


Article

IoT-Inspired Framework of Intruder Detection for Smart Home Security Systems

Tariq Ahamed Ahanger , Usman Tariq , Atef Ibrahim , Imdad Ullah  and Yassine Bouteraa

College of Computer Engineering and Sciences, Prince Sattam Bin Abdulaziz University, Al-Kharj 11942, Saudi Arabia; u.tariq@psau.edu.sa (U.T.); aa.mohamed@psau.edu.sa (A.I.); i.ullah@psau.edu.sa (I.U.); y.bouteraa@psau.edu.sa (Y.B.)

* Correspondence: t.ahanger@psau.edu.sa

Received: 1 August 2020; Accepted: 18 August 2020; Published: 21 August 2020



Abstract: The proliferation of IoT devices has led to the development of smart appliances, gadgets, and instruments to realize a significant vision of a smart home. Conspicuously, this paper presents an intelligent framework of a foot-mat-based intruder-monitoring and detection system for a home-based security system. The presented approach incorporates fog computing technology for analysis of foot pressure, size, and movement in real time to detect personnel identity. The task of prediction is realized by the predictive learning-based Adaptive Neuro-Fuzzy Inference System (ANFIS) through which the proposed model can estimate the possibility of an intruder. In addition to this, the presented approach is designed to generate a warning and emergency alert signals for real-time indications. The presented framework is validated in a smart home scenario database, obtained from an online repository comprising 49,695 datasets. Enhanced performance was registered for the proposed framework in comparison to different state-of-the-art prediction models. In particular, the presented model outperformed other models by obtaining efficient values of temporal delay, statistical performance, reliability, and stability.

Keywords: smart foot mat; Internet of Things (IoT); Adaptive Neuro-Fuzzy Inference System (ANFIS)

1. Introduction

Internet of Things (IoT) technology has been a major driver for the technological progress of Information and Communication Technology (ICT)[1,2]. Developments of small, internet-enabled, and wireless sensors have not only revolutionized the ubiquitous data perception methodology, but it has inserted a vision of smartness in the ambient environment everywhere [3,4]. According to the Statista survey, the global IoT market is expected to pass 1.6 trillion US Dollars by 2025 (Source: <https://www.statista.com>). This includes an estimation of 34.2 billion connected IoT devices around the world (Source: <https://iot-analytics.com>). Advancements of the IoT paradigm has realized numerous innovations that were nearly impossible in previous decades due to under-developed technology [5]. Some of these include Smart Homes [6], Mobile Healthcare [7], Intelligent Transportation [8], Smart Food Hubs [9], and Smart Agriculture [10]. Additionally, IoT technology contributes significantly to provisioning security in the form of wireless cameras, motion sensors, and smart locking mechanisms [11]. However, continuous research is still going on in the development of smart security systems for homes and buildings by incorporating the novel vision of IoT technology and Fog Computing [12]. Fog computing, as coined by [13], is a virtual platform for provisioning real-time computation, the capacity to store, and services at the network between the users and data storage, which are present over the network [14]. The collaboration of IoT-Fog technology can analyze IoT data for security-based decision-making in time-sensitive manner [15].

1.1. Research Field

Smart Homes and Intelligent Buildings are characterized by ubiquitous services and effective decision-making with enhanced accuracy. Designing smart security solutions has always been a challenging aspect for researchers around the world. Security in the form of biological-locks, automated doors, and smart alarms has been deployed to wireless protection for homes, buildings, and parking. However, recent studies have shown vulnerabilities in these security solutions. A survey report presented by Protect America depicts 75% of the smart devices are vulnerable to the security breach (Source: <https://www.protectamerica.com/>). Moreover, there are 32 risks identified by the Jacobsson et al. [16] out of 25% were classified as highly vulnerable. Therefore, need-of-the-hour is to minimize current smart security risks which are derived from human factors either directly or indirectly. This demands novel security solutions that can be easily implanted in the smart home scenario as extra protection. With an advanced model of smart security, both privacy and safety can be enforced to further assess the capability of IoT-inspired secure frameworks.

1.2. Research Motivation

The IoT-Fog-Cloud hybrid solution offers an appropriate mechanism to store, manage, and interpret all-encompassing information in a time-sensitive manner. IoT sensors, including wireless networks, preceptors, and RFIDs can transmit pervasive information to remote devices [17]. The development of sensing technologies can also generate stochastic data with minimal delay [18]. For optimum performance, sophisticated artificial intelligence technologies such as machine/deep learning are incorporated for accomplishing the notion of the smart mat-based framework [19]. The core part of the presented system is to map and analyze the various identity-oriented parameters in real time. Additionally, the comprehensive literature review has identified multiple research gaps;

1. Detection of real-time identity-based parameters of intruder personnel has not been addressed specifically by the researchers. it is essential to develop user-centered decision-making strategies.
2. Minimal research has been presented for regularized monitoring of home security and related attributes by the monitoring officials, thereby compromising the home security.
3. Another factor that has been minimally explored in state-of-the-art research is the incorporation of ANFIS-PSO for interactive intruder detection decision-making.
4. Finally, limited work has been done to quantify the identity parameters for effective decision-making by security officials and users.

1.3. State-of-the-Art Research Objectives

This section provides major contributions presented by the proposed home security framework. In the current research, several compact, internet-equipped IoT sensors are embedded in the smart mat, which consistently gathers data regarding the user's identity parameters for preventing intrusion. When IoT embedded mat is stepped on by the user, the identity of the user is monitored based on certain parameters. Moreover, users get alerted by activation of pleasant chime or loud alarm as per acquaintance or intruders' presence, respectively. Significantly, identity-related information is generated which includes parameters like weight, foot size, pressure, movement, which is further analyzed for person identification via the fog computing node. Figure 1 displays the conceptual illustration of the proposed framework. Specifically, the presented framework is aimed at realizing the following objectives to realize the overall secure mat-based system.

1. Monitors identity-based attributes by using IoT devices equipped in the smart mat in real time for the identification of intruders.
2. Classifies identity-based attributes in 2 classes, Authentic Class and Non-Authentic Class using the Bayesian Belief Model (BBM) which is quantified in probabilistic feature of Probability of Authenticity (PoA).

3. Enabling data analysis in time-sensitive manner, using the Temporal Granulation Process for collecting and processing information. It is further quantified into the Authentic Index (AI) for the prediction of identity-related information over the Fog-Cloud computing framework.
4. Predicts the probability of authenticity based on temporal aspects of AI value by using the Adaptive neuro-fuzzy inference system (ANFIS) mechanism.
5. State-of-the-art validation of the presented framework performance in comparison to decision-modeling techniques.

