for millions of individuals who are unable to benefit from current technologies such as digital interfaces, the internet, and personal computers. Nowadays, developments in information communication and technology (ICT) are transforming the way we handle and interact with our environment, making it easier and more convenient. However, individuals with disabilities face numerous restrictions and challenges, hindering their full involvement and access to the devices. This paper proposes an efficient and trusted communication mechanism that utilizes knowledge factors and friendship similarity schemes to improve the accessibility and accuracy of information transmission in a networked environment for disabled people. The proposed mechanism ensures the involvement of trusted devices in the network for accuracy and immediate decisions for disabled individual. The proposed approach is validated and compared to existing methods using various security metrics, including social trust, objective trust, experienced trust, and recommended trust. Through this research, we aim to address the barriers faced by individuals with disabilities and provide them with equal opportunities to benefit from modern technological advancements.

1. Introduction

In every society, individuals with physical difficulties face challenges in carrying out their daily household tasks and activities. Those who experience significant difficulties or rely on others for completing their tasks are often referred to as disabled. Disability has traditionally been a barrier for millions of individuals who are unable to benefit from current technologies such as digital interfaces, the internet, and personal computers [1,2]. Recent reports indicate that approximately 7%-10% of the global population, comprising millions of people, are excluded from basic constitutional rights and services. The term disability encompasses individuals whose impairments do not prevent their participation in regular activities, such as walking, seeing, hearing, self-care, and communication.

Nowadays, developments in society, particularly in information communication and technology (ICT), are transforming the way we handle and interact with our environment, making it easier and more convenient [3]. Societal concern revolves around gaining access to knowledge and information through emerging technologies. However, people with disabilities often face significant restrictions and barriers, hindering their full access and involvement. The technological expansion and revolution have introduced novel and improved services for effective communication and societal engagement. Governments are shifting their service provisions to focus more directly on trades and citizens through the internet. ICT is expected to assist disabled individuals by enabling knowledge practices, although their adoption of ICT remains lower compared to non-disabled individuals [4]. For instance, a disabled person attempting to use an ATM to withdraw funds may en-

[*] Corresponding author.
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 (A. Gumaei), mmhassan@ksu.edu.sa (M.M. Hassan).

https://doi.org/10.1016/j.aej.2023.08.044
Received 12 June 2023; Received in revised form 20 July 2023; Accepted 14 August 2023
Available online 1 September 2023

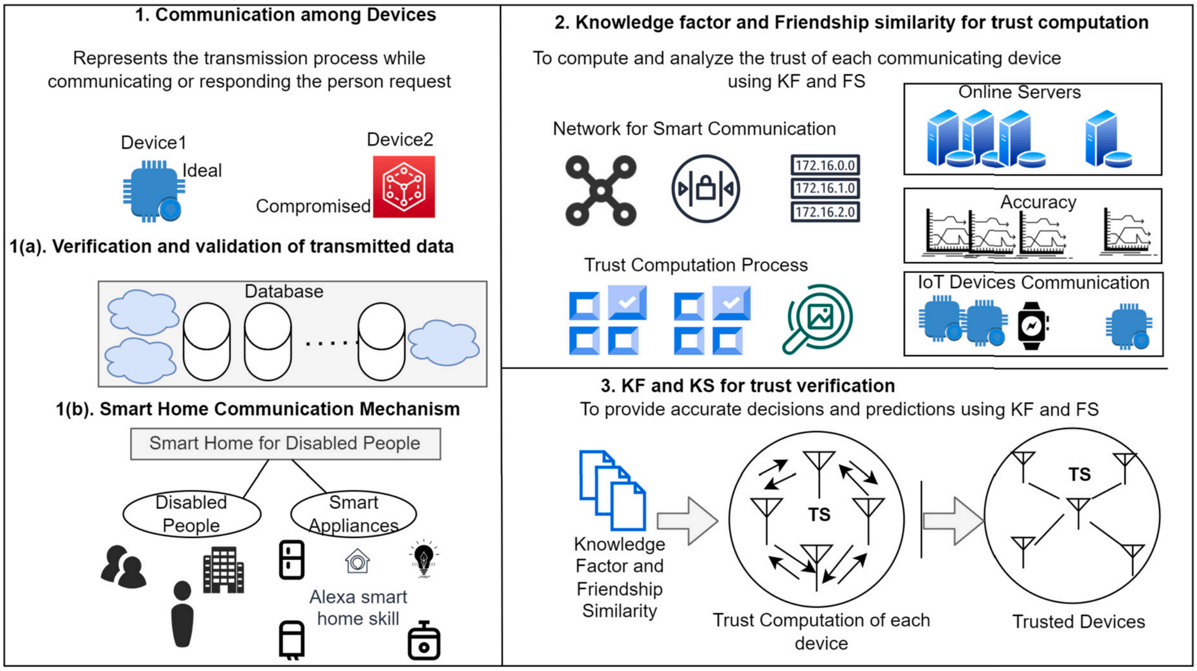
1. Communication among Devices
Represents the transmission process while communicating or responding the person request
Device1
Ideal
Device2
Compromised
1(a). Verification and validation of transmitted data
Database
1(b). Smart Home Communication Mechanism
Smart Home for Disabled People
Disabled People
Smart Appliances
Alexa smart home skill
2. Knowledge factor and Friendship similarity for trust computation
To compute and analyze the trust of each communicating device using KF and FS
Network for Smart Communication
172.16.0.0
172.16.1.0
172.16.2.0
Online Servers
Accuracy
Trust Computation Process
IoT Devices Communication
3. KF and KS for trust verification
To provide accurate decisions and predictions using KF and FS
Knowledge Factor and Friendship Similarity
TS
Trust Computation of each device
TS
Trusted Devices

Fig. 1. Overall process of the proposed framework.

counter challenges despite having access to smart or intelligent devices. A minor alteration in any device could greatly impact the individual's current situation, potentially resulting in financial loss or endangering their well-being.

