JOURNAL OF MULTIDIMENSIONAL RESEARCH & REVIEW

**Website: http://www.jmrr.org** **Vol.2, Iss.2 Pages:61-75**

# A CONCEPTUAL VIEW OF BIOMETRIC USAGE IN IOT

**Dr G Yashodha**

**Dept of Computer Technology, KG College of Arts and Science, Coimbatore, Tamilnadu, India - 641043**

**Article Received: April 2021 Published: July 2021**

## Abstract

Internet of Things (IoT) is a catchword, where all digital devices are linking with each other to talk some information. These devices are encroaching on our daily life including home appliances, offices, health etc. Safety is the major concern for the Internet of Things (IoT). Whenever devices are linked then authentication is required for secure communication. So, authentication forms the gateway for a secure communication system. Authentication with text PINs still widely used but have become uncertain. Therefore, it is an vital concern to discourse by using biometric authentication. This paper presents the conceptual idea of securing internet of Things network using biometric authentication.

***Keywords: IoT, Biometric, Secure, Authentication, Digital devices***

## I INTRODUCTION

Internet of Things is the collection of interconnected devices connected to the Internet. To collect, store, and exchange data among each other, these devices are embedded with different types of actuators, wired/wireless sensors, and software along with other required electronic objects. Each device has an Internet Protocol (IP) address and is capable of collecting and transmitting information across a network without human assistance or interference. Some examples of IoT are autonomous vehicles, smart homes, wearables, connected healthcare systems, and tracking and monitoring systems. The architecture of IoT can be represented by the following four stages:

Networked Devices: Implanted sensors, actuators, and other important electronic gadgets gather data from the genuine actual world for additional handling.

Data Acquisition System: The data gathered from the past stage is typically as a simple sign. The job of the information procurement framework is to total and change over this sign into advanced structure for additional preparing.

Edge Analytics: After digitizing the data, the edge analytic stage is responsible for preprocessing and enhanced analysis before feeding it to cloud analytics.

Cloud Analysis: This is the last and significant phase of IoT engineering where inside and out examination occurs and criticism is produced. In light of amendment and meeting the quality and prerequisites, information is sent to the cloud-based framework or actual server farm. Figure 1 addresses the four-stage IoT design.

## II APPLICATION OF IOT

IoT has been executed in a few spaces, from keen home and keen city to modern robotization, individual to social applications, agribusiness to the medical services framework. IoT's capacity can in any case be utilized to assist society to grow new applications. A portion of the significant true uses of IoT are referenced underneath.

Wearables: Wearable innovation is most likely the principal IoT-sent industry, and the interest for its items expanded radically. Presently, savvy watches are utilized to screen dozing/strolling movement measure pulses, and screen circulatory strain.

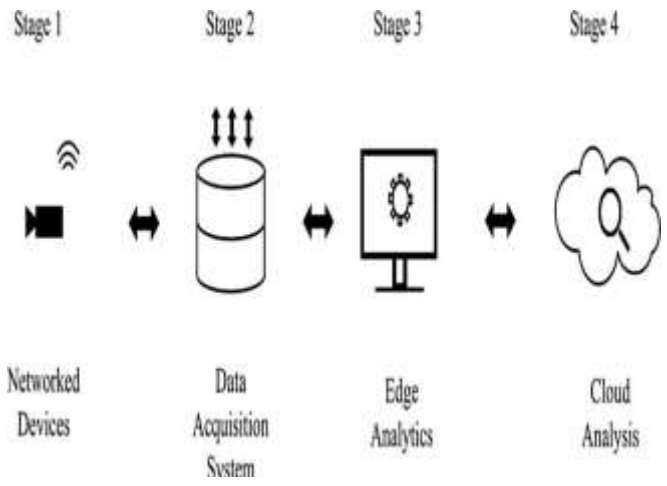


Fig 1 Architecture of IoT showing all four stages.

A tiny electrode that is responsible for collecting information is placed under the skin. Collected data from the sensor are sent to the monitoring device using radio frequency.

Smart Home: sensors and actuators that are associated with home devices, for example, climate control systems and coolers, can screen the climate in a house or office. These gadgets can likewise kill on/off light sensors like electric bulbs/CFLs agreeing today/night. A temperature sensor can handle cool dependent on the current climate. This will save a more prominent measure of electric energy just as cash. A savvy smoke alarm sensor can be utilized to distinguish fire/smoke and produce a caution. The framework can likewise be utilized to send the alarm message to the closest clinic and fire detachment division. A keen camera can distinguish mishaps and theft and create caution just as ready messages to the closest medical clinic just as police headquarters for additional activity naturally without clients' mediation. IoT-empowered water tab and clothes washer can save a gigantic measure of water.

These days, organizations are working together with one another to make IoT-empowered items to offer better support to clients. Philips has dealt with a venture named "Home of the not-so-distant future", where they planned shrewd actual articles utilized at home. A comparative exertion in IoT was made by Siemens, where they attempted to make each gadget astute with no interconnection among them. The specialist based shrewd home recreation framework was made at "The Multi-Agent Systems Lab" by the University of Massachusetts. Intel additionally delivered many home systems administration conventions (counting UPnP), which are open-source executions [1]. Despite the fact that we have created numerous insightful gadgets to make home brilliant, there are some open difficulties like security, selection to another climate, and significant expense of knowledge, which actually should be tended to [2].

