Cognitive Computation
https://doi.org/10.1007/s12559-018-9543-3

A Brain-Inspired Trust Management Model to Assure Security in a Cloud Based IoT Framework for Neuroscience Applications

Mufti Mahmud[1] · M. Shamim Kaiser[2] · M. Mostafizur Rahman[3] · M. Arifur Rahman[4] · Antesar Shabut[5] · Shamim Al-Mamun[6] · Amir Hussain[7]

Received: 29 December 2017 / Accepted: 10 January 2018

Abstract

Rapid advancement of Internet of Things (IoT) and cloud computing enables neuroscientists to collect multilevel and multichannel brain data to better understand brain functions, diagnose diseases, and devise treatments. To ensure secure and reliable data communication between end-to-end (E2E) devices supported by current IoT and cloud infrastructures, trust management is needed at the IoT and user ends. This paper introduces an adaptive neuro-fuzzy inference system (ANFIS) brain-inspired trust management model (TMM) to secure IoT devices and relay nodes, and to ensure data reliability. The proposed TMM utilizes both node behavioral trust and data trust, which are estimated using ANFIS, and weighted additive methods respectively, to assess the nodes trustworthiness. In contrast to existing fuzzy based TMMs, simulation results confirm the robustness and accuracy of our proposed TMM in identifying malicious nodes in the communication network. With growing usage of cloud based IoT frameworks in Neuroscience research, integrating the proposed TMM into existing infrastructure will assure secure and reliable data communication among E2E devices.

Keywords ANFIS · Neuro-fuzzy system · Cybersecurity · Behavioral trust · Data trust · Quality of service · Neuroscience big data · Brain research

Introduction

In recent years, biological data has grown significantly, coupled with technological developments, enabling scientists to acquire data simultaneously from multiple levels and channels of a living system [1], and also simulate large scale brain networks [2, 3]. One of the major contributors to this biological big data is Neuroscience [4]. Brain signals, e.g., Electroencephalogram (EEG), Electrocorticogram (ECoG), Neuronal Spikes (AP), Local Field Potentials (LFPs) along with brain imaging techniques, e.g., Magnetoencephalography (MEG), Magnetic Resonance Imaging (MRI), Functional MRI (fMRI), Positron Emission Tomography (PET) have been extensively used in the diagnosis of neurodegenerative diseases [5, 6], neuropsychiatric disorders [7], and developmental disorders such as Autism Spectrum Disorder [8]. Additionally, this data has been effectively utilized in developing various data-driven disease models [9, 10].

Modern day Neuroscience research is driven by data (see Fig. 1). Both clinical and experimental neuroscience research generate huge amounts of data [11] and analyzing these to draw meaningful conclusions is very challenging [12]. The extracted knowledge from these data facilitates the development and refining of data-intensive models and descriptions of underlying biological phenomena for facilitating experimental design [13]. The data analytics and modeling phases are computationally intensive, and

Mufti Mahmud and M. Shamim Kaiser are co-first authors.

✉ Mufti Mahmud
muftimahmud@gmail.com

✉ M. Shamim Kaiser
mskaiser@juniv.edu

1 NeuroChip Lab, Department of Biomedical Sciences, University of Padova, Via f. Marzolo 3, 35131 Padova, Italy

2 Institute of Information Technology, Jahangirnagar University, 1342 Dhaka, Bangladesh

3 School of Mathematics, American International University - Bangladesh, 1213 Dhaka, Bangladesh

4 Department of Computer Science, University of Sheffield, Sheffield, S1 4DP, UK

5 Anglia Ruskin University, CM1 1SQ Chelmsford, UK

6 Saitama University, Saitama, 338-8570, Japan

7 University of Stirling, FK9 4LA Stirling, Scotland, UK

Published online: 02 April 2018

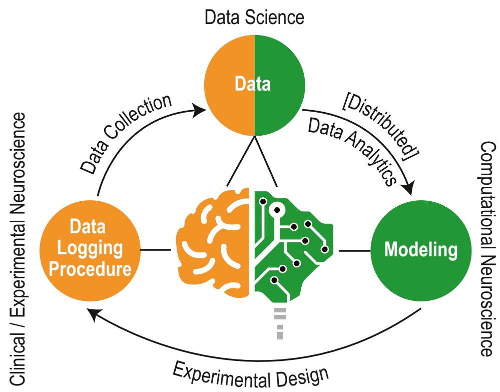

Fig. 1 Cycle of modern Neuroscience research

advancements in artificial intelligence [14] and cloud computing [15] allow scientists to perform these steps smoothly. In particular, 'cloudification' has significantly aided scientists by providing 'software as a service' (e.g., service oriented architecture or SOA) instead of running data-intensive analytics and modeling locally in the computers. In other words, cloud computing and big data paradigms have converted context-aware research into exhaustive, data-driven research.

More recently, with the emergence of the Internet of Things (IoT), various sensors can be connected to the cloud for seamless resource sharing. Such IoT-Cyber Physical Systems (IoT-CPS) can provide a platform for data-driven research and design of appropriate medical services for patients. The IoT-CPS tailored to patient monitoring and care have been around for a few years now and have enabled hospitals and healthcare processionals to seamlessly exchange patients' data even from remote locations. These data may represent a wide range of healthcare parameters collected through the IoT for healthcare (IoHT) sensors. One of the main challenges of this type of IoT-CPS is to ensure privacy and information security. Thus, trust management plays a vital role for end users, acting as a first step of information security. Despite the fact that trust management is required for all frameworks dealing with biological data acquirable through IoHT devices, neuroscience data stands apart from others and requires special attention due to its high variability and spontaneity. While in many biosignals (e.g., Electrocardiogram, Electromyogram) periodicities and similarities have been noticed in terms of frequency content, amplitude and shape, neuroscience datasets (e.g., EEG, ECoG, LFPs, AP) have been known for variabilities [16–18] making them more prone to misidentification, misclassification and misinterpretation, particularly in cases when signals are acquired without any experts. Therefore, to design robust IoT-CPS based telemedicine systems for neuroscience applications, extra care must be taken to ensure the trustworthiness of IoHT nodes.