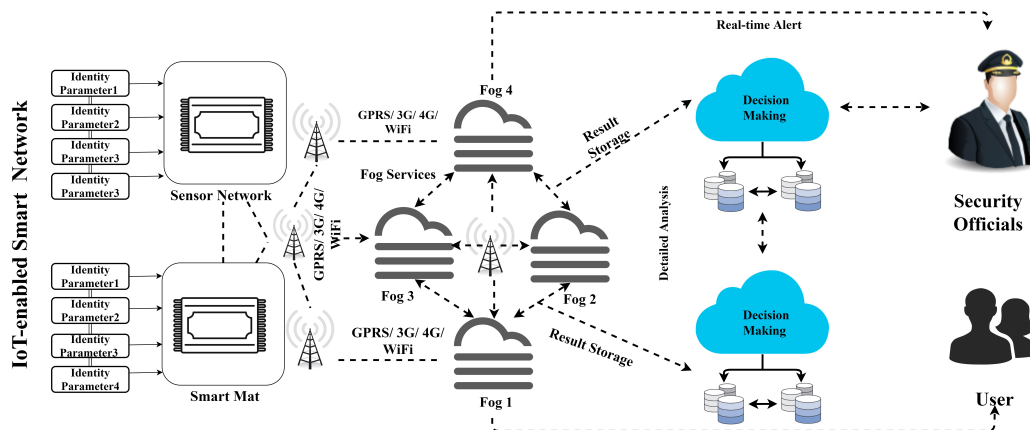


Figure 1. Conceptual Framework of Intruder Detection and Monitoring System.

Paper Organization: Remainder of the article is structured as; Section 2 reviews some of the vital literature works in smart home-based security frameworks. Section 3 discusses the detailed architecture of the presented framework. Section 4 presents the simulation for validation purposes. Section 5 concludes the article with significant research pathways.

2. Literature Review

Researchers around the world have presented numerous architectures confining to the home security and surveillance system. Matthies et al. (2019) [20] introduced CapMat system comprising of a smart foot mat that supports user identification and multi-phase authentication for applications. However, the proposed system was unable to feature any form of foot-based interactivity. Huang et al. (2020) [21] developed the IoT Inspector tool for users to monitor traffic on home networks from intelligent home devices. The authors addressed that such data permit new research into intelligent homes via 2 safety and privacy case studies. Minoli et al. (2020) [22] examined several existing automation smart home IoT-based architectures to provide a reliable assessment of the provided environment and further evaluates the pertinence of blockchain mechanisms. The authors addressed the complexities associated with the deployment of blockchain security in smart home frameworks. Mallikarjuna et al. (2020) [23] proposed Feedback-based resource management (FBRM) system for efficiently managing the resources and IoT devices. Moreover, it is evaluated using the iFogSim toolkit and validated in conjunction with existing approaches and has been analyzed in terms of QoS metrics. Desai et al. (2020) [24] addressed numerous issues for IoT-automation system using android mobile applications and NodeMCUs. The key emphasis of the study is data gathering and transmission by the sensor nodes to mobile devices for user-oriented operations. Popa et al. (2019) [25] proposed a modular cloud-based platform for gathering, aggregating, and storing all the data collected from the smart environment. The presented architecture enhanced the interoperability between the environmental sensors and actuators and also allowed the models to be modified in real time, depending on the raw data obtained. Ranjan et al. (2013) [26] presented “RF Doormat”, a device that tracks the crossing of doors in people’s rooms in a multi-person household. The presented system was effectively used in commercial buildings with the widespread use of RFID embedded ID cards. Cheng et al. (2016) [27] performed a variety of studies to analyze the intelligent surface,

exploring several possibilities for operation detection both as a cover for furnishings and as a floor in daily life. The measurement is based on specific contact with a textile surface. It can detect activities through movement propagation of body parts, and actions. Sokullu et al. (2020) [28] introduced a revolutionary IoT-based framework for safety and early alerts generation for supporting elderly and individuals with a short-term memory loss (MCI patients, dementia patients, etc.). Data is gathered from environmental sensors to identify their behaviors. The patient's conduct at home was tracked and data was maintained for relatives and/or caregivers. Suciu et al. (2015) [29] evaluated different components and methodologies for the efficient integration of cloud-based IoT-enabled big data systems. The presented study also provided a secure e-health architectural design to monitor and efficiently analyze health data. Sun et al. (2012) [30] developed a pre-alarm device focused on tailing dam control computing systems based on IoT and Internet. The system intended to maximize the protection of the dam by controlling flooded channels, water levels, and dam deformation in real time. The device has been implemented extensively in various barrages and effective outcomes have been obtained. Based on the extensive state-of-the-art review, a comparative analysis has been depicted in Table 1 with the presented model.

Table 1. State-of-the-Art Comparative Analysis Studies (A Available, NA Not Available).

Related Work	Fog	IoT	Temporal Analysis	Classification	Cognitive Decision	User-Centered	Time-Sensitive	Precision	Numerical	Stability	Reliability	Security Protocols
Ranjan et al. (2013) [26]	NA	A	NA	A	NA	NA	NA	NA	NA	NA	NA	NA
Sowjanya et al. (2016) [31]	NA	A	NA	NA	NA	NA	NA	NA	NA	NA	NA	A
Sun et al. (2012) [30]	NA	A	NA	A	NA	NA	NA	NA	NA	NA	NA	A
Cheng et al. (2016) [27]	NA	A	NA	NA	NA	NA	A	A	NA	A	A	A
Sokullu et al. (2020) [28]	NA	A	A	A	NA	NA	A	A	NA	NA	A	A
Suciu et al. (2015) [29]	NA	A	NA	A	NA	NA	NA	A	NA	A	NA	A
Matthies et al. (2019) [20]	NA	A	NA	NA	NA	NA	NA	A	NA	NA	A	A
Chiang et al. (2016) [15]	A	A	A	A	NA	NA	NA	NA	NA	NA	NA	NA
Proposed Technique	A	A	A	A	A	A	A	A	A	A	A	A

In Table 1, A indicate Available, NA indicate Not Available.

3. Proposed Methodology

Figure 2 shows the proposed IoT-based framework for assessing identity-based parameters in the pervasive environment of homes and personal apartments. The presented technique consists of 4 phases including Data Perception Phase (DPP), Data Analysis Phase (DAP), Data Extraction Phase (DEP), and Intelligent Prediction Phase (IPP). Initially, data is collected in a time-sensitive manner using several IoT sensors that are embedded on the smart foot mat. For real-time intruder detection and decision-making, the collected data is transferred on to the associated fog computing device. Furthermore, extensive data is transmitted to the connected cloud computing platform for cognitive decision analysis by security officials. The detailed functionally performed by each phase is depicted ahead.

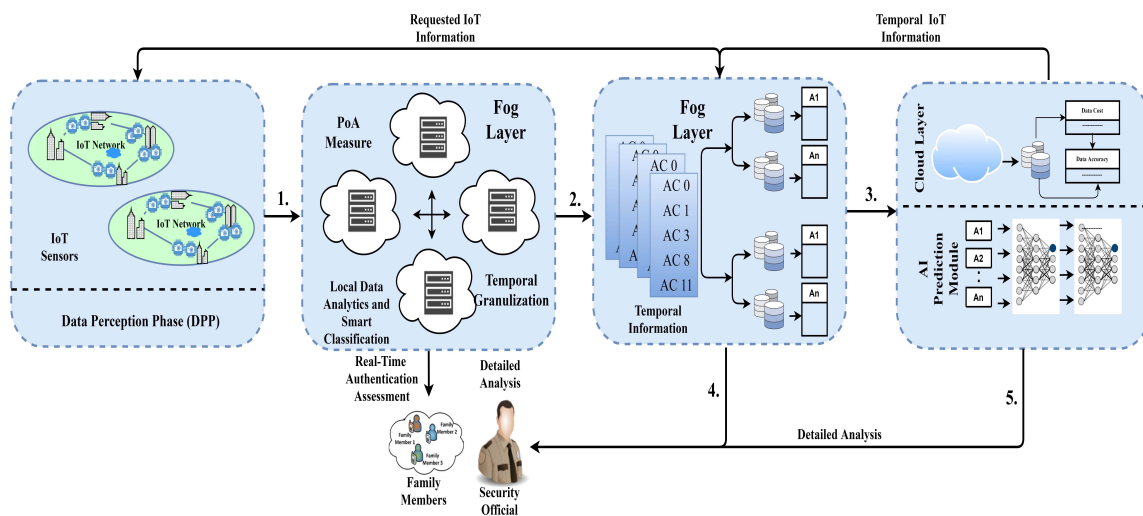


Figure 2. Modular Framework for Smart Intruder Detection.