Smart Cities: According to the UN report, by 2050, 66% of the world population will live in urban areas. In the survey, it is reported that Tokyo remains the world largest city (38 million inhabitants), followed by New Delhi (25 million), Shanghai (23 million), and Mexico and Mumbai (21 million each)1. With a drastic increase in the population, the consumption of

resources and the distribution of energy become a challenge. To minimize consumption and provide better service to the people in the city, IoT emerged as a great solution to this problem. The use of IoT can optimize resources such as water supply management; traffic network – to avoid congestion; power grid; and parking space. Cleanliness is also one of the important factors to make a city smart. The IoT technology can be used for the development of a smart waste management and sewage disposal system [3]. IoT-enabled meters can be used to monitor efficient electricity consumption and theft of electricity around the world [4]. Nowadays, IoT devices are used to monitor air and sound pollution and the purity of water supply. The IoT-enabled devices used to make a city smart are actually physical and can be vulnerable to break of a cyber-attack. Therefore, the data collected by these devices must be secured to assure the safety of people in the city where they live and work.

Industrial Automation: For any industry, the quality of the product and faster development play a crucial role in the return of the investment. A moderate-scale industry requires high manpower to maximize the development of products. Their production can be faster if the IoT technique is used for the automation of products, even from re-engineering to packaging. A plant/factory can be operated and maintained remotely; information exchange between IoT-enabled devices can maximize the productivity [5]. Real-time data acquired by sensors can be used to automate and quicken the manufacturing process at a low cost. However, using IoT in industry automation is very challenging. General challenges

such as data and service security, trust, information privacy, and data integrity need to be assured.

Health Care: While we have achieved significant results in improving people's health through medicines and antidotes, accuracy is still needed in medical diagnostic reporting and

real time; monitor the collection of test samples such as blood and urine; automatically gather information such as blood disease detection at an early stage. Health care is another area where IoT can be used to track people (staff and patients) in real time; monitor the collection of test samples such as blood and urine; automatically gather information such as blood pressure, diabetes, and body temperature according to the scheduled date and time; and authen-ticate hospital staff to access a secure place and monitor patients based on their biometric characteristics and help them to avoid mistakes that are usually made, such as drug, dose, and time [6,7].

Agriculture: This is one of the sectors that can be largely influenced by the use of IoT [8]. In countries such as India, Bangladesh, and Brazil, most of the people stay in rural areas, and their profession is agriculture. The use of IoT-enabled devices not only decreases human effort but also increases productivity [9]. Enabling automation in agriculture by collecting information such as nutrients and humidity suggests the best time for irrigation; optimizing the use of fertilizers can save money, time, and effort of farmers.

## III TYPES OF SECURITY AND ATTACKS IN IOT

IoT is just an arrangement of contraptions that are related with each other similarly as the Internet. These contraptions accumulate each and such a data, for instance, a for every kid's name, age, address, money related advancement status, credit/charge card nuances, prosperity information, and biometric data, and store them in the device. They similarly share these nuances with various contraptions whenever required. The interconnected and between frameworks organization plan of IoT makes it by and large exposed against attack. Coming up next are the five essential kinds of attacks that can be made in IoT [10].

Man-in-the-Middle Attack: In this type of attack, an attacker invades communication between the sender and the receiver, and the invader acts as an original sender and sends a fake message to the receiver, while the receiver thinks that he/she is getting a message from the actual sender.

Botnet: A botnet is a network of devices integrated for remote control and malware delivery. This type of attack is used by hackers/criminals to steal personal data, banking information, and push emails [11].

Denial-of-Service (DoS): This type of attack generally happens when a ser-vice that usually works is unavailable. At the time of unavailability, devices through botnet are programmed to request the service [12].

Social Engineering: In this type of attack, the goal of an attacker is to get personal information such as email ID and bank account details from an individual. Attackers try to access the target system and install malicious software so that whenever authorized persons access the sensitive data, it can redirect these secure data to attackers.

Physical Attack: Due to the distributed nature of IoT, most of the devices are used outdoors, and attackers try to tamper with hardware components [10].

The need for security isn't restricted to having the chance to get information over the Internet or PC structure. There are different applications that we access in our reliably life, like banking, PDAs, certifiable access of IoT-connected with contraptions, and PC assets, which need insistence. To attest IoT as a got structure, perceiving proof of an individual who gets to IoT-empowered gadgets truly is essential. All together to upgrade security in IoT, we by and large utilize a prominent proof card or sharp card, secret articulation, or PIN. These standard strategies for check are now utilized by us, at any rate there are sure cut off focuses; for instance, a sharp card can be lost or taken, and reviewing complex passwords is badly designed, while a direct secret key can be guessed by the computer programmer with relatively few endeavors. Biometric is one of the reactions for bear these difficulties and issues. As such, in the going with zone, we talk about biometrics, kinds of biometrics and its attributes, and the working model of a biometric structure in detail.