Mahmud et al. introduced a service-oriented architecture for web based collaborative biomedical signal analysis [19]. As an initial platform with three main components (i.e., users, contributors, and services), this model assumed inherent security of the internet and exploited certificate based security as an authentication scheme for contributors and users, to both deploy and utilize services. The same architecture can be extended by delegating incoming data from IoT devices to the cloud for analysis. Additionally, a cloud-based healthcare system was proposed in [20] to provide convenient patient-centric healthcare services. In this model, the cloud performed big data analytics and authors reported significant performance improvements in the cloud-based system, which can also be adapted for smart healthcare applications. Further, biologically inspired cloud resource provisioning was proposed for optimal handling of big healthcare data [21].

While the assumption of a secure cloud is appropriate in the context of currently discussed communication models, discarding malicious transmission—identified by the nodes' profile information, behavior, and data similarity—is vital to ensure the optimized performance, reliability, and robustness of a system. In the current scenario, profile information is validated by authentication services, and the nodes behavior and data similarity are handled by a trust management system. To make a more trustworthy system, Shabut et al. identified malicious nodes based on their behavior and improved packets delivery through a multi-hop relay network excluding any misbehaving nodes [22]. Another work proposed a dynamic cluster based recommendation model to minimize data sparsity or cold start situations using nodes behavior, to improve quality of service (QoS) of end-to-end (E2E) transmission [23]. Chen et al. proposed a Fuzzy reputation-based trust model (TRM) for IoT-CPS which estimated the nodes trust from their behavior and showed an improved performance in comparison to a communication system without trust [24]. An ant colony-based trust model was presented to determine the trust value of wireless nodes which exhibited improved accuracy [25]. Context-aware multiservice trust management systems were proposed in [26, 27] which filtered malicious nodes in the E2E and heterogeneous IoT architectures with high accuracy. Another trust management model (TMM) was proposed to evaluate the trustworthiness of nodes in a wireless sensor network through beta distribution. The aggregated trust value from data and energy was used to identify untrustworthy relay nodes to reduce internal threats [28]. Yet another trust management system, based on an agent's trustworthiness and confidence, was proposed to evaluate the trustworthiness of IoT nodes [29]. Moreover, a joint social and QoS TMM was presented to find the trust level of wireless nodes in a mobile adhoc network [30].

However, identifying malicious transmission using only nodes behavior is not sufficient to ensure reliable communication. It is important to guarantee that data generated by the nodes is error-free—which is a big challenge—and a TMM that takes into account both nodes behavior and data similarity, can offer a solution to confirm nodes reliability.

This paper presents an Adaptive Neuro-Fuzzy based Brain-inspired TMM targeting a cloud-based IoT architecture. This aims to determine data trust and behavioral trust for all IoT devices and relay nodes, to ensure reliable data communication between E2E devices. Further, we investigate the effects of trust management on QoS issues of the cloud based IoT architecture, suitable for neuroscience applications.

Cloud Based IoT Architecture

The big data and cloud are two paramount elements for creating collaborative frameworks to analyze brain signals (e.g., EEG, ECoG, AP, LFPs) and brain images (e.g., MEG, MRI, fMRI, PET), and to perform data-driven modeling [19]. Due to the wide range of advantages offered by such architectures, they have become increasingly popular in recent years [31].

Focusing on applications related to Neuroscience, Fig. 2 illustrates a cloud-based IoT framework which comprises three main components: the IoT end (composed of data generating devices), the cloud component (providing access and connectivity, and processing and analysis of data), and the user end (providing analyzed and processed data to users, e.g., doctors, caregivers, and researchers). In this framework, the data from various Neurotechnology empowered devices is collected for the development of state-of-the-art techniques pertaining to intelligent healthcare and advancement of Neuroscience research. At the IoT end, also known as perception layer, various data generating devices are connected to respective transceiver devices to forward data to the cloud through the IoT gateway, whether for data analytics or simply for storage. Additionally, brain signals generated at the IoT end are also used for operating various medical and assistive devices (e.g., automatic wheelchair, robotic arm) [31, 32] to provide better monitoring and improved quality of life. The cloud is used for defining the access and the network, and perform data storage and analytics. Extending the work of Mahmud et al. [19], in our framework, we consider the cloud to be secure through existing certification and authentication models (see Fig. 3). Finally, at the user end, service consumers can access and visualize the processed data based on granted rights and privileges.

In cloud-based IoT architectures, the IoT devices or nodes generate data owing to various Neuroscience applications. Like human relationships, these nodes collaborate with each other through certain predefined social properties, specifically the 'Trust Compositions' (see Section 7). The values of these social properties are propagated on the IoT and user ends (known as 'Trust Propagation'). During direct or indirect interactions, the