3.1. Data Perception Phase (DPP)

DPP is the initial phase of the proposed approach for retrieving the real-time data values from the sensors mounted on the smart mat. The key tasks performed by this phase are the interpretation and sensation of data values concerning user identification, weight, foot size, pressure, foot width, and movement. The quantitative findings are communicated to the Raspberry Pi (fog computing device) for further analysis after the data is acquired. As an addendum to sensation, the DPP phase provides security throughout the network and storage procedure. The security of the IoT network relies on the usage of specific protocols for the transfer of data from system-to-system and system-to-server [32]. All data from and to IoT system can be secured using various cryptography protocols namely Transport phase Security (TLS) Protocol, Secure Sockets phase (SSL), and Elliptic Curve Cryptography ECC [33,34]. These protocols ensure secure communications for the network protocols including the HTTP (Hypertext Transfer Protocol) and MQTT (Message Queuing Telemetry Transport) Protocol [35]. Also, IoT computing involves data server nodes on a distant site [36]. Advance privacy policies like bio-metric authenticity monitoring, client authentication, and AES (Advance Encryption Storage) allow secure IoT data storage [37].

3.2. Data Analysis Phase (Dap)

Identity-based attributes are obtained in time-sensitive manner from the smart mat. Such parameters are evaluated for real-time decision-modeling using a fog computing paradigm. Fog computing devices are compact and low-storage hardware devices that allow computational tasks to be carried out in time-sensitive manner based on the data instances [38]. Moreover, fog computing

enables data processing, storage, and networking between IoT and cloud storage [39]. Various fog computing systems distributed on a commercial basis namely Arduino Gemma, Raspberry Pi, and Intel Edison [40]. The main task of the DAP phase is to efficiently analyze the data over the fog computing system based on identity-specific pre-defined values. Conspicuously, the BBM (Bayesian Belief Model) is used for categorization based on a prevalence measure termed as Probability of Authenticity (PoA).

Definition 1. *Probability of Authenticity (PoA): It is a probabilistic measure to establish the existence of intruder at a specific time-slot Δt . In specific, PoA calculates the presence of intruders stepped onto mat through rigorous quantification.*

The aforementioned definition provides a numerical measure to evaluate an intruder, stepped onto the smart mat. In other words, PoA assesses the interdependent parameters for intruder detection in time-sensitive manner. PoA is used to form 2 categories of data instances namely Authentic Class and Non-Authentic Class. This classification ensures that the intruders are adequately examined.

1. *Authentic Class:*

This data set comprises of those parameter measures which indicate non-intruder or authentic personnel. These parametric values are represented safe as well as compliance values with the security measures. Moreover, data perturbation including increased weight and abnormal shoe-based parameters can be detected using Expectation-Maximization [41] technique.

2. *Non-Authentic Class:*

This class is intended to acquire parameter values that are vulnerable and indicates the presence of unauthentic personnel. On the basis of data classification, the Non-Authentic Class has a detrimental effect for home security and thus it is indispensable to assess such measures for providing prevention against intrusion.

3.2.1. Classification Based on BBM

BBM Model is used for the classification of datasets into different classes [42]. As described earlier, 2 classes are mentioned based on different identity-based parameters. For mathematical analysis, let an instance of data is represented by a vector $A_i = (a_1, a_2, \dots, a_n)$ where A_i represents the i th identity-based attributes, with the assuming that all the identity-based parameters are not bi-related. The conditional probability of intruder detection A_i of class L_j is denoted by $P(\frac{L_j}{a_1, a_2, \dots, a_n})$. Since large input attributes are possible and a certain identity-based parameter may have a variable measure, then the presented formulation result in inconsistency. Henceforth, the modified BBM is formulated as $P(\frac{L_j}{A_i}) = \frac{P(L_j)P(A_i/L_j)}{P(A_i)}$.

On the other hand, the probability of $P(L_j)P(A_i/L_j)$ can be significantly enhanced on the basis of combined probability function as

$$\begin{aligned} P(L_j)P(A_i/L_j) &= P(a_1, a_2, \dots, a_n, L_j) \\ &= P(a_1/a_2, \dots, a_n, L_j)P(a_2, \dots, a_n, L_j) \\ &= P(a_1/a_2, \dots, a_n, L_j)P(a_2/a_3, \dots, a_n, L_j)P(a_3, \dots, a_n, L_j) \\ &= P(a_1/a_2, \dots, a_n, L_j)P(a_2/a_3, \dots, a_n, L_j), \dots, P(a_{n-1}/a_n, \dots, a_n, L_j) \times P(a_n/L_j)P(L_j) \end{aligned}$$

In addition, it is supposed that each feature a_i of identity parameter is not completely reliant upon any other measure a_j i.e., $i \neq j$. Then $P(a_i/a_{i+1}, \dots, a_n, L_j) = P(a_i/L_j)$.

Therefore, the joint probability is described as follows:

$$\begin{aligned} P(L_j) &= \prod_{i=1}^n P(L_j)P(a_i/L_j) \\ P(\frac{L_j}{a}) &= \prod_{i=1}^n P(L_j)P(a_i/L_j)/P(a) \end{aligned}$$

In the equation described above L_j depicts the Authentic Class and Non-Authentic Class of parameters.

3.3. Data Extraction Phase (Dep)

DEP is an essential phase in which valuable database samples can be abstracted. Data values for identity-based data values can be extracted over the timeframe to provide accurate quantitative analysis. Temporary Granulation Process (TGP) is a method used for data mining. TGP is extracted using the temporal abstraction approach illustrated in [2]. TGP consists of 2 main phases, TGP Abstraction and TGP Aggregation. Both phases are addressed ahead.

Definition 2. *TGP Abstraction ($r_i, \Delta t$): Given a data value r_i for an identity-based attribute and time-slot of Δt , TGP Abstraction is represented for time event (t_i) and data value r_i such that for $t_i \rightarrow \Delta t$, $PoA(r_i) > \zeta$ (pre-defined measure) and is represented as $[r_i, t_i]$.*

Definition 2 comprises of ζ depicts the related threshold of the i th identity-based attribute. The main goal of TGP Abstraction (r_i, t_i) is to associate every attribute of a user U with the certain time interval. In other terms, t_i depicts the measure of time at which the data r_i is registered for the user U . Accordingly, each data measure attained for user U is sequentially related to its corresponding time interval through the usage of TGP Accumulation.