## IV INTRODUCTION OF BIOMETRIC SECURITY

Compared to traditional methods of authentication, biometrics proved to be the most secure one. In simple words, biometrics is the process of identifying a per-son based on their biological

traits. The most commonly used traits for authentication are fingerprint, face, iris, ear, gait, etc. The selection of these traits depends on the application and deployment environment. Biometrics is divided into two types of modality: (1) Behavioral and (2) Physiological. The traits under both types of modalities are shown in Figure 2. A detailed description of these modalities is given below.

A. Behavioral Modality

Social biometrics is the field of study identified with the examination of practices in human exercises that are extraordinary in acknowledgment and estimation. It incorporates examination of the example of mouse use, stride example, and keystroke design; signature investigation; and investigation of the example of holding a cell phone and squeezing catches [13]. A portion of these attributes that are generally utilized for validation are clarified beneath.

Gait: The walking pattern of a human being is known as gait pattern. It has been proved that the gait pattern of each person is unique and it can be used to identify an individual [14]. Using IoT-enabled devices and sensors (wearable and non-wearable), it is easy to capture gait data and extract statistical features for further analysis [15]. Parameters and features that can be extracted by gait pattern using machine learning techniques are the velocity of a subject, placement distance between two successive steps, foot direction, the number of steps in a unit time, etc.

Signature: Signature matching is still used by some systems to identify peo-ple every day. However, it is easy to copy someone's style of signature. Many applications have been developed to recognize a person based on their signature. These systems measure the speed, shape, speed of strokes, acceleration, and pressure on the pad while signing [16]. Machine learning algorithms are widely used to improve the performance of the system.

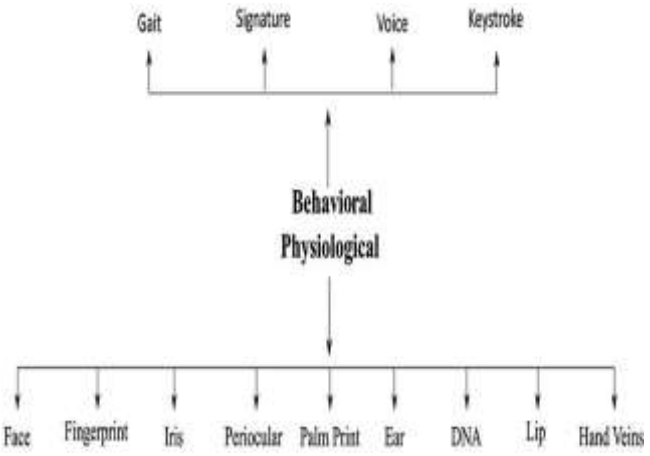


Fig 2 Biometric traits in physiological and behavioral modalities.

However, accuracy is still a challenging issue and needs to be improved.

Keystroke: In Ref. [13], it has been reported that a user can be identified based on their typing pattern. The speed at which the user presses a key, the time between two successive keypresses, finger placing pattern, etc., can be measured by machine learning techniques. A similar effort was made in Ref. [17], where a better result was obtained using an optimizer in deep learning.

Voice: IoT-enabled sensors can be used to measure the movement of lips, jaws, and tongue. Parameters such as the pitch and intensity of sound can be considered as a feature, and machine learning/deep learning models can be trained to recognize a person based on their voice [18]

B. Physiological Modality

Fingerprint: From academics to companies, the physiological biometric system is one of the most used applications. The reason behind this is that in any environment, it can be easily installed and used by the users. Cost-effective maintenance makes it suitable for small organizations. The texture pattern of the human fingers has been shown to have ridges and valleys (also known as "minutiae" points) and is unique for each person. These features can be extracted using image processing and machine learning techniques, which can be used to match a query with database samples [19].

Face: After fingerprint, face is another characteristic that is used to identify an individual. The benefit of this approach is that it does not require user participation and is ideal for an unconstrained environment. Features such as local binary pattern (LBP), principal component analysis (PCA), lin-ear discriminant analysis (LDA), and phase intensive global pattern (PIGP) are some popular algorithms used to extract features from the face image. These features are used to train machine learning models using various ML techniques [20–23].

## V SECURITY OF A BIOMETRIC SYSTEM AGAINST SEVERAL TYPES OF ATTACKS

The assaults on a biometric framework can be named immediate and circuitous assaults [37]. Direct assaults are done by assaulting the biometric ID gadgets themselves, while in aberrant assaults, assailants attempt to break security by attacking the correspondence channel or any product module. In direct assaults, an alternate personality can be made by the assailant without giving any biometric attribute, while in parodying, an aggressor attempts to enter the biometric framework by introducing a character of another person [24].

To get the biometric framework from caricaturing assaults, it is important to recognize genuine biometric characteristics introduced to the sensor and falsely made examples. For this reason, in Ref. [25], an enemy of mocking strategy was proposed for face acknowledgment applications. The contemplated strategy is isolated into three levels, i.e., information obtaining level (sensor), highlight extraction level, and score age level. At these levels, distinctive AI procedures are utilized for various purposes.