1.1. Objective

As technology continues to introduce new ways and methods for enhancing people's lives in efficient and remarkable ways, it becomes crucial to ensure the security and protection of intelligent devices involved in automating systems. For individuals with disabilities who require special care and attention, updating and ensuring the accuracy of the objects and devices they rely on for carrying out daily tasks becomes even more significant. To safeguard against malicious activities, it is essential to propose a secure and trusted mechanism specifically tailored for disabled individuals. While numerous schemes have been proposed by scientists and researchers, there is a need for a more precise, automatic, and real-time decision-making process [5,6]. The proposed approach's overall framework, depicted in Fig. 1 having 3 subsections such as communication among devices, Knowledge Factor (KF) and friendship similarity (FS) and contract theory for trust verification. The first subsection communication among devices represents the interaction and transmission process for verification and validating the communication process among intelligent devices. It incorporates smart devices that enable disabled individuals to lead more secure lives at home. Intelligent communication among these devices allows for immediate decisions to prevent harm to individuals. In addition, subsection two represents KF and FS computes the trust among devices which are involved in communication process. The legitimacy of each communicating device is determined through trust models, utilizing knowledge factors and friendship similarity, ensuring a seamless process. Further, third subsection includes KF and FS that shows the continuous surveillance among individuals.

1.2. Contribution

The contribution of this paper is to propose an efficient and secure communication mechanism utilizing knowledge factor and friendship similarity schemes to enhance accessibility and accuracy during information transmission in the network [7,8]. The individual contributions of the paper are organized as follows:

- The social trust-based method, knowledge factor, is employed to measure the legitimacy of each communicating device while assessing device accuracy.
- The knowledge factor (KF) is integrated with the friendship similarity (FS) scheme to further refine recommendations based on users' experiences.
- The proposed approach is validated and verified against existing methods, using a comparative analysis of various security metrics.

Though KF and FS are existing approaches and used by various researchers in the literature. In this paper, our contribution is to integrates both the mechanism and use them in real-time transmission of information in healthcare application for disabled individuals. The theoretical and practical significance of the paper is to establish a secure and efficient communication among devices in the network. Theoretically the integration of KS and FS schemes is to maintain the trust and immediate response to the individuals ensuring real-time communication with the intelligent devices. However, the practical significance of the proposed scheme is to enhance the computational and communicational steps for providing a strong complexity in the network. The immediate response is one of the important factor for the disabled people that are completely relied on intelligent devices. Therefore, it is needed to include secure and accurate smart devices for the real-time decisions that is computed using KF and FS schemes in the proposed approach.

The paper is organized as follows. Section 2 provides a literature survey on the interaction between disabled individuals and smart devices for enhancing their safety. Section 3 discusses the proposed mechanism aimed at ensuring the security and trustworthiness of the communication devices within the network. The validation and verification of the proposed mechanism are presented in section 4. Finally, section 5 concludes the paper and discusses future directions.

2. Related work

This section discusses various security and trust-based communication algorithms, schemes, or approaches proposed by researchers and

Table 1
Summary of existing security methods for disabled people methods.

Authors	Proposed Framework	Method Used	Limitations
Freitas et al. [9]	low-cost edge cutting technology	provide a safety to the disabled persons by continuously supervising their health status	Increases storage overhead
Ch. et al. [10]	Obstacle identification	presented the GPS technology for real time location findings	Provides untrusted scenarios
Hadjadj and Halimi [11]	System-based architecture	Incorporated the fuzzy logic with improved accuracy and uncertainty in knowledge	Increases communication overhead during transmission
Stamford and Peach [12]	Deep learning mechanism	explored the locally linear embedding for visualization	Increases the key management, and communication overheads
Sendra et al. [13]	smart collaboration system	Smart system protocol and network algorithm for verifying the performance	Requires delay in analysis
Olaya and Herrera [14]	Electromyography device for accessing the bio signals	A deadline-aware trusted collaboration mechanism to ensure privacy in the network	Increases the communication overhead
Higashino et al. [15]	enumerated various research issues	Build smart and safe residents for disabled persons	Increases computational overhead
Garbutt and Kyobe [16]	elemental knowledge of life quality	Proposed a conceptual model for investigating the knowledge practices	Incurs long delays in legitimate device identification
Shahkooh and KhodaBandeh [17]	investigated the motivators for addressing disabilities guidelines	Accessing the technical consideration and technical websites for their improvement	Incurs long delays while identifying the malicious threats
Trielsa and Angeline [18]	Focused on three types of disabilities	inclusived the e-commerce platforms and designs for increasing the sales	Has large communication and storage overhead

scientists to facilitate efficient and safe interactions with the environment using intelligent devices.

Freitas et al. [9] have proposed a low-cost edge-cutting technology to provide specialized healthcare services to individuals with special needs, enabling them to live independently at home. The residents were equipped with a range of sensors and intelligent devices to continuously monitor their health status and ensure their safety. Ch. et al. [10] designed a smart stick with obstacle detection capabilities for individuals with visual impairments. The stick incorporated moisture sensors and pit hole detectors to identify water and holes on the street. Additionally, the stick utilized GPS technology for real-time location tracking and included a message alert system in case of accidents. The proposed mechanism was simulated and verified using an ATmega 328U microcontroller, enhancing the mobility of disabled individuals. Hadjadj and Halimi [11] proposed a system-based architecture utilizing semantic web technology to reduce data heterogeneity and improve interoperability. The mechanism incorporated fuzzy logic to handle accuracy and uncertainty in knowledge representation. Stamford and Peach developed a deep learning mechanism for image classification, focusing on nine specific interest points. They explored the use of locally linear embedding to visualize information before and after the classification process, demonstrating superior performance compared to existing mechanisms.