Definition 3. *TGP Aggregation (r_1, t_1), (r_2, t_2), ..., (r_n, t_n): Considering TGP Abstraction with sequential data samples for Δt time frame, then TGP Aggregation contributes to the fusion of data instances with heterogeneous identity-based attributes that have adverse attribute measures in the time-instant frame Δt .*

Definition 4. *Authentic Index (AI): Given a user U and associated TGP for identity-based attributes in time-slot of Δt , then AI is a probabilistic measure for quantifiable detection of intruders on the basis of identity attribute measure reported in Δt time.*

Definition 4 provides a consistent quantitative assessment of identity-based measures of the User U for a given time frame. Figure 3 shows a brief formulation of the TGP mechanism for the AI approximation. In Table 2, several steps have been presented to evaluate AI in a certain time window Δt .

Table 2. Identity AI Analysis Procedure

AI Analysis Procedure
1: Input IoT measures for n identity-based attributes and relevant PoA measures. $\zeta, \alpha, \beta, \phi$ are the associated weights.
2: Set $AI_{\Delta t} = \text{Null}(0)$.
3: Assess PoA measure of identity-based attribute 1 with pre-defined threshold measure.
4: If $PoA_1 > \kappa_1$, Then Sum $\zeta \times PoA_1$ to AI.
5: Assess PoA measure of identity-based attribute 2 with pre-defined threshold measure.
6: If $PoA_2 > \kappa_2$, Then Sum $\alpha \times PoA_2$ to AI
Repeat for all attribute
7: Evaluate PoA measure of n th identity-based attribute with prefixed threshold measure.
8: If $PoA_n > \kappa_n$, Then Sum $\alpha \times PoA_n$ to AI
9: Cumulative $AI = \zeta \times PoA_1 + \alpha \times PoA_2 + \beta \times PoA_3 + \dots \phi \times PoA_n$

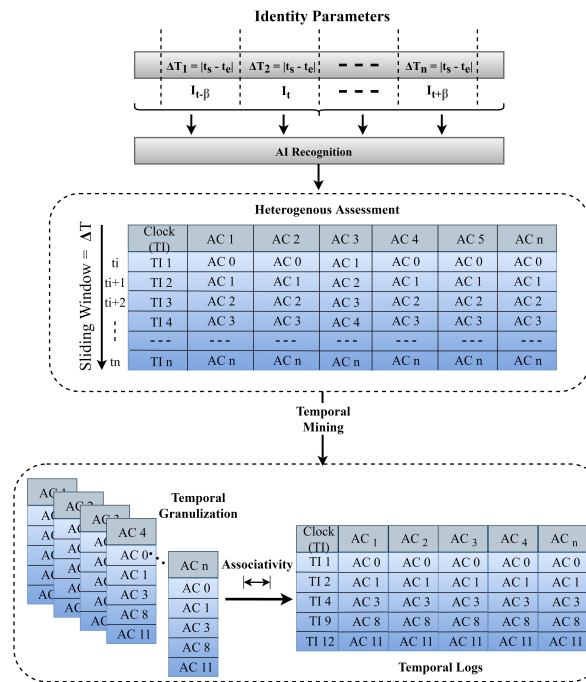


Figure 3. Granulation Procedure.

3.4. Intelligent Prediction Phase (IPP)

IPP is the final phase of the presented framework for provision prediction-based decision-making using Adaptive Neuro-Fuzzy Inference System (ANFIS) technique. ANFIS model is used by several researchers in several disciplines for analytical decision-making process [43]. ANFIS is used to solve highly complex and non-linear problems [44]. Figure 4 illustrates the five-phased ANFIS architecture with inputs. The Fuzzy Logic provides a multi-value input logic from one parental input vector describing one value set in reference to a set of other variables [45]. In the proposed framework, a fuzzy inference model for the input of non-linear map vectors is used. Each identity-based parameter is evaluated within a space-time window in the current study using the proposed ANFIS model. For instance, data values are provided to ANFIS for which its predictability value can be determined to prevent intrusion of home security over a specified time-space window. The detailed mathematical evaluation of ANFIS phases is discussed ahead.

(a) Fuzzification (Phase 1): The first phase of the ANFIS system is fuzzy unit, which uses Membership Functions (MFs) to convert inputs into a fuzzy set. Every node in this phase is responsive and shown as follows:

$$Q_j^1 = \gamma k_j(z) \quad (1)$$

where the gaussian membership function is represented as Q_j^1 , z is supposed as the input is fed to the node j , and K_j is supposed as the descriptive attribute linked with a node function [46]. In the present context, spatio-time data measures for several identity-based attributes in the initial fuzzification phase are actually provided.

(b) Product rule (Phase 2): The neurons in the first phase transmit the input data to the next phase by performing the element-based product formation and are mathematically represented as follows:

$$Q_j^2 = \gamma X_j(z) \times \gamma E_j(s), \quad j = 1, 2 \quad (2)$$

where $X_j(z)$ and $E_j(s)$ represent the nodes in phase 2.

(c) Normalization (Phase 3): Every neurons of this phase calculates the proportion of the single firing strength rule to the amount of each firing strength rule as shown in Equation (3). The firing strength of y'_j is indicated and simplified as follows:

$$Q_j^3 = y'_j = \frac{y_j}{y_1 + y_2}, j = 1, 2 \quad (3)$$

(d) De-fuzzification (Phase 4): This phase is accountable for evaluating the contribution of the j th rule to the final output. The following standardized consequent variables are identified as the f_j , a_j , and u_j attributes. The de-fuzzification mechanism in this phase is as follows:

$$Q_j^4 = y'_j d_j = y'_j (f_j z + a_j s + u_j) \text{ for } j = 1, 2 \quad (4)$$

(e) Output generation (Phase 5): The output phase is considered to measure the sum of all outputs from all nodes, and to measure the ultimate value Q_j^5 as represented in Equation (5):

$$Q_j^5 = \sum y'_j d_j = \frac{\sum_j y_j d_j}{\sum_j y_j} \quad (5)$$

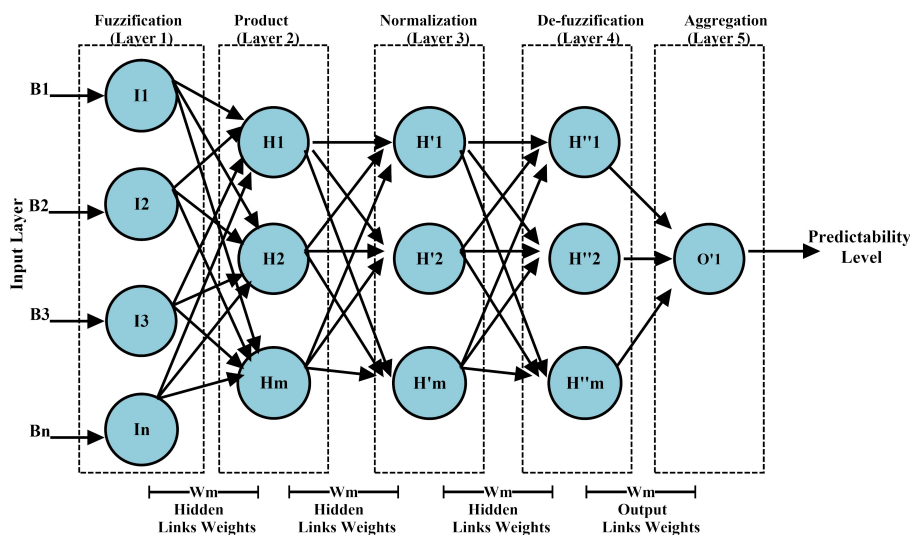


Figure 4. Adaptive Neuro-Fuzzy Inference System (ANFIS) Structure.