A similar effort was made by Chingovska et al. in Ref. [26]. They developed an anti-spoofing framework named Expected Performance and Spoofability (EPS) using the Replay-Attack

database. They used four baseline face verification systems based on Gaussian mixture model (GMM), local Gabor binary pattern histogram sequences (LGBPHS), Gabor jets (GJet), and intersession variability (ISV) modeling using discrete cosine transform (DCT) features. The performance of the system is evaluated by calculating the false acceptance rate (FAR), false rejection rate (FRR), half total error rate (HTER), and SFAR (the rate of wrongly accepted spoofing attacks). Compared to all, the performance of ISV is found to be good.

In Ref. [27], the vulnerability of face recognition-based biometric against spoo-ing attacks was investigated. A part-based face representation and GMM proposed by McCool and Marcel [28] was used for the face verification system. The studied method was evaluated on 1300 video clips, and the author investigated attacks attempting to collect 50 different identities. The experimental result shows the maximum vulnerability of the face database.

Choi et al. considered refusal of-administration (DoS) assaults [29]. They found a weakness in Yoon and Kims [30], like absence of secrecy, biometric acknowledgment blunder, check issue, and weakness to a DoS assault. Expanding Yoon and Kims' work, they proposed fluffy extraction-based biometric validation in the remote sensor organization. They led a security examination analysis to assess the presentation of the proposed technique and found the recommended approach is safer contrasted with other confirmation strategies.

To adapt to the replay assault, in Ref. [31], hereditary and transformative biometric security (GEBS) was proposed by Shelton et al. They created dispensable component extractors (FEs) utilizing hereditary and transformative calculation and proposed two supportive of tocols dependent on the utilization of FEs and their format or highlight vector (FV), which are utilized to verify an individual. Exploratory results guarantee that the created applications are effectively used to conquer the issue of a replay assault.

More often than not, individuals imagine that formats put away in the data set are secure, however indeed, those put away layouts can be controlled by the aggressor. Accordingly, in Ref. [32], Shehu et al. contemplated a strategy to identify altering in the highlights put away in the information base. SVM is prepared utilizing unique just as tempered layouts of the finger impression information base. The test result shows that the proposed approach can identify modification with 90% exactness.

The assaults made on the different modules, particularly at information securing gadgets, can be abstained from by separating segregating highlights and utilizing proper AI arrangement strategies to settle on an official conclusion. A grouping strategy is supposed to be acceptable on the off chance that it can order real and faker clients and limit bogus acknowledgment and dismissal with adequate exactness. The most mainstream and generally utilized arrangement procedures in AI are examined underneath.

## VI MACHINE LEARNING ALGORITHMS USED TO DEVELOP BIOMETRIC SYSTEMS IN IOT

The presentation of a biometric framework can be improved by utilizing different AI methods to remove and examine predominant aspects. A few characterization calculations have been proposed and effectively used to group authentic and sham subjects from an enormous populace. This part talks about the arrangement techniques that exist in the writing, which are by and large used to build up a biometric framework.

k-Nearest Neighbors (KNN): KNN is one of the most fundamental but essential classification algorithms. It is also called a lazy method of learn-ing, which stores the vectors in the training dataset, and until classification, all processing is delayed. The feature vector is extracted and compared with all stored samples by means of a distance function when the system is requested with a query sample. The algorithm returns class as a result along with the k-nearest neighbor of the queried sample. It is used in the supervised learning field and can be used to detect intrusion and in data mining applications and pattern recognition. Due to its ability to classify data efficiently, it is also used in biometrics.

In Ref. [33], an efficient method of personal identification using KNN was proposed. Extending the work of Gunetti et al. (where they compared query input to every sample of the database [48]), in this study, the use of KNN classifier is limited to the number of comparisons within a cluster. However, the calculated FAR and FRR are found to be as in [34], but authentication performance is improved by 66.7%. ANN is one of the powerful and frequently used techniques to train a model. However, with less amount of data, the system fails to classify a new test sample. Therefore, in Ref. [35], Azmi et al. trained KNN by extracting the Freeman chain code (FCC) as a feature. Performance result is obtained by evaluating it on the MCYT bimodal database using Euclidean distance as a similarity measure, and verification is performed using KNN. The experimental result claims that the proposed method produces better outcomes compared to other methods when tested on the same database with an FRR and FAR of 6.67% and 12.44%, respectively, with an AER of 9.85%.

Support Vector Machine (SVM): SVM is a generally utilized classifier for grouping and relapse issues. Its will probably fit a hyperplane that can isolate various classes. Because of its force and straightforwardness to prepare/test the ML model, it is broadly utilized in biometric applications [36,37]. It has been effectively used to characterize individuals dependent on their physiological and social qualities. In Ref. [38], individuals distinguishing proof dependent on client communication designs with the cell phone was proposed. Contact information were gathered, and a model was prepared by learning the touch example of clients during the enlistment stage. KNN, just as SVM with RBF part, was utilized for order. The trial result shows that the framework can acknowledge/reject individuals dependent on the way he/she utilizes the gadget. The proposed technique yields an EER of 0% and somewhere in the range of 2% and 3% in an intra-meeting and intersession verification climate, individually. Individual recognizable proof dependent on the finger vein design was proposed by Wu et al. [39]. In their examination, they utilized CCD and infrared LED cameras to catch tests. Pictures were preprocessed to eliminate commotion, and highlights were separated utilizing direct discriminant investigation (LDA). To accelerate the distinguishing proof cycle, head part examination (PCA) was applied to decrease the element measurement. SVM was utilized for

grouping. From the trial, 98% grouping exactness was noticed, and the framework can recognize individuals in 0.015 seconds.