Sendra et al. [13] described a smart collaboration system that enables the mobility of individuals to monitor or recognize activities within a group. The authors proposed a smart system protocol and network algorithm to evaluate the system's performance. Olaya and Herrera [14] developed an electromyography device to access biosignals and improve quality of life. They also utilized a computer access device to capture motion using inertial sensors. Higashino et al. [15] identified research issues in developing Intelligent Community Disaster Countermeasures Systems (ICDCS) to create smart and safe environments for disabled individuals. Their focus areas included resilient disaster response and up-to-date crowd mobility predictions at the edge. Garbutt and Kyobe [16] investigated the fundamental knowledge of life quality for disabled individuals and proposed a conceptual model to explore their knowledge practices and roles within the community. Shahkooh and KhodaBandeh [17] examined motivators for addressing disability guidelines and government efforts to improve technical considerations and accessibility of websites for disabled individuals. Trielsa and Angeline [18] conducted quantitative and statistical analysis to address three types of disabilities—hearing loss, low vision, and physical navigation—achieving an accessibility rate of 62%. They also explored e-commerce platforms and designs to increase sales among disabled individuals. Pandey et al. [19] and Ch. [10] are considered as two baseline approaches as BA1 and BA2 for validating the computed results against proposed framework. Pandey et al. [19] have proposed a structural designing approach for maintaining a sustainable goal to the disabled individuals by integrating with blockchain and intelligent devices. A summary of the related work is presented in Table 1.

2.1. Problem statement

Although scientists have proposed numerous security schemes and approaches [20–23], very few of them have focused on improving the lives of disabled individuals. This paper presents a secure, efficient, and trusted communication mechanism using smart devices for disabled people. In situations where disabled individuals may not be able to take immediate action, the legitimacy of each communicating device should be periodically analyzed. The paper introduces an effective method of communication among smart devices used by disabled individuals, utilizing trust-based schemes such as Knowledge Factor (KF) and Friendship Similarity (FS). The devices which are analyzed depending upon their various communicating factors are further categorized into two different types such as legitimate and malicious after computing their trust values using KF and FS schemes.

3. Proposed framework

Trust mechanisms play a crucial role in identifying the legitimacy and detecting behavioral changes in communicating devices. While various cryptographic and algorithmic approaches have been presented, these methods often introduce computational delays, key management challenges, and storage overhead. Numerous trust-based methods exist, including social trust, objective trust, experienced trust, recommended trust, and more. In our problem statement, where safety and information accuracy are of utmost importance, this paper integrates experienced trust and social trust using KF and FS trust methods to ensure network accuracy, as illustrated in Fig. 2. The depicted Fig. 2 represents how the devices are categorized into legitimate and malicious according to their various behavioral types. The KF and FS are the two trust-based metrics that are used to surveillance each individual communicating in the network. The disabled person that is completely reliable on the intelligent devices can be easily communicate with them. The trusted devices will communicate efficiently in real time situations in the network.

As many abbreviations and symbols are used in the paper, they are listed and described in Table 2.

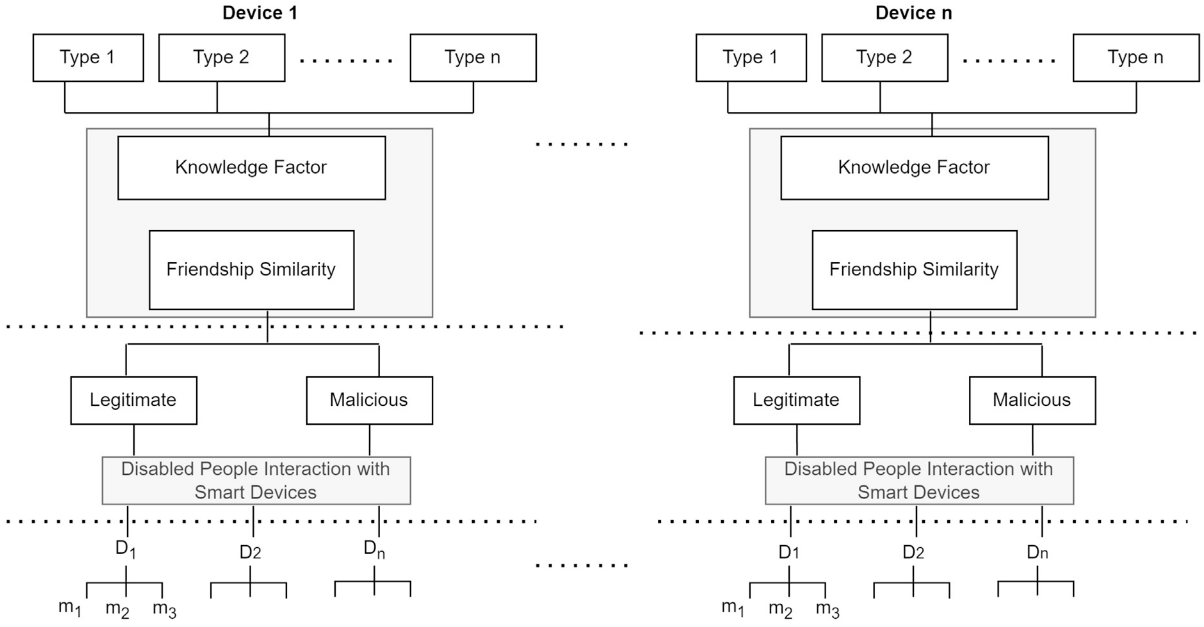

Fig. 2. Proposed Model.

Table 2
Definition and Abbreviations.

Symbol	Description
KF	Knowledge Factor
FS	Friendship Similarity
$\vec{BV}_i$	Binary Vector of device i
$FriSim_D(d_i,d_j)$	Friendship similarity among device i and device j
C_j	Communication rating
$SiandS_j$	List of surrounding or friends
$Cons_{rat}$	Considered ratings
$Non-cons_{rat}$	Non considered ratings
$Indiff_{rat}$	Indifferent ratings
AA_{d_i,d_j}	Agreement-agreement among d_i and d_j
DD_{d_i,d_j}	Disagreement-disagreement among d_i and d_j
AD_{d_i,d_j}	Agreement-disagreement among d_i and d_j
DA_{d_i,d_j}	Disagreement-agreement among d_i and d_j
$exp_belief^{d_i,d_j}$	Trust experience of d_i over d_j
$exp_disbelief^{d_i,d_j}$	Distrust experience of d_i over d_j
Belief	Verification time of result broadcasting
T_n	Transmission time of unverified device
$U_{bn}(k)$	Profit of TS using type-$-k$ nodes
U_k	Utility Function

Table 3
Trust Values.