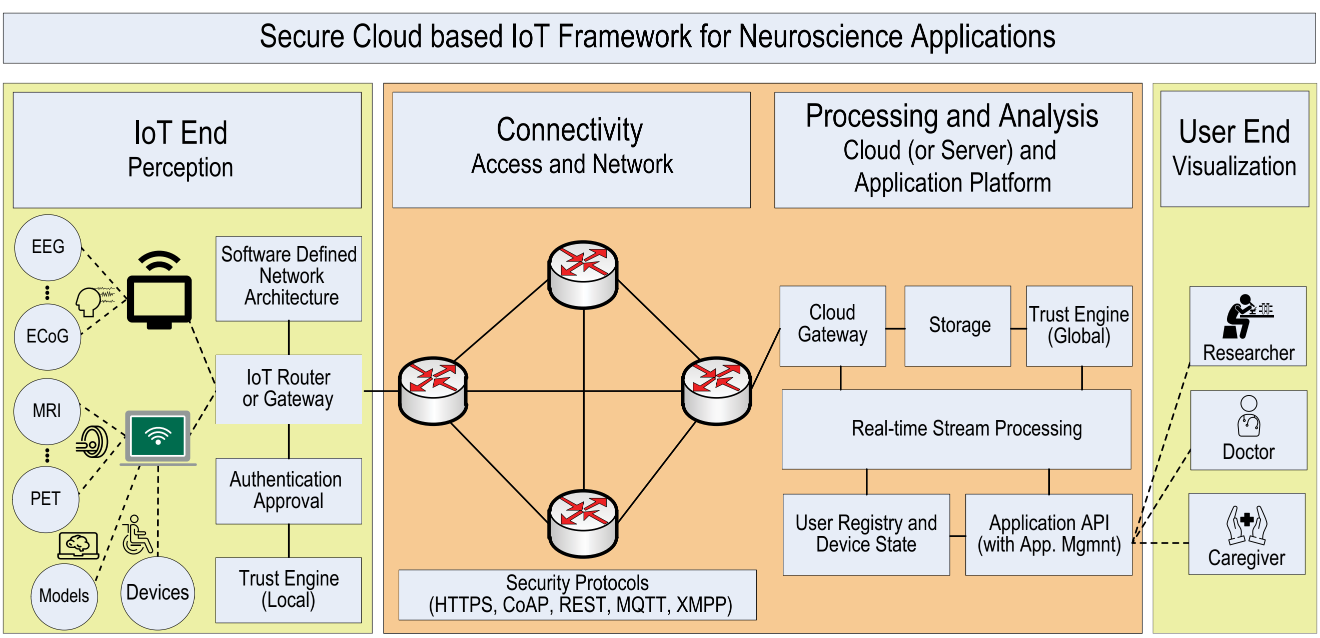

Fig. 2 Cloud based IoT Architecture for Neuroscience Applications. All the IoT sensor nodes are deployed in the perception layer (IoT site)

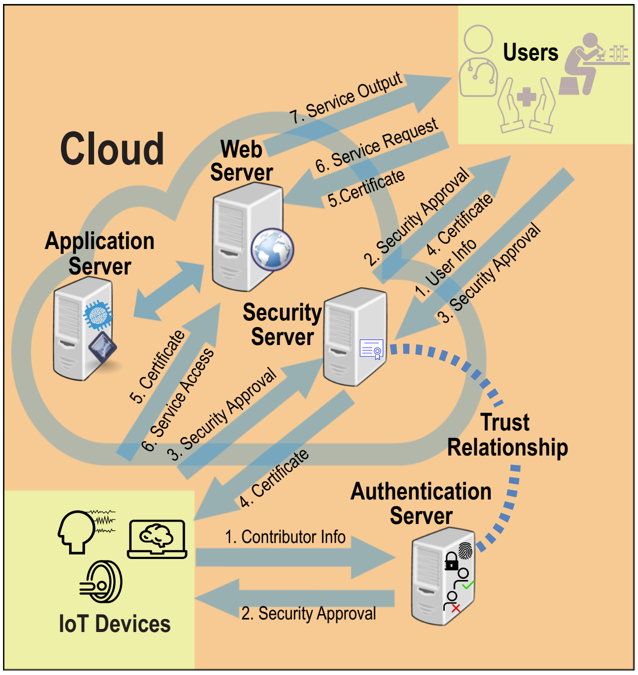

Fig. 3 Cloud authentication model (adapted from [19])

trust metrics of each node are aggregated through static weighted sum, neuro-fuzzy method, and Bayesian inference (known as 'Trust Aggregation'). The trust value of each node is then updated when an interaction is completed (known as 'Trust Update'). This update can also be carried out periodically for energy efficiency. The block diagram of the trust management steps is illustrated in Fig. 4.

Trust Management Model

The proposed TMM is illustrated in Fig. 5, where IoT nodes directly or via local/global relay nodes (such as smartphones, routers, etc.) interact with sensor hubs (see Fig. 2) to establish successful communication links. The individual trust levels of the IoT devices and relay nodes require evaluation in order to discard the malicious nodes [33].

As data communication in the access and cloud layer is secured, IoT and user ends become the main focus of our TMM, for ensuring E2E trust among IoT devices and users for cloud-based Neuroscience applications. IoT devices and relay nodes are assumed to have social relationships among themselves. Thus, the interactions and collaborations among

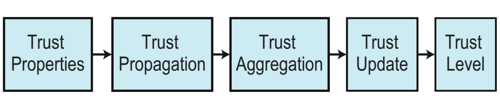

Fig. 4 Block diagram showing various steps of a trust evaluation process

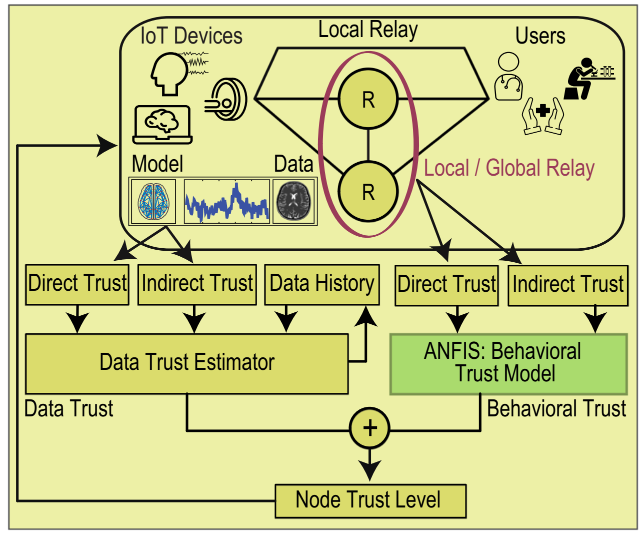

Fig. 5 The trust management model. Data trust and behavioral trust values are aggregated to find the trust level of the sensor and relay nodes.

these nodes are employed to evaluate the trust level of each node. In deducing E2E trust level, certain relationship among nodes are considered which include– node profile information, node behavioral trust, and data trust [34].

Node profile information is assured by the authentication service, whereas behavioral and data trust are estimated using adaptive neuro-fuzzy inference system (ANFIS) and weighted-additive method, respectively. The node behavioral evidence is assessed through direct and indirect interactions among the nodes. For each node, the assessment of behavioral trust is carried out whilst considering three factors related to that node– RFI, intimacy, and honesty. The data trust is assessed by estimating the deviation of a node's instantaneous data from the historical data of that node. Both direct and indirect methods can be employed to evaluate data trust of a node.