Naive Bayes (NB): The NB classifier assumes that the probability distribution of the feature vector of a subject is the same as if that user returns in future and claims for authentication by giving the same biometric trait that was given during enrollment. It also assumes the values of feature vectors extracted from a subject are different and unique to the features of other subjects.

To show the effectiveness of the NB classifier, in Ref. [40], a finger vein-based biometric identification system was developed. Database images were preprocessed, followed by the region-of-interest (ROI) selection; afterward, fast filter, Gabor filter, and freak descriptor were used to extract the feature that was trained using the naive Bayes classifier. For comparison of the results, discriminant analysis of extracted features was done. The experimental result shows the superiority of the NB classifier with an accuracy of 98.38% over discriminant analysis (94.46%). Although it was possible to extract discriminating patterns using feature extraction techniques, all these patterns were not useful and increased the dimension of features. Therefore, a feature subset selection approach was studied by Kumar et al. in Ref. [41]. They extracted features from hand images and selected a subset of the pattern from whole features, which are necessary to build an identification system. They used several classifiers such as KNN, SVM, decision tree, naive Bayes, and FFN to compare the performance of the proposed method.

Decision Trees (DT): For forecast and grouping issues, choice tree is considered as a successful method that encourages the framework to settle on choices dependent on the arrangement of rules. In the space of biometrics, include vector segments are assessed by choice hubs, while leaf addresses the subject alloted to each biosignal. In Ref. [42], a choice tree-based examination done by Kumar et al., the creators characterized certifiable and fraud clients by settling on a choice dependent on the fluffy parallel choice tree (FBDT) calculation. To validate a client utilizing the keystroke design, in Ref. [43], client distinguishing proof dependent on an equal choice tree was proposed. In this examination, eight preparing subsets of every client were acquired by separating the preparation set into four subsets, trailed by a wavelet change of each subject. The presentation of the calculation was assessed by figuring the bogus dismissal rate and bogus acknowledgment pace of 9.62% and 0.88%, individually.

Random Forest (RF): Like other ML calculations, irregular tree is utilized in characterization and relapse issues. It extricates information from information. As the name recommends, it is an assortment of choice trees. During order utilizing the arbitrary backwoods, every choice tree predicts a class mark, and dependent on the greatest vote, irregular tree settles on a choice. Because of its incredible exhibition, it is perhaps the most utilized methods to make expectations in biometric security.

An indoor area acknowledgment framework dependent on Wi-fi utilizing the savvy and the arbitrary woodland was proposed in Ref. [44]. To situate acknowledgment issues, the creators

utilized the Basic Service Set Identifier (BSSID) and the Received Signal Strength Indication (RSSI). Execution speed and exactness of the framework were improved by applying the sifting interaction and irregular timberland. The trial result shows the reliable exhibition independent of less information and area data. In Ref. [45], the irregular timberland was utilized to settle on choices dependent on the coordinating with scores produced by numerous biometric gadgets. Three biometric gadgets dependent on face, finger impression, and hand math were utilized for experimentation. Consolidating scores produced by these gadgets, the exhibition of irregular woods was examined. The creators additionally led probes an alternate subset of the dataset.

Gaussian Mixture Model (GMM): The objective of GMM is to group the data points that belong to the same distribution. In the biometric system, a GMM is generated for each class, and for a given query image, the sample is compared with the GMM of all classes to generate likelihood as an output [46]. Based on the result, the sample is considered to belong to the class that has a maximum likelihood. The Gaussian mixture model is mostly used to develop a voice-based biometric system [47] and to develop a multi-model authentication system based on face and speech [48,49].

Convolutional Neural Network (CNN): Utilizing AI methods, we get critical accomplishment to get framework utilizing biometric highlights. Be that as it may, in some cases, the framework neglects to validate an individual in an unconstrained climate. Customary strategies for confirmation dependent on ML remove includes physically and characterize them utilizing SVM, KNN, and so forth These handpicked highlights are not adequate to recognize a subject; accordingly, a programmed method of highlight extraction is required. This is the reason the utilization of profound learning in the field of biometrics comes into the image. Profound l acquiring (convolutional neural organization) takes in highlights from the given information consequently and utilizes the learned information to settle on a choice on new information. CNN creates high precision as well as rates up the ID favorable to cess, which is an incredible requirement for gadgets associated in the IoT climate

To validate an individual utilizing an IoT-empowered gadget utilizing iris as a biofeature, Liao et al. prepared a U-formed CNN design [50]. The exhibition of the strategy was assessed on the CASIA and BATH data sets, which comprise of 20,000 and 24,156 picture tests, separately. The exploratory outcomes show that the proposed strategy can yield 98.55% and 99.71% exactness on the BATH and CASIA iris data sets, separately. In Ref. [51], a finger vein acknowledgment based verification framework utilizing profound learning was examined. They built up a structure named FVR-DLRP, which can ensure unique biometric information regardless of whether the aggressor translates the client's secret key.