Devices	TV	TV	TV	TV	TV
D_i	5	5	5	5	5
D_j	1	1	1	1	1

3.1. Knowledge factor (KF)

Distrust and insufficient trust values leads to stay away from the technology, therefore, there must be some other factors to include while computing the accurate trust value of any device. Knowledge factor is one of trust method that is based on repeated interaction among devices to improve the perfection in the device. Table 3 determines the rating of two devices $d1$ and $d2$ by analyzing their common behavior on a scale of $1-5$.

The existing models computes the distrust and trust between devices; however, our proposed model computes the belief of each other's including experience and recommendation by others in the network. Based upon knowledge factor, the proposed model computes the belief, disbelief, recommendation and experience values accordingly. The definition of each metric according to proposed model which is based upon identifying the legitimacy of devices in disabled people as illustrates as follows:

- **Belief**: it is defined as theoretical aspect a device has about other positive behavior based upon their past interactions.
- **Disbelief**: it is defined as theoretical aspect a device has about negative or over active behavior based upon their past interactions.
- **Recommendation**: it is defined as the advice of a device for another device that can be rely upon based upon recommended device trust history.
- **Experience**: experience is the total amount of interactions either positive or negative in a network based upon their present or past communications.

3.2. Friendship similarity (FS)

It is defined as one of the powerful social intimacies for finalizing the recommendations based upon experiences. After two devices d_i and d_j exchange their list of friends or surroundings as s_i and s_j, the can compute 2 binary vectors as $\vec{BV}_i$ and $\vec{BV}_j$, the vector will be 1 if the device is in friend list otherwise the vector will be 0. Let, $||\vec{A}||$ be the norm of vector $\vec{A}$ and $|\vec{B}|$ be the cardinality of set B, the cosine similarity of $\vec{BV}_i$ and $\vec{BV}_j$ can be computed as $FriSim_f(d_i,d_j)$:

$$FriSim_f(d_i,d_j) = \frac{\overrightarrow{BV_i,} \vec{BV}_j}{||\vec{BV}_i||\ ||\vec{BV}_j||} = \frac{|S_i \bigcap S_j}{\sqrt{|S_i|.|S_j|}} \tag{1}$$

The classification of experience is described in two different ways such as rely or deny of a device as exp_{rely} and exp_{deny}. In case where both the devices agreed upon same values or ratings such as device D_j's rating on an communication C_j is represented as R_dj, C_j. Now D_i's rating R_{di^dj} (I) for another device D_j after the interaction I is defined as:

$$\left.\begin{array}{r} 1\ Otherwise \\ 2\ 2.0 < |R_{d_j,c_j} - R_{d_i,c_i}| < 3.0 \\ 3\ 1.0 < |R_{d_j,c_j} - R_{d_i,c_j}| <= 2.0 \\ 4\ 0.5 < |R_{d_j,c_j} - R_{d_i,c_j}| <= 1.0 \\ 5\ 0.0 < |R_{d_j,c_j} - R_{d_i,c_j}| <= 0.5 \end{array}\right\} \tag{2}$$

The rating set of device D_i has given on another device D_j for all interactions between them as $R_{d_i}(D_j) = R_{d_i}^{d_j}(i)$ for all λ, and collection of all interactions of d_i to all rest devices in the system.

The ratings set for considered, not considered and indifferent interactions are presented as $consi_{rat}^{d_i}$, $d_j(I)$, $nonconsi_{rat}^{d_i}$, $d_j(I)$ and $indiff_{rat}^{d_i}$, $d_j(I)$ are illustrated as:

$$Cons_{rat}^{d_i,d_j}(I) = R_{d_i}^{d_j}(I)|\forall R_{d_i}^{d_j}(I)\epsilon R_{d_i}(d_j) and R_{d_i}^{d_j}(I) > 3$$

$$nonCons_{rat}^{d_i,d_j}(I) = R_{d_i}^{d_j}(I)|\forall R_{d_i}^{d_j}(I)\epsilon R_{d_i}(d_j) and R_{d_i}^{d_j}(I) < 3$$

$$Indiff_{rat}^{d_i,d_j}(I) = R_{d_i}^{d_j}(I)|\forall R_{d_i}^{d_j}(I)\epsilon R_{d_i}(d_j) and R_{d_i}^{d_j}(I) = 3$$

In order to further measure the rely and deny of trust among devices, two fuzzy sets on each device is determined under agreement and disagreement as:

$$\left.\begin{array}{r} Aggrement_{d_i} 0\ R_{d_i}^{d_j}(I) = 1 \\ \frac{(R_{d_i}^{d_j}(I)-1)}{4} 1 < R_{d_i}^{d_j}(I) < 5|\forall R_{d_i}^{d_j}(I)\epsilon A_i \\ 1\ R_{d_i}^{d_j}(I) = 5 \end{array}\right\} \tag{3}$$

$$\left.\begin{array}{r} Disaggrement_{d_i} 1\ R_{d_i}^{d_j}(I) = 1 \\ \frac{5-(R_{d_i}^{d_j}(I))}{4} 1 < R_{d_i}^{d_j}(I) < 5|\forall R_{d_i}^{d_j}(I)\epsilon A_i \\ 0\ R_{d_i}^{d_j}(I) = 5 \end{array}\right\} \tag{4}$$