Mathematically, the trust level of a given node (j) denoted by $\mathcal{T}_j$ is estimated by summing up behavioral and data trust as Eq. 1.

$$\mathcal{T}_j(t) = \mathcal{T}_j^{nb}(t) + \mathcal{T}_j^{d}(t), \quad (1)$$

where, $\mathcal{T}_j^{nb}(t)$ is the evaluated behavioral trust and $\mathcal{T}_j^{d}(t)$ is the evaluated data trust.

Evaluation of Behavioral Trust

Behavioral Trust Metrics

The trust properties for the behavioral trust of a node are discussed below.

Relative Frequency of Interaction (RFI) Zhang et al. studied the interaction frequency among nodes [35]. Interaction frequency refers to the number of interactions, between assessor and assessee, that take place within a given unit of observation time. The higher the successful interaction rate, the higher the degree of closeness. This indicates the assessee node is a trustworthy node. It has also been reported that the closeness in a relationship (e.g., friendship) can be predicted from past interactions and confounds future interactions [36, 37]. Therefore, the RFI-aware trust, $\mathcal{T}_j^{RFI}$, can be calculated by Eq. 2.

$$\mathcal{T}_j^{RFI} = \frac{n_j}{N}, \tag{2}$$

where, n_j is the number of interactions between the assessee node j and the assessor node in an observation period t, whereas, N is the total number of interactions between node j with other k nodes during t.

Intimacy In any social context, the intimacy or relationship duration of interaction is an important factor in calculating trust level. The higher the time of interaction between an assessee node and an assessor or guarantor node, the higher the intimacy. Considering the total time spend of an assessor node i with the assessee node j as t_{ij} and the cumulative time spend of j with other k guarantor nodes as t_{kj}, the intimacy ($\mathcal{T}_j^I$) can be calculated by Eq. 3 [38].

$$\mathcal{T}_j^I = \frac{t_{ij}}{t_{ij} - t_{kj}}. \tag{3}$$

Honesty Honesty is one of the main factors for establishing social trust between two given nodes. It can be determined using the successful and unsuccessful interactions of those nodes. Usually, the value of honesty lies between [0,1], i.e., $\mathcal{T}_j^H \in [0, 1]$. In other words, $\mathcal{T}_j^H = 0$ means no successful interaction, and $\mathcal{T}_j^H(t) \to 1$ means the assessee node j is a trustworthy node. While a_j and b_j denote successful and unsuccessful interactions, respectively, their values are estimated using the Beta distribution [39, 40], where the distribution $f(p|a_j, b_j)$ is expressed by the Gamma function $\Gamma(\cdot)$ with $0 \le p \le 1$, $a_j > 0$, $b_j > 0$; and $p \ne 0$ if $a_j < 1$ and $p \ne 1$ if $b_j < 1$ [41]. Finally, the honesty aware trust value can be calculated by Eq. 4.

$$\mathcal{T}_j^H(t) = \frac{a_j}{a_j + b_j}. \tag{4}$$

Node Behavioral Trust

The node behavioral trust is calculated from both direct and indirect interactions between nodes. At a given time t, an assessor node directly interacts with the assessed node and evaluates the direct trust level (i.e., $\mathcal{T}_j^{d,nb}(t)$) from previous direct interactions. Based on the guarantee provided by the adjacent nodes the indirect trust level (i.e., $\mathcal{T}_{kj}^{ind,nb}(t)$) can be evaluated. The guarantor nodes (k number of nodes) provide a guarantee based on the previous interactions with the assessed node. The behavioral trust of j-th node is given by Eq. 5.

$$\mathcal{T}_j^{nb}(t) = \mathcal{T}_j^{d,nb}(t) + \sum_k \frac{1}{\mathcal{H}_k} \mathcal{T}_{kj}^{ind,nb}(t), \tag{5}$$

where, $\mathcal{H}_k$ is the hop count for the k-th guarantor node.

ANFIS Based Node Behavioral Trust Model

Fuzzy inference system (FIS) is a rule-based expert system which can mimic the Brain's logical inference to represent a system. In ANFIS, a fuzzy inference system is employed to represent a nonlinear system with any complexity. The parameters of the input and output membership functions can be tuned by the backpropagation or hybrid backpropagation-least squares algorithm [42, 43]. Due to its adaptive nature, ANFIS is more powerful in comparison to FIS.

The node behavior is evaluated by the ANFIS model as illustrated in Fig. 6. The system consists of three inputs – RFI, intimacy, and honesty. Each input has three linguistic terms or membership functions (MFs), i.e., *Low*, *Medium*, and *High*. Therefore, there are nineteen possible IF-THEN

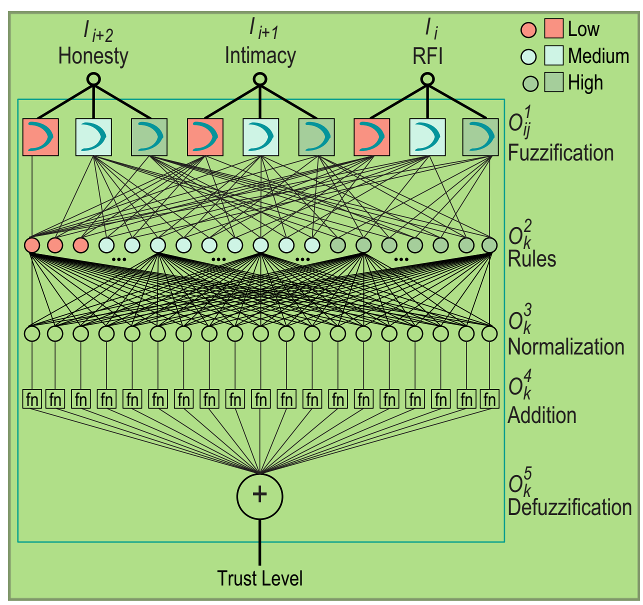

Fig. 6 ANFIS for the node behavioral trust calculation. The model evaluates node behavioral trust based on the RFI, intimacy, and honesty. The 'fn' denotes the y_k function in the form $y_k = \sum_i w_{ki} I_i + b_k$

rules in the rule based system (see Fig. 6) and one output called node behavioral trust level.