A liveness and face acknowledgment based admittance control model was proposed by Chandraker et al. [52]. In Ref. [53], a computerized entryway lock framework was intended to reinforce the security in the IoT climate. The created framework can catch the picture of an individual and send it to the cell phone if an unapproved client endeavors to break the entryway lock. A comparable exertion toward the improvement of home security in IoT utilizing face acknowledgment was made in Ref. [54].

In Ref. [55], security the board for live video investigation in IoT was considered. RTFace was fabricate dependent on between outline following and OpenFace. Utilizing RTFace, a protection mindful design was proposed.

## VII CONCLUSION

With upgrades in of Internet and correspondence innovations, the interest for IoT has expanded. In this way, protection and security of assortment and capacity of sensi-tive data turns into a test. There are numerous sorts of safety assaults that can happen at an alternate degree of IoT design. In this examination, we talked about a portion of these assaults, like man-in-the-center, disavowal of-administration, botnet, and actual assault. To get to a gotten framework, validation and approval of end clients dependent on conventional methods just as the utilization of biometrics is clarified. We pre-sented a working model of a biometric framework, diverse biometric modalities, and the attributes used to distinguish an individual. Weakness in biometrics, for example, assault on information assortment gadgets, include extraction methods, the biometric data set itself, and dynamic module is featured. We talked about different strategies for identification of assaults, for example, mocking assault, replay assault, and disavowal of-administration on the biometric framework utilizing AI methods. We additionally talked about techniques to get biometric parts, for example, formats in the data set and information procurement gadgets themselves. AI strategies utilized for preparing just as characterizing certifiable and counterfeit clients, for example, k-closest neighbors, support vector machine, guileless Bayes classifier, choice trees, arbitrary woodland, and Gaussian combination model are clarified in a nutshell alongside their applications accessible in the writing. At last, we present a cutting edge profound learning method and its presentation to recognize an individual dependent on their biometric attributes. For this reason, we prepared a CNN model like yet more modest (top to bottom) than ResNet with two norm and freely accessible face and iris information bases. Execution boundaries were determined, and the presentation of the contemplated model was contrasted and customary ML strategies. The exploratory outcome obviously shows the excellency of profound learning as far as exactness, review, F1-score, and precision for both the face and iris information bases.

The use of biometrics is developing alongside development in the interest of IoT. Thusly, we can presume that procedures, for example, profound learning in biometrics can be utilized to improve the exhibition and security of IoT-empowered gadgets, secure information move, distinguish phony and authentic clients, keep an eye on a city and traffic in a savvy way, and perceive an individual and crime without any problem.

## REFERENCES

1. Li Jiang, Da-You Liu, and Bo Yang. Smart home research. In Proceedings of International Conference on Machine Learning and Cybernetics (IEEE Cat. No. 04EX826), vol. 2, pp. 659–663. IEEE, 2004. DOI: 10.1109/ICMLC.2004.1382266.

2. Meensika Sripan, Xuanxia Lin, Ponchan Petchlorlean, and Mahasak Ketcham. Research and thinking of smart home technology. In International Conference on Systems and Electronic Engineering (ICSEE 2012), pp. 61–63, 2012.