There are four possible ways of these two fuzzy sets between devices d_i and d_j namely agreement-agreement $AA_{(d_i,d_j)}$, disagreement-disagreement $DD_{(d_i,d_j)}$, agreement-disagreement $AD_{(d_i,d_j)}$ and disagreement-agreement $DA_{(d_i,d_j)}$. The computational model for identifying the legitimacy of devices are categorized in these four ways namely $recommendation_{belief}$ and $recommendation_{disbelief}$ utilizing these agreement and disagreement values are determined as follows:

$$Recommendation_{belief} = Agg(d_i, d_j)$$
$$(1 - agg(d_i, d_j) \times reliability(d_i, d_j)$$
$$Recommendation_{disbelief} = Disagg(d_i, d_j)$$
$$(1 - agg(d_i, d_j) \times reliability(d_i, d_j)$$

The reliability measures the uncertainty and ignorance of trust in the network that can be further termed as:

$$Reliability(d_i, d_j) = \frac{1 - |indiff_{ra}^{d_i,d_j}(I)| + |indiff_{rat}^{d_i,d_j}(I)|}{|R_{d_i}(d_j)| + |R_{d_i}(d_j)|} + FriSim_{d_i,d_j}$$

Further, the experience of one device over another as $exp_{belief}^{d_i,d_j}$ and $exp_{disbelied}^{d_i,d_j}$ is computed as:

$$Exp_{belief}^{d_i,d_j} = \frac{|P_j^+|}{max|P_i|, |P_j|} \times \frac{|P_j^+|}{max|P_i|\forall i} + FriSim_{d_i,d_j}$$

$$Exp_{disbelief}^{d_i,d_j} = \frac{|P_j^-|}{max|P_i|, |P_j|} \times \frac{|P_j^-|}{max|P_i|\forall i} + FriSim_{d_i,d_j}$$

Where $|P_j^+|$ and $|P_j^-|$ are positive and negative interactions of device j. Finally, the belief and disbelief values from device d_i and device d_j are computed as:

$$belief_{d_i}^2(d_j) = \frac{2 \times rec_{belief} \times exp_{belief}^{d_i,d_j}}{(rec_{belief} + exp_{belief}^{d_i,d_j}} + FriSim_{d_i,d_j}$$

$$disbelief_{d_j}^2(d_j) = \frac{2 \times rec_{disbelief} \times exp_{disbelief}^{d_i,d_j}}{(rec_{disbelief} + exp_{disbelief}^{d_i,d_j}} + FriSim_{d_i,d_j}$$

Once the belief and disbelief of the devices are computed using knowledge factor and friendship similarity, the final trust values of beliefs and disbelieves are computed as follows:

$$Belief_{d_i}(d_j) = \frac{w_1 \times belief_{d_i}^1(d_j) + w_2 \times belief_{d_i}^2(d_j)}{w_1 + w_2} + FriSim_{d_i,d_j}$$

$$Disbelief_{d_i}(d_j) = \frac{w_1 \times disbelief_{d_i}^1(d_j) + w_2 \times disbelief_{d_i}^2(d_j)}{w_1 + w_2} + FriSim_{d_i,d_j}$$

An algorithm for recognizing the legitimacy of smart devices so that disabled persons can fully rely on the communicated device can be analyzed through their beliefs and disbelief's as mentioned in Algorithm 1. The Algorithm 1 illustrates the computation of trust values using KF and FS of communicating devices in the network.

Algorithm 1: Friendship Similarity and Knowledge Factor Trusted Models

```
Require: Both types of devices (legitimate, altered) are represented in graph
  network.
Input: (1) Number of devices $D$, $D = d_i, d_j ... d_n$
Output: Device is either legitimate or altered
For $t^- \rightarrow 0$ do
Step 1: Compute KS in order to determine the belief and disbelief
    $FriSim_f(d_i, d_j) = \frac{\vec{BV_i}, \vec{BV_j}}{||\vec{BV_i}||\ ||\vec{BV_j}||} = \frac{|S_i \bigcap S_j}{\sqrt{|S_i|.|S_j|}}$
Step 2: Belief
    $belief_{d_i}^2(d_j) = \frac{2 \times rec_{belief} \times exp_{belief}^{d_i,d_j}}{(rec_{belief} + exp_{belief}^{d_i,d_j}} + FriSim_{d_i,d_j}$
Step 3: Disbelief
    $disbelief_{d_j}^2(d_j) = \frac{2 \times rec_{disbelief} \times exp_{disbelief}^{d_i,d_j}}{(rec_{disbelief} + exp_{disbelief}^{d_i,d_j}} + FriSim_{d_i,d_j}$
End For
Step 3: Choose $d_i, d_j ... d_n$ having TV ≥ 9.5
[weight, accuracy, decision values] = belief and disbelief $(d_i, d_j)$
```

4. Performance analysis

Table 4 and Table 5 show the simulation parameters and the predefined values used for evaluation. In order to extract the trust features based upon their internal behavior and activities used in knowledge factor and friendship similarity score, it is needed to trace and track number of features. The authors have used SIGCOMM-2009 conference that is available on CRAWDADA [24,25] which contains activity logs, device proximity, data layer and message application logs. The number of features has been decided such as RS, CFD, MC that is related to IoT raw data for experimentation.

Table 4
Simulation Parameters of Framework.

Parameter	Value
Number of devices	250
Number of Interaction	1256
Rate of compromised devices	[5, 20]%
Trust values	[0, 1]
Transmission power	[5, 20] dBm
Communities	Legitimate = 1012 and Altered = 244
Computational resources	10^3 CPU cycle/unit time

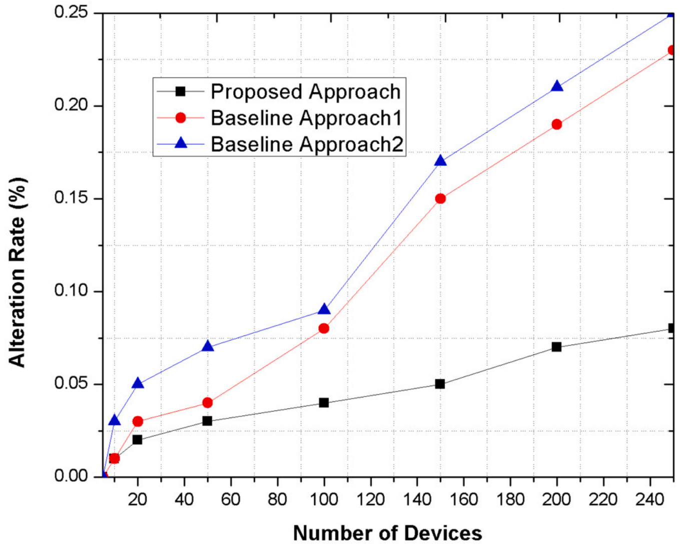

Fig. 3. Accuracy.