In a wide variety of applications for the development of prediction models, the ANFIS showed encouraging performance. However, the model optimization process can significantly improve modeling quality and accuracy. A wide range of methodologies, including Particle Swarm Optimization (PSO), for optimizing the parameters and outputs of the ANFIS system are available. In comparison to other approaches with the ultimate goal of optimization, the PSO process is exceptional. The PSO method was inspired by the bird's behavior. This study incorporates the beneficial aspects of the algorithm. The PSO technique was influenced by birds in need for food. The particles in this model change their locations and trajectories according to their knowledge and input from others. Therefore, it was suggested that the particle has a cognitive function. The method of optimization is focused on competitiveness and particle cooperation. If PSO is used to address modeling problems, the paths and speeds of particle states may be observed. Three vectors Y_j , E_j , and $Abest_j$ describe the characteristics of a particle where Y_j is the specific location, E_j is the current speed, and $Abest_j$ is the best spatial positioning of the particle in pursuit, and $zbest_j$ is the optimal

solution for the whole community of particles. The direction and trajectory of a particle are slowly modified based on the following formula:

$$e(l+1) = e(l) + d_1 \text{random}(0,1) \times [abest(l) - present(l)] + d_2 \text{random}(0,1) \times [zbest(l) - present(l)] \quad (6)$$

$$present(l+1) = present(l) + e(l+1) \quad (7)$$

where $e(\cdot)$ is the particle speed in the l^{th} and $(l+1)^{\text{th}}$ repetition, $present(\cdot)$ is the particle position, d_1 and d_2 are the learning constants which are higher than zero, and a random integer between $[0, 1]$ is referred with $\text{random}(\cdot)$. Equation (7) represents the process for upgrading the particle size including the historic velocities and global best positions of a particular particle.

4. Experimental Implementation

The proposed model for identity-based estimations comprises of 3 important measures. Initially, the data values related to the user identity-based parameters such as weight, foot size, pressure, and movement are measured by specific sensors equipped within the IoT-mat. For in-depth analysis, the collected data from these devices is transmitted for temporal evaluation to the fog computing node. Therefore, findings will be recorded and displayed to the homeowner through the handheld device in real time. Henceforth, the proposed framework has been evaluated from 5 major viewpoints.

1. Identification of the temporal delay time in the generation of identity-based findings by different computational phases.
2. Estimate the categorization efficacy for the presented BBM model of data classification.
3. Quantitative identity-based prediction estimation for intruder detection.
4. Analyze the prediction model's reliability across increased number of data segments.
5. Determine the system stability to identify the presented model's effectiveness.

4.1. Simulation Environment

The model was simulated over a challenging dataset acquired from the Online repository of UCI with 49,695 data instances. Identity-based parameters namely weight, foot scale, movement, pressure were obtained. The presented frameworks enable the homeowner to check the information of an unauthenticated person. Different data instances with heterogeneous physical measurements were identified and assessed for system reliability. Moreover, attributes of age, height, weight, and other physical features vary considerably. It allows the presented system to be more widely used in practice. The iFogSim simulator is used for computational analysis of fog-related data processing. iFogSim details are available in [47].

4.2. Temporal Delay Determination

Executing Delay is considered to be the computing time of the presented ANFIS-based adaptive predictive-modeling. In other terms, it is depicted as the total time needed to generate ANFIS-based decisions. Let $T_{\text{ANFIS Generation}}$ signifies the time for ANFIS formulation and $T_{\text{Predictive-Modeling}}$ signifies the time at which the decision is made. Therefore, $\text{Temporal Delay} = T_{\text{ANFIS Formulation}} + T_{\text{Predictive-Modeling}}$. For a temporal delay evaluation of the proposed system, the findings are contrasted with existing models, including K-Nearest Neighbors (KNN), Artificial Neural Network (ANN), and Support Vector Machine (SVM). Results were obtained after close analysis of different data sets. The temporal delay for the datasets is shown in Figure 5. On average, the time required to detect intruders by using a smart mat with IoT sensors was about 22.55 s as compared to 32.26 s by ANN, 36.66 s by SVM, and 38.11 by KNN respectively. Conspicuously, the proposed model is more effective in temporal delay as compared to state-of-the-art prediction models.

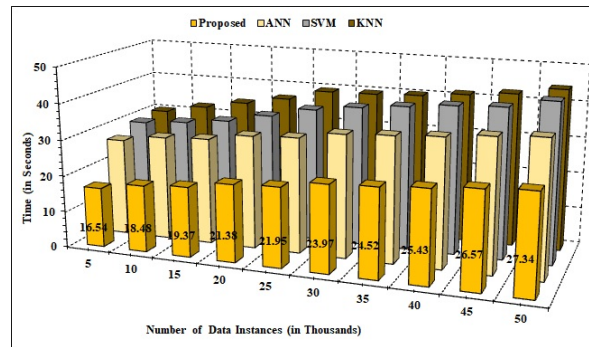


Figure 5. Cumulative Temporal Delay.

4.3. Classification Efficiency

Classification efficiency evaluates 3 performance estimators, namely Precision(Prec), Specificity(Spec), and Sensitivity(Sens) for the proposed model. As the baseline classifier, 2 state-of-the-art classification techniques were incorporated. These involve the Decision Tree (DT) and Support Vector Machine (SVM). It is important to note that during implementation only the classification methodology is modified, whereas the rest of the model stays unchanged. Also, as seen in Table 3, the average of such results is recorded for different datasets. For numerical simulation, the Waikato Environment for Knowledge Analysis (WEKA) is used (Source: <https://www.cs.waikato.ac.nz/>). WEKA is an open-source performance assessment toolkit usable commercially.

1. The proposed model can be noted to report a mean precision measure of 93.09% for the data sets collected. Compared to this, DT achieved an accuracy of 91.68% and 91.37% was recorded by SVM. Henceforth, the proposed BBM model is more efficient than other classification methods.
2. The presented approach can record a higher value of 92.03% as compared with DT (90.10%) and SVM (90.54%) for specificity analysis. It shows that the proposed model is better.
3. Another aspect for performance assessment of the proposed model is sensitivity analysis. In the current scenario, it can be seen that the presented model has a high value of 92.19% relative to 91.29% for DT and 91.28% for SVM. Henceforth, based on data classification, the proposed model is more effective and reliable.

Table 3. Categorization Efficacy; (Prec Precision, Spec Specificity, Sens Sensitivity).