There are five layers– Fuzzification, Rule, Normalization, Defuzzification and Output. Detailed description of each of these layer is described in [32, 42, 43]. The outputs of the layers are expressed by:

$$
\begin{aligned}
\text{Fuzzification:}\quad O_{ij}^{1} &= \mu_{ij}(I_i),\\
\text{Rule:}\quad O_{k}^{2} &= \prod O_{ij}^{1} = \prod \mu_{ij}(I_i),\\
\text{Normalization:}\quad O_{k}^{3} &= \frac{O_k^2}{\sum_k O_k^2},\\
\text{Defuzzification:}\quad O_{k}^{4} &= O_k^3 y_k,\ \ y_k = \sum_i w_{ki} I_i + b_k,\\
\text{Output:}\quad O_{k}^{5} &= \mathcal{T}_j^{nb}(t) = \sum_k O_k^4,
\end{aligned}
$$

where, $i = 1, 2, 3$; $j = 1, 2, 3$; $k = 1, 2, ..., 19$; μ_{ij} is j-th MF for input I_i, w_{ki} and b_k are consequent parameters; and $\mathcal{T}_j^{nb}(t)$ is given by Eq. 5.

The ANFIS model is trained with the input-output datasets generated from the NS2 simulator [44]. This dataset is generated for the placement of 50 nodes where a percentage of the nodes are configured as misbehaving nodes. Beta distribution calculated the failure and success of the interactions. For the predefined rule-based, the ANFIS model has changed the MFs, and premise/ consequent parameters for finding the node-behavior trust value. Figure 7 shows the output surface plots of ANFIS model where node behavioral trust is plotted against the trust properties (a) honesty and RFI, and (b) honesty and intimacy.

Evaluation of Data Trust

The data trust of a node consists of direct and indirect trust based on the historical data of the node(s).

Direct Data Trust. The value of direct data trust depends on the deviation of a node's instantaneous data from its historical data. The historical data are the average value of the node's data for a specific period. Mathematically, the direct data trust, $\mathcal{T}_j^{dd}(t)$, of the j-th node with the i-th relay can be expressed by Eq. 6.

$$
\mathcal{T}_j^{dd}(t) = \begin{cases} \mathcal{T}_{max} & \text{for } D_j^{dd}(t) = D^{his} \\ \frac{1}{|D_j^{dd}(t) - D^{his}|} & \text{for } D_j^{dd}(t) \neq D^{his}, \end{cases} \tag{6}
$$

where, D_j^{dd} is the instantaneous data of j-th node during direct interaction whereas D^{his} is the historical data.

Indirect Data Trust The indirect data trust, $\mathcal{T}_j^{di}$ is the average value of the deviation of a node's instantaneous data from the historical data of k nodes with j-th relay under the assumption that the included nodes are all trusted. Mathematically, $\mathcal{T}_j^{di}(t)$ can be expressed by the Eq. 7.

$$
\mathcal{T}_j^{di}(t) = \begin{cases} \mathcal{T}_{max} & \text{for } \frac{\sum_k D_{kj}^{ind}(t)}{k} = D^{his} \\ \frac{1}{|\frac{\sum_k D_{kj}^{ind}(t)}{k} - D_j^{his}|} & \text{for } \frac{\sum_k D_{kj}^{ind}(t)}{k} \neq D_j^{his}, \end{cases} \tag{7}
$$

where, D_{kj}^{ind} is the instantaneous data of j-th node during indirect interaction with k nodes.

Having obtained the direct and indirect trust values, data trust of the j-th node is calculated by Eq. 8.

$$
\mathcal{T}_j^{d}(t) = \mathcal{T}_j^{dd}(t) + \sum_k \frac{1}{\mathcal{H}_k} \mathcal{T}_j^{di}(t - t_m), \tag{8}
$$

where, t_m is the previous interaction time at the m-th slot.

Performance Metrics

The proposed brain-inspired TMM, suitable for cloud based IoT frameworks targeting Neuroscience applications, has been evaluated using Packet Forwarding Ratio (PFR) [45]; Network Throughput (NetT) [46–49]; Average Energy Consumption Ratio (AECR) [29]; Accuracy [32]; and F-measure [50].

PFR The PFR is the ratio between a number of packets received by the IoT CPS and the number of packets transmitted by the source node. The PFR decreases when the forwarded packets are dropped due to reasons like– buffer

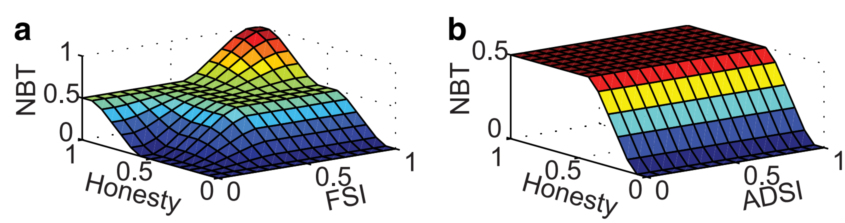

Fig. 7 The output surface plots of ANFIS where node behavioral trust is plotted against the trust properties **a** honesty and RFI and **b** honesty and intimacy

overflow, blocking, route failure. Mathematically, the E2E PFR is calculated by Eq. 9.

$$\text{PFR} = \frac{\sum_k PKT_{rec}}{\sum_n PKT_{send}}, \tag{9}$$

where PKT_{rec} and PKT_{send} are the number of packets received by the destination node and packets send by the source node. The source node sends n number of packets and destination node receives k number of packets, and $k < n$.

NetT The NetT can be defined as the rate at which the source transmissions are delivered successfully to the destination over the link(s) between the source-destination pair. The value of the throughput declines with the appearance of misbehaving nodes in the network. Mathematically, the NetT is calculated by Eq. 10.

$$\text{NetT} = \frac{N_{success}}{t_{trans}}, \tag{10}$$

where $N_{success}$ is the number of successful transmission delivered to the destination and t_{trans} is the considered transmission interval.