4.1. Simulation setup

Table 4 leads to the number of parameters finalized for dataset. In order to match with the IoT content, each device is having at least 1 interaction between each other among 250. After obtaining the trust vector $\vec{BV}_i$ for each pair of devices, the results are deliberately omitted from very close proximity. The number of devices for validating the results are considered as 250 that are interacting with each other around 1256 times. The number of compromised devices for validating the proposed approach is increasing with the increase of network size with a rate of 5% to 20% maximum respectively. The communities that are considered initially as legitimate and compromised during the transmission processes are 1012 and 244. The resources are computed at 10^3 cycles per CPU time.

Fig. 3 illustrates the accuracy rate distribution with respect to each feature as discussed above. It can be observed from the figure that the alteration rate is close to 0.25 as the information is collected from the devices are closely speeded. The trust value is normalized between 0 and 1, one means the device is 100% trustworthy and 0 means untrusted interactions among devices.

However, the alteration represents the weaker associations due to dissimilar intentions in their behavior. In addition, the variation of trust is distributed with respect to their duration, co-operatives and frequency during the transmission of information between devices. The simulation performance of proposed model is done along with their complexity while interacting among each other. For analyzing the behavior of each device, approximate 1500 interactions are used to validate the legitimacy of communicating device. The verification delay to identify the legitimacy of proposed mechanism is depicted in Fig. 4 that shows the amount of time required to analyze the trust and response time of each communicating device upon request on the demand of people.

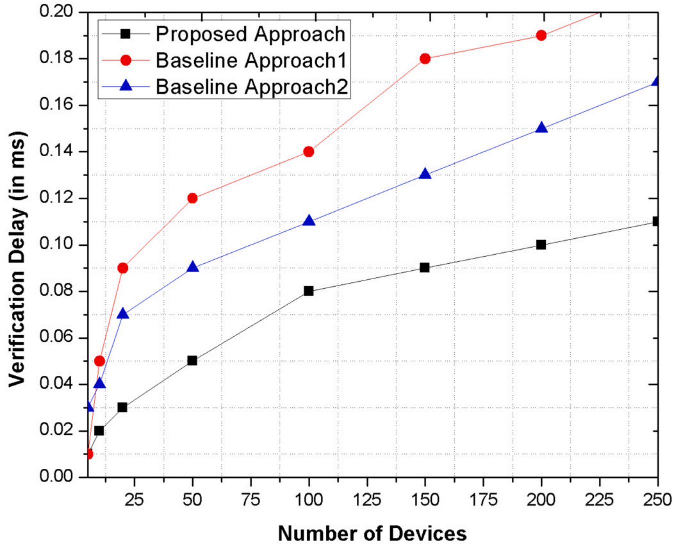

Fig. 4. Verification Delay.

4.2. Baseline approaches

The proposed mechanism is simulated against two recent mechanisms of providing an efficient security to the disabled individuals. Pandey et al. [19] and Ch. [10] are considered as two baseline approaches as BA1 and BA2 for validating the computed results against proposed framework. Pandey et al. [19] have proposed a structural designing approach for maintaining a sustainable goal to the disabled individuals by integrating with blockchain and intelligent devices. Ch, et al. [10] have proposed an edge-based smart application mechanism for disabled individuals who are visually impaired. The need to edge-computing using intelligent devices can be used to ensure a secure communication mechanism. In addition, our proposed mechanism represents the benefits of integrating trust-based recommendation system at edge-computing for speed up the communication process with accuracy and security for real-time processing in the network.

4.3. Results and discussion

In order to filter out the trusted devices, Fig. 5 represents the various results obtained after applying friendship similarity and aggregation schemes. Fig. 5 represents the trust values distribution as compared to existing approach with respect to the mentioned features. Similarly, Fig. 5 represents the boundary among untrustworthy and trustworthy regions. In addition, Fig. 6 illustrates the slightly variation in results as compare to others. The untrustworthy and trustworthy nature of any device can be easily computed by recognizing their behavior in the network. The devices having higher trust values are active with higher friendship similarity and aggregation rate as compare to the device having less trust values.

The belief, disbelief and difference among values is easily identified in different colors as depicted in 6 by counting various features. The alteration rate and blockchain verification latency can be easily recognizable in succeeding Fig. 5 and Fig. 6.

The alteration of device compromised by the intruders in order to gain their own benefits can be easily done in existing mechanisms as compare to proposed scheme as shown in Fig. 7. The integration of aggregation methods and friendship similarity score made the complex computation process to prove the legitimacy of device during transmission of information in the network. The alteration rate of proposed scheme as depicted in Fig. 5 is very less as compare to existing schemes because of blockchain mechanism that maintains the transparency in the network.

Table 5
Algorithm comparison.

S.No.	Approaches	Trustworthy	Devices	Untrustworthy
1	Baseline Scheme1, Baseline Scheme2, Proposed Approach	50	43, 45, 47	7, 5, 3
2	Baseline Scheme1, Baseline Scheme2, Proposed Approach	100	78, 89, 97	22, 11, 3
3	Baseline Scheme1, Baseline Scheme2, Proposed Approach	150	110, 125, 137	40, 25, 13
4	Baseline Scheme1, Baseline Scheme2, Proposed Approach	200	175, 187, 191	25, 13, 9
5	Baseline Scheme1, Baseline Scheme2, Proposed Approach	250	195, 235, 243	55, 15, 7

Table 6
Accuracy Percentage.