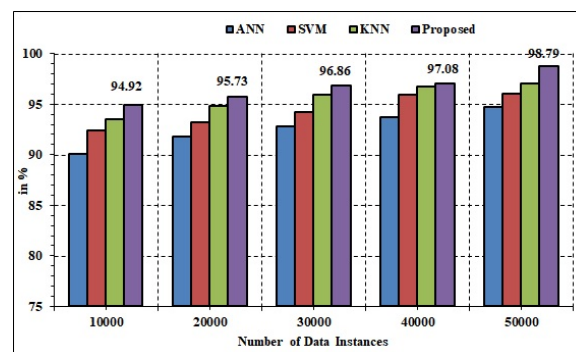
Model	BBM Classifier			DT Classifier			SVM Classifier		
Dataset	Prec	Spec	Sens	Prec	Spec	Sens	Prec	Spec	Sens
5000	94.45%	92.04%	93.82%	92.82%	89.02%	90.67%	92.42%	89.14%	90.11%
10,000	92.78%	91.94%	92.32%	91.52%	91.22%	91.72%	91.02%	91.69%	91.04%
15,000	93.57%	91.98%	92.52%	91.42%	90.33%	92.34%	90.06%	90.43%	92.08%
20,000	93.73%	90.84%	91.32%	92.52%	89.14%	90.49%	92.32%	90.63%	90.59%
25,000	91.56%	92.44%	92.54%	91.22%	90.22%	92.09%	91.64%	91.26%	92.39%
30,000	92.32%	90.32%	91.32%	92.21%	91.14%	91.07%	92.76%	91.02%	91.83%
35,000	93.82%	89.93%	91.31%	91.26%	89.82%	90.24%	91.14%	90.79%	89.16%
40,000	92.32%	90.54%	92.62%	92.12%	89.45%	91.15%	92.06%	89.89%	91.34%
45,000	91.85%	89.35%	92.42%	90.44%	90.10%	92.04%	89.18%	90.42%	92.14%
50,000	92.42%	91.01%	91.72%	91.32%	90.59%	91.10%	91.18%	90.14%	91.60%

4.4. Prediction Efficiency

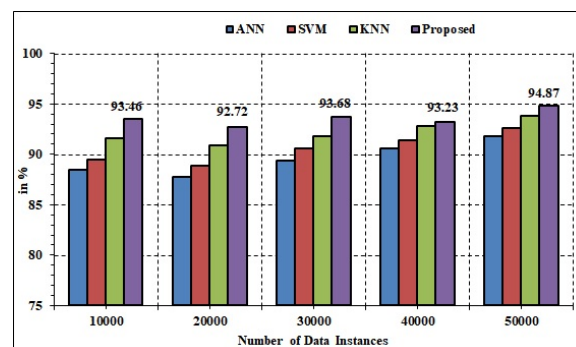
Prediction efficiency relates to the probability of intruder detection after the evaluation of specific parameters. The comparative study has been carried out with state-of-the-art decision-taking models namely Artificial Neural Network (ANN), Support Vector Machine (SVM), and K-Nearest Neighbor (KNN) for quantification of the performance improvements. The findings have been calculated. It is

important to note that only decision-making techniques have been modified and the remaining model is unaltered. Performance measurement is evaluated in terms of Accuracy, Sensitivity, Coefficient of Determination, and F-Measure. Detailed results are depicted ahead.

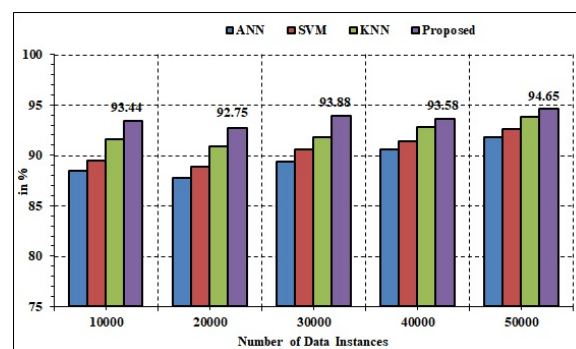
1. The proposed model has recorded a higher value of 93.66% as compared with ANN (89.57%), SVM (90.55%), and KNN (92.19%) for accuracy analysis. Figure 6a shows that the model proposed is much better.
2. The presented model has registered higher value of 93.59% as compared with ANN (87.53%), SVM (88.56%), and KNN (89.29%) for sensitivity analysis as shown in Figure 6b.
3. The proposed model has attained a higher value of 93.68% as compared with ANN (85.57%), SVM (89.45%), and KNN (91.32%) for F-Measure analysis. Figure 6c shows that the model proposed is much better.
4. Results of the proposed model is also estimated in terms of the Coefficient of Determination analysis as shown in Figure 6d. In the current scenario, it can be found that the presented model has a comparatively higher value of 95.63% which is far better as compared to other models.



(a) Accuracy

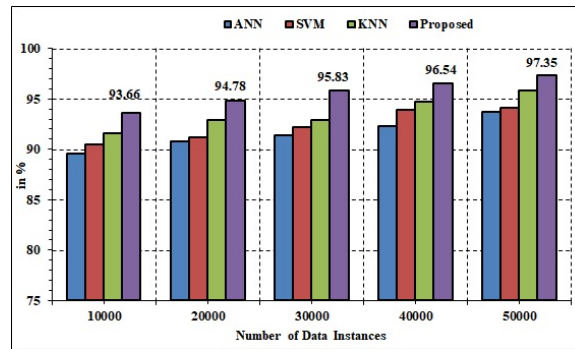


(b) Sensitivity



(c) F-Measure

Figure 6. Cont.



(d) Coefficient of Determination

Figure 6. Prediction Efficiency.

Henceforth, based on the results, it can be concluded that in the current scenario, the represented decision-making model is more effective and efficient than state-of-the-art decision-modeling techniques.

4.5. Reliability Assessment

To verify the reliable behavior of the presented framework, the prediction techniques are updated, and most of the system remains identical. The findings of the reliability assessment simulation are depicted in Figure 7. The average prediction model accuracy is defined by comparative reliability variations with 3 state-of-the-art prediction models such as Support Vector Machine (SVM), conventional Artificial Neural Network (cANN), and k-Nearest Neighbor (k-NN). Once the number of data sets for experimental implementation is expanded, efficiency levels are associated with higher values than other simulation strategies for the presented model. Particularly compared to K-NN, cANN, and SVM prediction models, the presented model has greater reliability of 93.15%. Reliability values have been registered as 90.91%, 91.72%, and 92.40% respectively for k-NN, cANN, and SVM. Based on these results, the proposed approach is more reliable over vast data sets relative to other decision-making models.

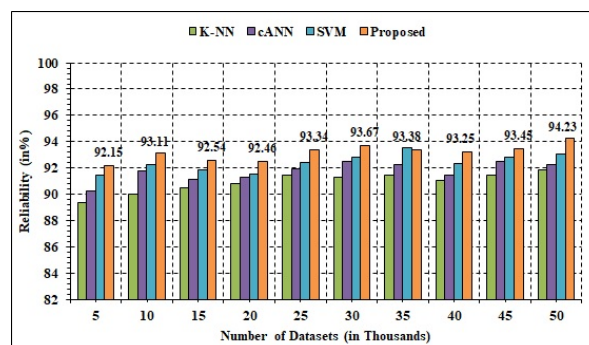


Figure 7. Reliability Analysis.