3. Andrea Zanella, Nicola Bui, Angelo Castellani, Lorenzo Vangelista, and Michele Zorzi. Internet of things for smart cities. IEEE Internet of Things Journal, 1(1): 22–32, 2014. DOI: 10.1109/JIOT.2014.2306328.
4. Miao Yun and Bu Yuxin. Research on the architecture and key technology of internet of things (IoT) applied on smart grid. In International Conference on Advances in Energy Engineering, pp. 69–72. IEEE, 2010. DOI: 10.1109/ICAEE.2010.5557611.
5. Hongyu Pei Breivold and Kristian Sandstro¨m. Internet of things for industrial automation–challenges and technical solutions. In IEEE International Conference on Data Science and Data Intensive Systems, pp. 532–539. IEEE, 2015. DOI: 10.1109/DSDIS.2015.11.
6. Nicola Bui and Michele Zorzi. Health care applications: A solution based on the internet of things. In Proceedings of the 4th International Symposium on Applied Sciences in Biomedical and Communication Technologies, p. 131. ACM, 2011. DOI:10.1145/2093698.2093829.
7. Amir-Mohammad Rahmani, Nanda Kumar Thanigaivelan, Tuan Nguyen Gia, Jose Granados, Behailu Negash, Pasi Liljeberg, and Hannu Tenhunen. Smart e-health gate-way: Bringing intelligence to internet-of-things based ubiquitous healthcare systems. In 12th Annual IEEE Consumer Communications and Networking Conference (CCNC), pp. 826–834. IEEE, 2015. DOI: 10.1109/CCNC.2015.7158084.
8. Yifan Bo and Haiyan Wang. The application of cloud computing and the internet of things in agriculture and forestry. In International Joint Conference on Service Sciences, pp. 168–172. IEEE, 2011. DOI: 10.1109/IJCSS.2011.40.
9. Ji-chun Zhao, Jun-feng Zhang, Yu Feng, and Jian-xin Guo. The study and application of the IoT technology in agriculture. In 3rd International Conference on Computer Science and Information Technology, vol. 2, pp. 462–465. IEEE, 2010. DOI: 10.1109/ICCSIT.2010.5565120.
10. Mohamed Abomhara and Geir M. Køien. Cyber security and the internet of things: Vulnerabilities, threats, intruders and attacks. Journal of Cyber Security and Mobility, 4(1): 65–88, 2015. DOI: 10.13052/jcsm2245-1439.414.
11. Elisa Bertino and Nayeem Islam. Botnets and internet of things security. Computer, (2): 76–79, 2017. DOI: 10.1109/MC.2017.62.
12. Lulu Liang, Kai Zheng, Qiankun Sheng, and Xin Huang. A denial of service attack method for an IoT system. In 2016 8th International Conference on Information Technology in Medicine and Education (ITME), pp. 360–364. IEEE, 2016. DOI: 10.1109/ITME.2016.0087.
13. Mohammad S Obaidat, Soumya Prakash Rana, Tanmoy Maitra, Debasis Giri, and Subrata Dutta. Biometric security and internet of things (IoT). In Biometric-Based Physical and Cybersecurity Systems, pp. 477–509. Springer, 2019. DOI: 10.1007/978-3-319-98734-719.
14. David Cunado, Mark S Nixon, and John N Carter. Using gait as a biometric, via phase-weighted magnitude spectra. In International Conference on Audio-and Video-Based Biometric Person Authentication, pp. 93–102. Springer, 1997. DOI: 10.1007/BFb0015984.
15. Alvaro Muro-De-La-Herran, Begonya Garcia-Zapirain, and Amaia Mendez-Zorrilla. Gait analysis methods: An overview of wearable and non-wearable systems, high-lighting clinical applications. Sensors, 14(2): 3362–3394, 2014. DOI: 10.3390/s140203362.
16. Andreas Fischer and Réjean Plamondon. Signature verification based on the kinematic theory of rapid human movements. IEEE Transactions on Human-Machine Systems, 47(2): 169–180, 2016. DOI: 10.1109/THMS.2016.2634922.
17. Yohan Muliono, Hanry Ham, and Dion Darmawan. Keystroke dynamic classification using machine learning for password authorization. Procedia Computer Science, 135: 564–569, 2018.
18. Andrew Boles and Paul Rad. Voice biometrics: Deep learning-based voiceprint authen-tication system. In 12th System of Systems Engineering Conference (SoSE), pp. 1–6, June 2017.
19. Sarat C Dass and Anil K Jain. Fingerprint-based recognition. Technometrics, 49(3): 262–276, 2007. DOI: 10.1198/004017007000000272.
20. Timo Ahonen, Abdenour Hadid, and Matti Pietika¨inen. Face recognition with local binary patterns. In European Conference on Computer Vision, pp. 469–481. Springer, 2004. DOI: 10.1007/978-3-540-24670-136.
21. Guo-Can Feng, Pong Chi Yuen, and Dao-Qing Dai. Human face recognition using PCA on wavelet subband. Journal of Electronic Imaging, 9(2): 226–234, 2000. DOI: 10.1117/1.482742.