Approaches	Algorithms	Accuracy %	Time Complexity	Space Complexity
Baseline Approach 1	Structural Design	89%	n × log (n)	n^2
Baseline Approach 2	Edge-based Smart Application	90%	n × log (n)	n^2
Proposed Approach	KF and friendship similarity	93%	log (n)	n

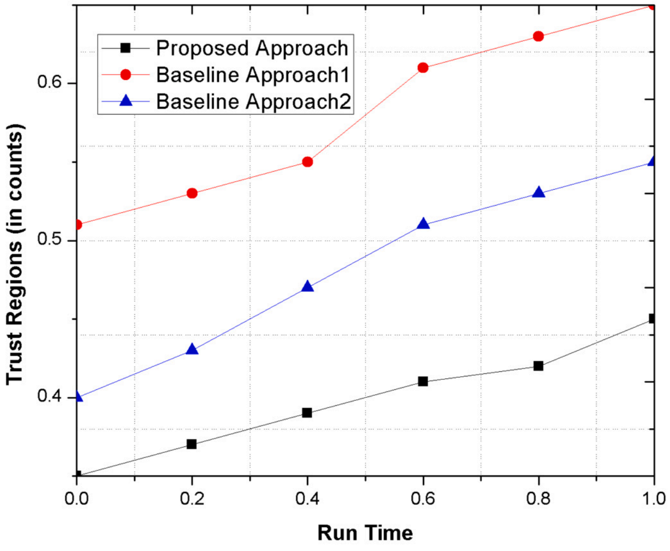

Fig. 5. Trust Regions.

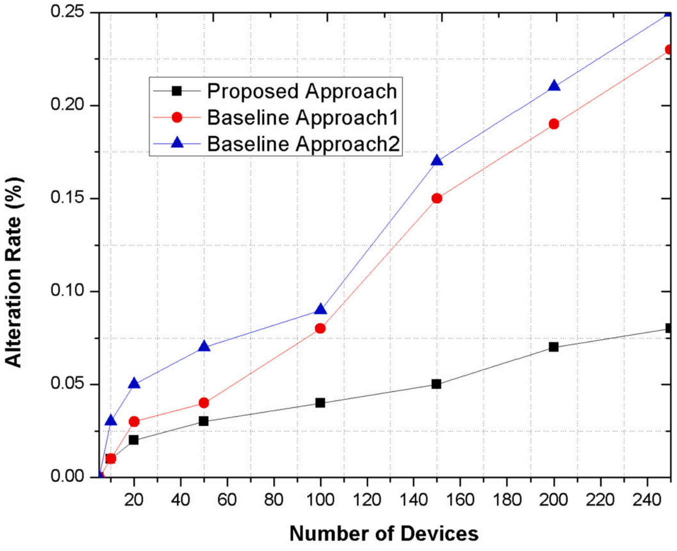

Fig. 7. Alteration Rate.

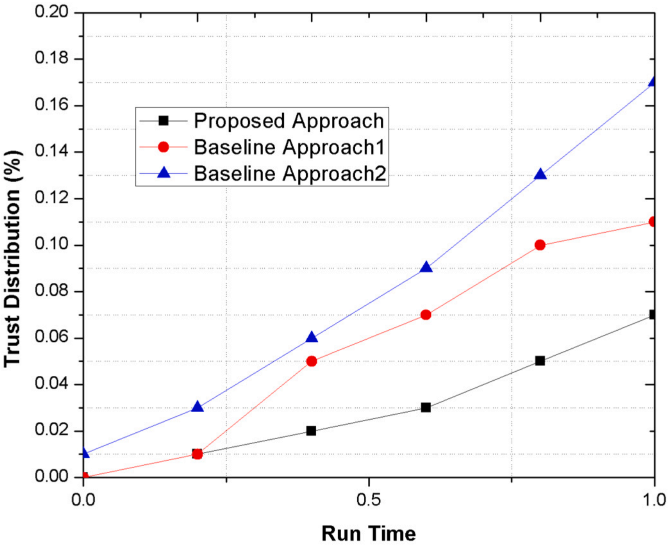

Fig. 6. Trust Distribution.

4.4. Summary

Similarly, the verification latency of both proposed and existing schemes where the verification process or delay of proposed mechanism during the establishment of network is approximately similar as compare to existing schemes. However, during the interaction process, the latency in case of proposed is very less as compare to existing as the trust values are computed after a specific interval of time in the network. The computed trust values reduce the further computational and verification process as highly trusted devices are the part of blockchain network. However, existing schemes, the accuracy and trustworthiness are measured before the interaction process and leads to increase the delay for further verification of devices in the network. The summary of accuracy percentage and complexity of schemes proposed by the authors is shown in Table 6. The trusted proposed mechanism can be further used in other applications while communicating and transmitting the information among devices such as transportation systems. The intelligent transportation system where intelligent devices are mandatory role for ensuring a real-time accurate and automotive decision-making. It is needed to include only trusted devices in the communication process. The proposed scheme KF and FS can be further used in ITS for providing an efficient and secure communication system. The limitation of proposed mechanism is continuous vigilance of the communicated devices while transmitting the information in the network. The continuous surveillance of devices may further enhance the accuracy with reduced delay that is considered as an important factor in case of disabled people where real-time response is taken at the foremost priority. In this paper, the devices are categorized as legitimate or altered however, we can not identify the legitimacy of a device while transmitting the information in real time situations.

5. Conclusion

People who experience a higher level of difficulty or depend on others for the completion of their tasks are often referred to as disabled. Disability has traditionally been a barrier for millions, who cannot take advantage of present technologies such as digital interfaces, the internet, and personal computers. According to a recent report, approximately 7-10% of the worldwide population, where millions of people are excluded from basic constitutional rights and services. The proposed mechanism efficiently able to provide a secure communication mechanism using trust-based approaches for providing an immediate response to the disabled people. The proposed mechanism is validated through the results that further outperforms various existing approaches in comparison to several security metrics, such as social trust, objective trust, experienced trust, and recommended trust.