4.6. Stability Assessment

Stability assessment is performed for testing the presented model for durability over the large data instances. Moreover, the stability of the system predicts total stabilization measures when the system is deployed over large data sets for a long period. Mean Absolute Shift (MAS) is used to measure the stability of the system. The value of the MAS is within the range of (0, 1) where the value of 0 implies minimal stability, and the maximum stability is represented by 1. The findings for the stability assessment of the proposed system are shown in Figure 8. It is observed that the proposed model can register a least value of 0.54, and a maximum value of 0.81, therefore resulting in an average value

of 0.70. Conspicuously, the presented framework is highly suitable and stable for an identity-based assessment in the home environment.

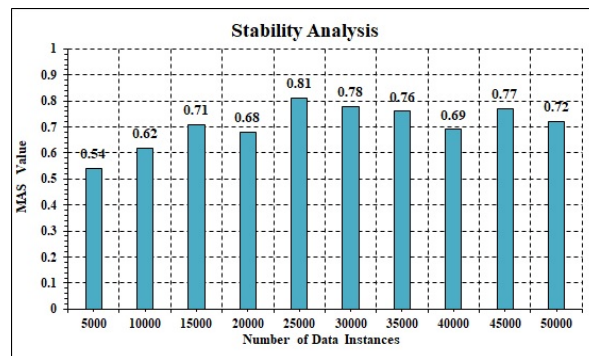


Figure 8. Overall System Stability.

5. Conclusions

Trio-logical aspects of IoT-fog-cloud technologies have presented numerous innovations in various industries. This study proposes an intruder detection framework based on an IoT-inspired foot mat. In particular, the overall goal of the proposed model is confined in 4 phases, namely the Data Perception Phase (DPP), Data Analysis Phase (DAP), Data Extraction Phase (DEP), and Intelligent Prediction Phase (IPP). Also, IoT data measures obtained from the smart mat are quantified in terms of the Probability of Authenticity (PoA) and Authentic Index (AI) measure. Moreover, a decision-making model inspired by Adaptive Neuro-Fuzzy Inference System (ANFIS) has been presented to predict the identity-based parameters recorded by the smart mat. A challenging dataset containing nearly 49,695 data instances is used for validation of the presented model. Statistical findings indicate that the proposed model has demonstrated increased values relative to state-of-the-art decision-making approaches. Conspicuously, it can be concluded that the presented model is substantially efficient and effective in detecting unauthentic personnel. For future research directions, network security is an important domain for exploration. Moreover, visualization of intruder parameters is another significant aspect of research.

Author Contributions: Conceptualization, methodology, and structure of the paper T.A.A. and U.T.; implementation T.A.A. and I.U.; writing—original draft preparation T.A.A. and Y.B.; writing—review and editing, U.T. and I.U.; supervision, A.I. All authors have read and agreed to the published version of the manuscript.

Funding: There is no external funding for this research work.

Acknowledgments: The authors would like to acknowledge the support of the Deanship of Scientific Research at Prince Sattam Bin Abdulaziz University under the research project # 2020/01/16466.

Conflicts of Interest: The authors declare no conflict of interest. The funders had no role in the design of the study; the collection, analyses, or interpretation of data; the writing of the manuscript, or the decision to publish the results.

References

- Gubbi, J.; Buyya, R.; Marusic, S.; Palaniswami, M. Internet of Things (IoT): A vision, architectural elements, and future directions. *Future Gener. Comput. Syst.* **2013**, *29*, 1645–1660. [\[CrossRef\]](#)
- Bhatia, M.; Sood, S.K. Temporal informative analysis in smart-ICU monitoring: M-HealthCare perspective. *J. Med. Syst.* **2016**, *40*, 190. [\[CrossRef\]](#)
- Lee, I.; Lee, K. The Internet of Things (IoT): Applications, investments, and challenges for enterprises. *Bus. Horiz.* **2015**, *58*, 431–440. [\[CrossRef\]](#)
- Bhatia, M.; Sood, S.K.; Kaur, S. Quantum-based predictive fog scheduler for IoT applications. *Comput. Ind.* **2019**, *111*, 51–67. [\[CrossRef\]](#)
- Sheth, A. Internet of things to smart iot through semantic, cognitive, and perceptual computing. *IEEE Intell. Syst.* **2016**, *31*, 108–112. [\[CrossRef\]](#)

6. Stojkoska, B.L.R.; Trivodaliev, K.V. A review of Internet of Things for smart home: Challenges and solutions. *J. Clean. Prod.* **2017**, *140*, 1454–1464. [\[CrossRef\]](#)
7. Bhatia, M.; Kaur, S.; Sood, S.K. IoT-Inspired Smart Toilet System for Home-Based Urine Infection Prediction. *ACM Trans. Comput. Healthc.* **2020**, *1*, 1–25. [\[CrossRef\]](#)
8. Javed, M.A.; Zeadally, S.; Hamida, E.B. Data analytics for Cooperative Intelligent Transport Systems. *Veh. Commun.* **2019**, *15*, 63–72. [\[CrossRef\]](#)
9. Bhatia, M.; Manocha, A. Cognitive Framework of Food Quality Assessment in IoT-inspired Smart Restaurants. *IEEE Internet Things J.* **2020**. [\[CrossRef\]](#)
10. Westermann, O.; Förch, W.; Thornton, P.; Körner, J.; Cramer, L.; Campbell, B. Scaling up agricultural interventions: Case studies of climate-smart agriculture. *Agric. Syst.* **2018**, *165*, 283–293. [\[CrossRef\]](#)
11. Khan, M.A.; Salah, K. IoT security: Review, blockchain solutions, and open challenges. *Future Gener. Comput. Syst.* **2018**, *82*, 395–411. [\[CrossRef\]](#)
12. Andreev, S.; Petrov, V.; Huang, K.; Lema, M.A.; Dohler, M. Dense Moving Fog for Intelligent IoT: Key Challenges and Opportunities. *IEEE Commun. Mag.* **2019**, *57*, 34–41. [\[CrossRef\]](#)
13. Bonomi, F.; Milito, R.; Zhu, J.; Addepalli, S. Fog computing and its role in the internet of things. In Proceedings of the First Edition of the MCC Workshop on Mobile Cloud Computing, Helsinki, Finland, 17 August 2012; pp. 13–16.
14. Bhatia, M.; Sood, S.K. Quantum Computing-inspired Network Optimization for IoT Applications. *IEEE Internet Things J.* **2020**. [\[CrossRef\]](#)
15. Chiang, M.; Zhang, T. Fog and IoT: An overview of research opportunities. *IEEE Internet Things J.* **2016**, *3*, 854–864. [\[CrossRef\]](#)
16. Jacobsson, A.; Boldt, M.; Carlsson, B. A risk analysis of a smart home automation system. *Future Gener. Comput. Syst.* **2016**, *56*, 719–733. [\[CrossRef\]](#)
17. Yassine, A.; Singh, S.; Hossain, M.S.; Muhammad, G. IoT big data analytics for smart homes with fog and cloud computing. *Future Gener. Comput. Syst.* **2019**, *91*, 563–573. [\[CrossRef\]](#)
18. Boveiri, H.R.; Khayami, R.; Elhoseny, M.; Gunasekaran, M. An efficient Swarm-Intelligence approach for task scheduling in cloud-based internet of things applications. *J. Ambient Intell. Hum. Comput.* **2019**, *10*, 3469–3479. [\[CrossRef\]](#)
19. Kim, T.H.; Hong, Y.S. Prediction of Body Weight of a Person Lying on a Smart Mat in Nonrestraint and Unconsciousness Conditions. *Sensors* **2020**, *20*, 3485. [\[CrossRef\]](#)
20. Matthies, D.J.; Elvitigala, D.S.; Muthukumarana, S.; Huber, J.; Nanayakkara, S. CapMat: A smart foot mat for user authentication. In Proceedings of the 10th Augmented Human International Conference 2019, Reims, France, 11–12 March 2019; pp. 1–2.
21. Huang, D.Y.; Apthorpe, N.; Li, F.; Acar, G.; Feamster, N. Iot inspector: Crowdsourcing labeled network traffic from smart home devices at scale. *Proc. ACM Interact. Mob. Wearable Ubiquit. Technol.* **2020**, *4*, 1–21. [\[CrossRef\]](#)
22. Minoli, D. Positioning of blockchain mechanisms in IOT-powered smart home systems: A gateway-based approach. *Internet Things* **2020**, *10*, 100147. [\[CrossRef\]](#)
23. Mallikarjuna, B. Feedback-Based Resource Utilization for Smart Home Automation in Fog Assistance IoT-Based Cloud. *Int. J. Fog Comput. (IJFC)* **2020**, *3*, 41–63. [\[CrossRef\]](#)
24. Desai, R.; Gandhi, A.; Agrawal, S.; Kathiria, P.; Oza, P. IoT-Based Home Automation with Smart Fan and AC Using NodeMCU. In *Proceedings of ICRIC 2019*; Springer: Heidelberg, Germany, 2020; pp. 197–207.
25. Popa, D.; Pop, F.; Serbanescu, C.; Castiglione, A. Deep learning model for home automation and energy reduction in a smart home environment platform. *Neural Comput. Appl.* **2019**, *31*, 1317–1337. [\[CrossRef\]](#)
26. Ranjan, J.; Yao, Y.; Whitehouse, K. An RF doormat for tracking people's room locations. In Proceedings of the 2013 ACM International Joint Conference on Pervasive and Ubiquitous Computing, Zurich, Switzerland, 12–16 September 2013; pp. 797–800.
27. Cheng, J.; Sundholm, M.; Zhou, B.; Hirsch, M.; Lukowicz, P. Smart-surface: Large scale textile pressure sensors arrays for activity recognition. *Pervas. Mob. Comput.* **2016**, *30*, 97–112. [\[CrossRef\]](#)
28. Sokullu, R.; Akkaş, M.A.; Demir, E. IoT Supported Smart Home for the Elderly. *Internet Things* **2020**, *11*, 100239. [\[CrossRef\]](#)