AECR The AECR is an another performance metric which is the ratio between the energy consumption for evaluating a trust metric (E_{te}) and the energy consumption for the data transmission (for sending (E_{send}) and for receiving (E_{rec})) of a node. The AECR of a malicious node is lower than that of a legitimate node as a malicious node does not participate in the packet forwarding or route discovery. Mathematically, AECR is calculated by Eq. 11.

$$\text{AECR} = \frac{\sum_n E_{te}}{\sum_n (E_{rec} + E_{send})}. \tag{11}$$

Accuracy Accuracy is the ratio between the numbers of total successful interactions and total interactions. Mathematically, accuracy A is expressed by Eq. 12 [51].

$$A = \frac{TP + TN}{TP + FP + TN + FN}, \tag{12}$$

where TP is the number of successful interactions categorized as successful, TN is the number of successful interactions categorized as unsuccessful, FP is the number of unsuccessful interactions categorized as successful, and FN is the number of unsuccessful interactions categorized as unsuccessful.

F-measure The Precision ($=TP/(TP + FP)$) as well as recall ($=TP/(TP + TN)$) are two important measures considered in evaluating a classification outcome [50]. It is calculated by the harmonic mean of both recall and precision, and mathematically it is expressed by Eq. 13.

$$\text{F-measure} = \frac{2}{1/recall + 1/precision}. \tag{13}$$

Table 1 Parameters and settings used in simulation

Parameters	Numerical value
Simulator	NS-2
Routing	AODV
Node distribution	Random
Traffic	CBR
Nodes	50
MAC	802.11
Speed	3 m/s
Packet size	512 bytes
Range	250 m
Max. connection	12
Reply delay	60 ms

Results

To verify the efficacy of the proposed TMM, simulation was performed in the NS-2 platform [44]. The parameters and setting employed in this platform are listed in Table 1. The results were obtained by running the simulation twenty times and then taking the average values of these runs. It was assumed that the nodes had wireless capabilities and were communicating either directly or through multihop relay nodes to the IoT-CPS. The Adhoc On-demand Distance Vector (AODV) routing protocol [52] was employed to simulate the communication scenario. The IoT devices or relay nodes were categorized two types– legitimate node

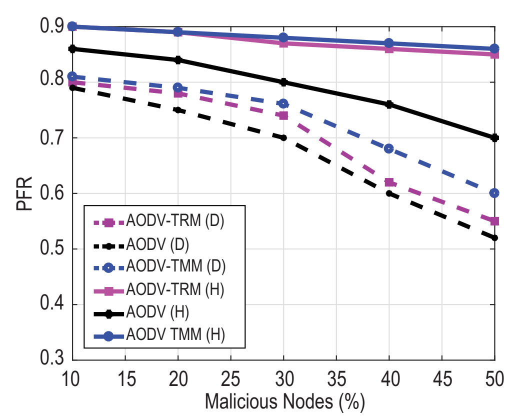

Fig. 8 The effect of malicious nodes on PFR

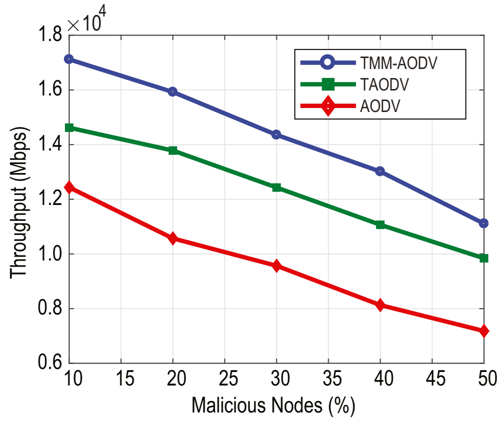

Fig. 9 The effect of malicious nodes on overall network performance

and malicious node. The legitimate nodes took part in the route discovery and packet forwarding process, whereas the malicious nodes in neither took part in packet forwarding nor in route discovery.

The ANFIS-based TMM was incorporated in the IoT-CPS network and all nodes were initialized with random trust values. Following a certain number of interactions the node behavior trust, and direct and indirect data trust were evaluated by the model.

The PFR dropped significantly when the malicious nodes arose in the IoT or user end. A node was termed malicious if it hid (H) in the route discovery phase or dropped (D) packets intentionally. Figure 8 depicts the effect of malicious nodes on the PFR. The PFR decreased as the percentage of malicious nodes increased from 10% to 50%. In both cases of malicious behavior, the proposed TMM outperformed TRM [24]. In addition, in terms of PFR, both TMM and TRM achieved better performance compared to AODV with no trust management framework (indicated as 'AODV').

The malicious nodes changed the overall network throughput as illustrated in Fig. 9. When the number of malicious nodes were increased (10 to 50%) and the remaining nodes showed legitimate behavior, the throughput of the network decreased. The performance drop was due to the fact that the appearance of the malicious nodes dropped packet forwarding in the network. The performance of the proposed TMM (AODV-TMM in Fig. 9) was compared with the trusted AODV (TAODV in Fig. 9) and AODV without trust (AODV in Fig. 9). The results showed that the proposed TMM outperforms the TAODV and AODV.

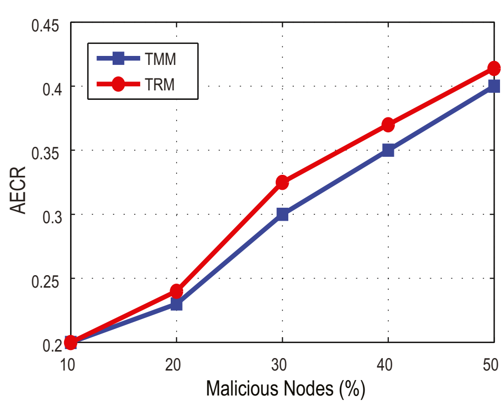

Fig. 10 The effect of malicious nodes on AECR

Table 2 Performance comparison of three types of Trust management techniques

Technique	Accuracy	f-measure
ANFIS (case 1)	0.967	0.97
ANFIS (case 2)	0.957	0.96
FIS	0.89	0.90

Additionally, the proposed TMM is more energy efficient (see Fig. 10). In comparison to the TRM, with the increasing number of malicious nodes (10 to 50%) present in the communication network, the proposed TMM consumes less energy during the data transmission process. The reduced AECR value, compared to the TRM, indicates that the proposed TMM is capable of identifying more malicious nodes in the communication network.