The dynamic alteration of legitimate devices by the intruders along with pattern recognition system can be further considered as an important factor. In addition, the continuous surveillance of the devices during real-time transmission of information must be analyzed and examined with some security techniques and approaches in the future communication 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] A.J. Hogan, Social and medical models of disability and mental health: evolution and renewal, CMAJ, Can. Med. Assoc. J. 191 (1) (2019) E16–E18.
[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] S.S. Kaware, S.K. Sain, Ict application in education: an overview, Int. J. Multidiscip. Approach & Studies 2 (1) (2015) 25–32.
[4] R. Jamwal, H.K. Jarman, E. Roseingrave, J. Douglas, D. Winkler, Smart home and communication technology for people with disability: a scoping review, Disabil. Rehabil., Assist. Technol. 17 (6) (2022) 624–644.
[5] S. Yu, K. Lv, Z. Shao, Y. Guo, J. Zou, B. Zhang, A high performance blockchain platform for intelligent devices, in: 2018 1st IEEE International Conference on Hot Information-Centric Networking, HotICN, IEEE, 2018, pp. 260–261.
[6] O.H. Chi, G. Denton, D. Gursoy, Artificially intelligent device use in service delivery: a systematic review, synthesis, and research agenda, J. Hosp. Mark. Manag. 29 (7) (2020) 757–786.
[7] H. Yang, F.R. Fan, Y. Xi, W. Wu, Bio-derived natural materials based triboelectric devices for self-powered ubiquitous wearable and implantable intelligent devices, Adv. Sustain. Syst. 4 (9) (2020) 2000108.
[8] H. Isyanto, A.S. Arifin, M. Suryanegara, Design and implementation of iot-based smart home voice commands for disabled people using Google assistant, in: 2020 International Conference on Smart Technology and Applications, ICoSTA, IEEE, 2020, pp. 1–6.
[9] D.J. Freitas, T.B. Marcondes, L.H. Nakamura, R.I. Meneguette, A health smart home system to report incidents for disabled people, in: 2015 International Conference on Distributed Computing in Sensor Systems, IEEE, 2015, pp. 210–211.
[10] R. Ch, C. Rupa, et al., Edge computing based smart application system for visually impaired challengers, in: 2023 International Conference on Sustainable Computing and Data Communication Systems, ICSCDS, IEEE, 2023, pp. 1382–1389.
[11] A. Hadjadj, K. Halimi, Improving health disabled people through smart wheelchair based on fuzzy ontology, in: 2021 8th International Conference on Internet of Things: Systems, Management and Security, IOTSMS, IEEE, 2021, pp. 1–6.
[12] J. Stamford, B. Peach, Scene detection using convolutional neural networks, in: 2nd IET International Conference on Technologies for Active and Assisted Living, TechAAL 2016, IET, 2016, pp. 1–6.
[13] S. Sendra, E. Granell, J. Lloret, J.J. Rodrigues, Smart collaborative system using the sensors of mobile devices for monitoring disabled and elderly people, in: 2012 IEEE International Conference on Communications, ICC, IEEE, 2012, pp. 6479–6483.
[14] A.F. Ruiz-Olaya, C. Lara-Herrera, Enhancing e-accessibility of disabled people using low-cost technology, in: 2016 8th Euro American Conference on Telematics and Information Systems, EATIS, IEEE, 2016, pp. 1–5.
[15] 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.
[16] M. Garbutt, M. Kyobe, Knowledge practices of people with disabilities and the role of ict, in: Fourth International Conference on Information and Communication Technology and Accessibility, ICTA, IEEE, 2013, pp. 1–6.
[17] K.A. Shahkooh, H. KhodaBandeh, Necessity of accessibility to e-government websites for disabled people, in: 2006 2nd International Conference on Information & Communication Technologies, vol. 1, IEEE, 2006, pp. 911–916.
[18] C.J. Trielsa, M. Angeline, The effect of inclusive design on easy accessibility for disabled e-commerce users in Indonesia, in: 2023 17th International Conference on Ubiquitous Information Management and Communication, IMCOM, IEEE, 2023, pp. 1–4.
[19] S. Pandey, A.K. 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, IEEE, 2023, pp. 319–323.
[20] M. Burhan, H. Alam, A. Arsalan, R.A. Rehman, M. Anwar, M. Faheem, M.W. Ashraf, A comprehensive survey on the cooperation of fog computing paradigm-based iot applications: layered architecture, real-time security issues, and solutions, IEEE Access 11 (2023) (2023) 73303–73329.
[21] G. Morabito, C. Sicari, A. Ruggeri, A. Celesti, L. Carnevale, Secure-by-design serverless workflows on the edge–cloud continuum through the osmotic computing paradigm, Int. Things 22 (2023) 100737.
[22] N. Ramkumar, D.K. Renuka, An analysis on augmentative and assistive technology for the speech disorder people, in: 2023 International Conference on Intelligent Systems for Communication, IoT and Security, ICISCoIS, IEEE, 2023, pp. 601–607.
[23] R. Nouisser, S.K. Jarraya, M. Hammami, Deep learning and kinect skeleton-based approach for fall prediction of elderly physically disabled, in: 2022 IEEE/ACS 19th International Conference on Computer Systems and Applications, AICCSA, IEEE, 2022, pp. 1–7.
[24] A.-K. Pietiläinen, E. Oliver, J. LeBrun, G. Varghese, C. Diot, Mobiclique: middleware for mobile social networking, in: Proceedings of the 2nd ACM Workshop on Online Social Networks, 2009, pp. 49–54.
[25] P. Anna-Kaisa, D. Christophe, CRAWDAD dataset thlab/sigcomm2009, 2012.