29. Suciu, G.; Suci, V.; Martian, A.; Craciunescu, R.; Vulpe, A.; Marcu, I.; Halunga, S.; Fratu, O. Big data, internet of things and cloud convergence—an architecture for secure e-health applications. *J. Med. Syst.* **2015**, *39*, 141. [\[CrossRef\]](#)
30. Sun, E.; Zhang, X.; Li, Z. The internet of things (IOT) and cloud computing (CC) based tailings dam monitoring and pre-alarm system in mines. *Saf. Sci.* **2012**, *50*, 811–815. [\[CrossRef\]](#)
31. Sowjanya, G.; Nagaraju, S. Design and implementation of door access control and security system based on IOT. In Proceedings of the 2016 International Conference on Inventive Computation Technologies (ICICT), Coimbatore, India, 26–27 August 2016; Volume 2, pp. 1–4.
32. Sha, K.; Wei, W.; Yang, T.A.; Wang, Z.; Shi, W. On security challenges and open issues in Internet of Things. *Future Gener. Comput. Syst.* **2018**, *83*, 326–337. [\[CrossRef\]](#)
33. Dabbagh, M.; Rayes, A. Internet of things security and privacy. In *Internet of Things from Hype to Reality*; Springer: Heidelberg, Germany, 2019; pp. 211–238.
34. Ammar, M.; Russello, G.; Crispo, B. Internet of Things: A survey on the security of IoT frameworks. *J. Inf. Secur. Appl.* **2018**, *38*, 8–27. [\[CrossRef\]](#)
35. Mendez Mena, D.; Papapanagiotou, I.; Yang, B. Internet of things: Survey on security. *Inf. Secur. J. A Glob. Persp.* **2018**, *27*, 162–182. [\[CrossRef\]](#)
36. Stergiou, C.; Psannis, K.E.; Kim, B.G.; Gupta, B. Secure integration of IoT and cloud computing. *Future Gener. Comput. Syst.* **2018**, *78*, 964–975. [\[CrossRef\]](#)
37. Sun, W.; Cai, Z.; Li, Y.; Liu, F.; Fang, S.; Wang, G. Security and privacy in the medical internet of things: A review. *Secur. Commun. Netw.* **2018**, *2018*, 5978636. [\[CrossRef\]](#)
38. Dastjerdi, A.V.; Buyya, R. Fog computing: Helping the Internet of Things realize its potential. *Computer* **2016**, *49*, 112–116. [\[CrossRef\]](#)
39. Tang, B.; Chen, Z.; Hefferman, G.; Pei, S.; Wei, T.; He, H.; Yang, Q. Incorporating intelligence in fog computing for big data analysis in smart cities. *IEEE Trans. Ind. Inform.* **2017**, *13*, 2140–2150. [\[CrossRef\]](#)
40. Atlam, H.F.; Walters, R.J.; Wills, G.B. Fog computing and the internet of things: A review. *Big Data Cogn. Comput.* **2018**, *2*, 10. [\[CrossRef\]](#)
41. Moon, T.K. The expectation-maximization algorithm. *IEEE Signal Process. Mag.* **1996**, *13*, 47–60. [\[CrossRef\]](#)
42. Liao, Y.; Xu, B.; Liu, X.; Wang, J.; Hu, S.; Huang, W.; Luo, K.; Gao, L. Using a Bayesian belief network model for early warning of death and severe risk of HFMD in Hunan province, China. *Stochastic Environ. Res. Risk Assess.* **2018**, *32*, 1531–1544. [\[CrossRef\]](#)
43. Nauck, D.; Klawonn, F.; Kruse, R. *Foundations of Neuro-Fuzzy Systems*; John Wiley & Sons, Inc.: New York, NY, USA, 1997.
44. Jang, J.S. ANFIS: Adaptive-network-based fuzzy inference system. *IEEE Trans. Syst. Man Cybernet.* **1993**, *23*, 665–685. [\[CrossRef\]](#)
45. Nedjah, N.; de Macedo Mourelle, L. *Fuzzy Systems Engineering: Theory and Practice*; Springer Science & Business Media: Heidelberg/Germany, Germany, 2005; Volume 181.
46. Reddy, C.S.; Raju, K. An improved fuzzy approach for COCOMO's effort estimation using gaussian membership function. *J. Softw.* **2009**, *4*, 452–459. [\[CrossRef\]](#)
47. Gupta, H.; Vahid Dastjerdi, A.; Ghosh, S.K.; Buyya, R. iFogSim: A toolkit for modeling and simulation of resource management techniques in the Internet of Things, Edge and Fog computing environments. *Softw. Pract. Exp.* **2017**, *47*, 1275–1296. [\[CrossRef\]](#)