Table 2 shows that the proposed TMM has higher accuracy (0.967 in case 1, when 5 linguistic terms were used: *Very Low*, *Low*, *Medium*, *High*, and *Very High*; and 0.957 in case 2, when 3 linguistic terms were used: *Low*, *Medium*, and *High*) in comparison to a FIS which has an accuracy of 0.89. In addition, the F-measure of the proposed TMM (case 1: 0.97 and case 2: 0.96) also obtained higher values than FIS (0.90).

Conclusion and Future Work

With the unprecedented growth of Brain data and IoT, cloud based data analytics solutions are gaining popularity, with security now a major concern. This paper has proposed a Brain-inspired TMM to secure data transmission and ensure data reliability for a cloud-based IoT architecture, targeting Neuroscience applications. The TMM evaluates both node behavioral trust and data trust using an ANFIS based node behavioral model and a weighted-additive method, respectively. Based on evaluated trust levels, the model constructs a list of trustworthy nodes. The performance of the proposed TMM was evaluated using PFR, throughput, AECR and accuracy. Simulation results show that the proposed TMM outperforms existing FIS based trust management algorithms. In the future, more sophisticated optimization techniques along with Bayesian statistics, Deep Learning, and Reinforcement Learning based TMM will be exploited. These will further ensure the security, reliability and accuracy of rapidly growing cloud-based IoT and Block Chain architectures.

Acknowledgments The work was supported by ACS Lab (http://www.acslab.info). The authors would like to acknowledge members of the ACS Lab for proof-reading the manuscript. Amir Hussain was supported by the UK Engineering and Physical Sciences Research Council (EPSRC) through grant numbers EP/I009310/1 and EP/M026981/1.

Author Contributions This work was carried out in close collaboration between all co-authors. MM, MSK, MMR, MAR, and SAM first defined the research theme and contributed an early design of the system. MSK and AS further implemented and refined the system development. MM and MSK first drafted the paper and all authors edited the draft. All authors have contributed to, seen, and approved the final manuscript.

Compliance with Ethical Standards

Conflict of Interest The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Ethical Approval This article does not contain any studies with human participants or animals performed by any of the authors.

Informed Consent As this article does not contain any studies with human participants or animals performed by any of the authors, the informed consent in not applicable.

References

1. Mahmud M, Kaiser MS, Hussain A, Vassanelli S. Applications of deep learning and reinforcement learning to Biological Data. IEEE Trans Neural Netw Learn Syst. 2018. https://doi.org/10.1109/TNNLS.2018.2790388 [Epub ahead of print].
2. Schadt EE, Linderman MD, Sorenson J, Lee L, Nolan GP. Computational solutions to large-scale data management and analysis. Nat Rev Genet. 2010;11(9):647–657.
3. Shahand S, Benabdelkader A, Jaghoori MM, Mourabit Ma, Huguet J, Caan MWA, et al. A data-centric neuroscience gateway: design, implementation, and experiences. Concurr Computat: Pract Exper. 2015;27(2):489–506.
4. Landhuis E. Neuroscience: Big brain, big data. Nature. 2017;541:559–561.
5. Sakkalis V. Applied strategies towards EEG/MEG biomarker identification in clinical and cognitive research. Biomark Med. 2011;5(1):93–105.
6. McMillan CT. Neurodegenerative disease: MRI biomarkers — a precision medicine tool in neurology? Nat Rev Neurol. 2016;12(6):323–324.
7. Liu S, Cai W, Liu S, Zhang F, Fulham M, Feng D, et al. Multimodal neuroimaging computing: a review of the applications in neuropsychiatric disorders. Brain Inf. 2015;2(3):167–180.
8. Al-jawahiri R, Milne E. Resources available for autism research in the big data era: a systematic review. Peer J. 2017;5:e2880.
9. Young AL, Oxtoby NP, Schott JM, Alexander DC. Data-driven models of neurodegenerative disease. Adv Clin Neurosci Rehabil. 2014;14(5):6–9.
10. Burns R, Vogelstein J, Szalay A. From cosmos to connectomes: the evolution of data-intensive science. Neuron. 2014;83(6):1249–1252.
11. Mahmud M, Pulizzi R, Vasilaki E, Giugliano M. QSpike tools: a generic framework for parallel batch preprocessing of extracellular neuronal signals recorded by substrate microelectrode arrays. Front Neuroinform. 2014;8:26. https://doi.org/10.3389/fninf.2014.00026.
12. Mahmud M, Vassanelli S. Processing and analysis of multichannel extracellular neuronal signals: State-of-the-art and challenges. Front Neurosci. 2016;10:248. https://doi.org/10.3389/fnins.2016.00248.
13. Neuro Cloud Consortium. To the cloud! a grassroots proposal to accelerate brain science discovery. Neuron. 2016;92(3):622–627.
14. Luo B, Hussain A, Mahmud M, Tang J. Advances in brain-inspired cognitive systems. Cogn Comput. 2016;8(5):795–796.
15. Hashem IAT, Yaqoob I, Anuar NB, Mokhtar S, Gani A, Ullah Khan S. The rise of “big data” on cloud computing: Review and open research issues. Inf Syst. 2015;47:98–115.
16. Mahmud M, Travalin D, Bertoldo A, Girardi S, Maschietto M, Vassanelli S. An automated classification method for single sweep local field potentials recorded from rat barrel cortex under mechanical whisker stimulation. J Med Biol Eng. 2012;32(6):397–404.
17. Mahmud M, Bertoldo A, Girardi S, Maschietto M, Vassanelli S. SigMate: A Matlab-based automated tool for extracellular neuronal signal processing and analysis. J Neurosci Methods. 2012;207(1):97–112.
18. Mahmud M, Cecchetto C, Vassanelli S. An automated method for characterization of evoked single-trial local field potentials recorded from rat barrel cortex under mechanical whisker stimulation. Cogn Comput. 2016;8(5):935–945.
19. Mahmud M, Rahman MM, Travalin D, Raif P, Hussain A. Service oriented architecture based web application model for collaborative biomedical signal analysis. Biomed Eng-Biomed Tech. 2012;57(Sl-1):780–783. https://doi.org/10.1515/bmt-2012-4412.
20. Zhang Y, Qiu M, Tsai CW, Hassan MM, Alamri A. Health-CPS: Healthcare cyber-physical system assisted by cloud and big data. IEEE Syst J. 2017;11(1):88–95.
21. Ullah A, Li J, Hussain A, Yang E. Towards a biologically inspired soft switching approach for cloud resource provisioning. Cogn Comput. 2016;8(5):992–1005.
22. Shabut AM, Dahal KP, Bista SK, Awan IU. Recommendation based trust model with an effective defence scheme for MANETs. IEEE Trans Mob Comput. 2015;14(10):2101–2115.
23. Shabut AM, Dahal K. Social factors for data sparsity problem of trust models in MANETs. In: Proceedings of the ICNC; 2017. p. 876–880.
24. Chen D, Chang G, Sun D, Li J, Jia J, Wang X. TRM-IoT: A trust management model based on fuzzy reputation for internet of things. Comput Sci Inf Syst. 2011;8:1207–1228.
25. Marzi H, Li M. An enhanced bio-inspired trust and reputation model for wireless sensor network. Procedia Comput Sci. 2013;19:1159–1166.
26. Ben Saied Y, Olivereau A, Zeghlache D, Laurent M. Trust management system design for the Internet of Things: A context-aware and multi-service approach. Comput Secur. 2013;39(Part B):351–365.
27. Dolera Tormo G, Gomez Marmol F, Martinez Perez G. Dynamic and flexible selection of a reputation mechanism for heterogeneous environments. Future Gener Comput Syst. 2015;49:113–124.
28. Fang W, Zhang C, Shi Z, Zhao Q, Shan L. BTRES: Beta-based Trust and Reputation Evaluation System for wireless sensor networks. J Netw Comput Appl. 2016;59:88–94.

29. Ruan Y, Durresi A, Alfantoukh L. Trust management framework for internet of things. In: Proceedings of the AINA; 2016. p. 1013–1019.
30. Chen IR, Guo J, Bao F, Cho JH. Integrated social and quality of service trust management of mobile groups in ad hoc networks. In: Proceedings of the ICICS; 2013. p. 1–5.
31. Zhang Y, Qiu M, Tsai CW, Hassan MM, Alamri A. Health-CPS: Healthcare cyber-physical system assisted by cloud and big data. IEEE Syst J. 2017;11(1):88–95.
32. Kaiser MS, Chowdhury ZI, Mamun SA, Hussain A, Mahmud M. A neuro-fuzzy control system based on feature extraction of surface electromyogram signal for solar-powered wheelchair. Cogn Comput. 2016;8(5):946–954.
33. Yan Z, Zhang P, Vasilakos AV. A survey on trust management for Internet of Things. J Netw Comput Appl. 2014;42:120–134.
34. Afsana F, Jahan N, Sunny FA, Kaiser MS, Mamun SA. Trust and energy aware Cluster modeling and spectrum handoff for cognitive radio ad-hoc network. In: Proceedings of the ICEEICT; 2015. p. 1–6.
35. Zhang ZX. The effects of frequency of social interaction and relationship closeness on reward allocation. J Psychol. 2001;135(2):154–164.
36. Jøsang A, Ismail R, Boyd C. A survey of trust and reputation systems for online service provision. Decis Support Syst. 2007;43(2):618–644.
37. Cherry B. Entrepreneur as trust-builder: interaction frequency and relationship duration as moderators of the factors of perceived trustworthiness. Int J Bus Glob. 2014;14(1):97–121.
38. Daly EM, Haahr M. Social network analysis for information flow in disconnected delay-tolerant MANETs. IEEE Trans Mob Comput. 2009;8(5):606–621.
39. Momani M, Takruri M, Al-Hmouz R. Risk assessment algorithm in wireless sensor networks using beta distribution. CoRR 2014. arXiv:1410.3041.
40. Liu Y, Chitawa US, Guo G, Wang X, Tan Z, Wang S. A Reputation Model for Aggregating Ratings Based on Beta Distribution Function. In: Proceedings of the ICCSE; 2017. p. 77–81.
41. Josang A, Ismail R. The beta reputation system. In: Proceedings of the BLED; 2002. p. 324–337.
42. Takagi T, Sugeno M. Fuzzy identification of systems and its applications to modeling and control. IEEE Trans Syst Man, Cybern. 1985;SMC-15(1):116–132.
43. Al-Hmouz A, Shen J, Al-Hmouz R, Yan J. Modeling and Simulation of an Adaptive Neuro-Fuzzy Inference System (ANFIS) for Mobile Learning. IEEE Trans Learn Technol. 2012;5(3):226–237.
44. Issariyakul T, Hossain E. Introduction to network simulator, Vol 2. Boston: Springer; 2009.
45. Gopinath S, Nagarajan N. Energy based reliable multicast routing protocol for packet forwarding in MANET. J Appl Res Technol. 2015;13(3):374–381.
46. Kaur R, Sharma N. Dynamic node recovery for improved throughput in MANET. In: Proceedings of the NGCT; 2015. p. 325–330.
47. Gupta NK, Pandey K. Trust based Ad-hoc on Demand Routing protocol for MANET. In: Proceedings of the IC3; 2013. p. 225–231.
48. Talreja R, Sathish S, Nenwani K. Trust Variable Factor : A trust based method to detect misbehaving nodes in MANET. In: Proceedings of the ICEEOT; 2016. p. 3238–3241.
49. Dhananjayan G, Subbiah J. T2AR: trust-aware ad-hoc routing protocol for MANET. Springer Plus. 2016;5(1):995.
50. Ghosh S, Biswas S, Sarkar D, Sarkar PP. A novel Neuro-fuzzy classification technique for data mining. Egypt Inform J. 2014;15(3):129–147.
51. Gu Q, Zhu L, Cai Z. In: Computational Intelligence and Intelligent Systems. Evaluation measures of the classification performance of imbalanced data sets. Berlin: Springer; 2009. p. 461–471.
52. Andel TR, Yasinsac A. Adaptive threat modeling for secure Ad Hoc routing protocols. Electron Notes Theor Comput Sci. 2008;197(2):3–14.