22. Juwei Lu, Konstantinos N Plataniotis, and Anastasios N Venetsanopoulos. Face recognition using LDA-based algorithms. IEEE Transactions on Neural Networks, 14(1): 195–200, 2003. DOI: 10.1109/TNN.2002.806647.
23. Sambit Bakshi, Pankaj K Sa, and Banshidhar Majhi. Phase intensive global pattern for periocular recognition. In Annual IEEE India Conference (INDICON), pp. 1–5. IEEE, 2014. DOI: 10.1109/INDICON.2014.7030362. 189 Person Authentication using ML
24. Christina-Angeliki Toli and Bart Preneel. Provoking security: Spoofing attacks against crypto-biometric systems. In World Congress on Internet Security (WorldCIS), pp. 67–72. IEEE, 2015. DOI: 10.1109/WorldCIS.2015.7359416.
25. Javier Galbally, Sébastien Marcel, and Julian Fierrez. Biometric antispoofing meth-ods: A survey in face recognition. IEEE Access, 2: 1530–1552, 2014. DOI: 10.1109/ACCESS.2014.2381273.
26 Ivana Chingovska, Andre Rabello Dos Anjos, and Sebastien Marcel. Biometrics evaluation under spoofing attacks. IEEE Transactions on Information Forensics and Security, 9(12): 2264–2276, 2014. DOI: 10.1109/TIFS.2014.2349158. 190 IoT Security Paradigms and Applications
27. Abdenour Hadid. Face biometrics under spoofing attacks: Vulnerabilities, countermea-sures, open issues, and research directions. In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition Workshops, pp. 113–118, 2014. DOI: 10.1109/CVPRW.2014.22.
28 Christopher McCool and Se´bastien Marcel. Parts-based face verification using local frequency bands. In International Conference on Biometrics, pp. 259–268. Springer, 2009. DOI: 10.1007/978-3-642-01793-327.
29. Younsung Choi, Youngsook Lee, and Dongho Won. Security improvement on biomet-ric based authentication scheme for wireless sensor networks using fuzzy extraction. International Journal of Distributed Sensor Networks, 12(1):8572410, 2016. DOI: 10.1155/2016/8572410.
30. Eun-Jun Yoon and Cheonshik Kim. Advanced biometric-based user authentication scheme for wireless sensor networks. Sensor Letters, 11(9): 1836–1843, 2013. DOI: 10.1166/sl.2013.3014.
31. Joseph Shelton, Kelvin Bryant, Sheldon Abrams, Lasanio Small, Joshua Adams, Derrick Leflore, Aniesha Alford, Karl Ricanek, and Gerry Dozier. Genetic & evolutionary bio-metric security: Disposable feature extractors for mitigating biometric replay attacks. Procedia Computer Science, 8: 351–360, 2012. DOI: 10.1016/j.procs.2012.01.072.
32. Yahaya Isah Shehu, Anne James, and Vasile Palade. Detecting an alteration in bio-metric fingerprint databases. In Proceedings of the 2nd International Conference on Digital Signal Processing, pp. 6–11. ACM, 2018. DOI: 10.1145/3193025.3193029.
33. Jiankun Hu, Don Gingrich, and Andy Sentosa. A k-nearest neighbor approach for user authentication through biometric keystroke dynamics. In IEEE International Conference on Communications, pp. 1556–1560, May 2008.
34. Daniele Gunetti and Claudia Picardi. Keystroke analysis of free text. ACM Transactions on Information and System Security (TISSEC), 8(3):312–347, 2005. DOI: 10.1145/1085126.1085129.
35 Aini Najwa Azmi, Dewi Nasien, and Fakhrul Syakirin Omar. Biometric signature veri-fication system based on freeman chain code and k-nearest neighbor. Multimedia Tools and Applications, 76(14): 15341–15355, 2017. DOI: 10.1007/s11042-016-3831-2.
36. Sun Yuan Kung, Man-Wai Mak, and Shang-Hung Lin. Biometric Authentication: A Machine Learning Approach. Prentice Hall Professional Technical Reference New York, 2005.
37. Jorge Blasco, Thomas M Chen, Juan Tapiador, and Pedro Peris-Lopez. A survey of wearable biometric recognition systems. ACM Computing Surveys (CSUR), 49(3): 43, 2016. DOI: 10.1145/2968215.
38. Mario Frank, Ralf Biedert, Eugene Ma, Ivan Martinovic, and Dawn Xiaodong Song. Touchalytics: On the applicability of touchscreen input as a behavioral biometric for continuous authentication. IEEE Transactions on Information Forensics and Security, 8: 136–148, 2013. DOI: 10.1109/TIFS.2012.2225048.
39. Jian-Da Wu and Chiung-Tsiung Liu. Finger-vein pattern identification using SVM and neural network technique. Expert Systems with Applications, 38(11): 14284–14289, 2011.
40. Insha Qayoom and Sameena Naaz. Discriminant analysis and naïve Bayes classifier- based biometric identification using finger veins. International Journal of Computer Vision and Image Processing (IJCVIP), 9(4): 15–27, 2019. DOI: 10.4018/IJCVIP.2019100102.
41. Ajay Kumar and David Zhang. Biometric recognition using feature selection and com-bination. In International Conference on Audio-and Video-Based Biometric Person Authentication, pp. 813–822. Springer, 2005. DOI: 10.1007/1152792385.

42. Amioy Kumar, Madasu Hanmandlu, and H. M Gupta. Fuzzy binary decision tree for biometric based personal authentication. Neurocomputing, 99: 87–97, 2013. DOI: 10.1016/j.neucom.2012.06.016. 191 Person Authentication using ML
43. Yong Sheng, Vir V Phoha, and Steven M Rovnyak. A parallel decision tree-based method for user authentication based on keystroke patterns. IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics), 35(4): 826–833, 2005. DOI: 10.1109/TSMCB.2005.846648.
44 Sunmin Lee, Jinah Kim, and Nammee Moon. Random forest and WiFi fingerprint-based indoor location recognition system using smart watch. Human-Centric Computing and Information Sciences, 9(1): 6, 2019. DOI: 10.1186/s13673-019-0168-7.
45. Yan Ma, Bojan Cukic, and Harshinder Singh. A classification approach to multi- biometric score fusion. In International Conference on Audio-and Video-Based Biometric Person Authentication, pp. 484–493. Springer, 2005. DOI: 10.1007/1152792350.
46. Douglas Reynolds. Gaussian mixture models. Encyclopedia of Biometrics: 827–832, 2015. DOI: 10.1007/978-0-38773003-5196.
47. Douglas A Reynolds, Thomas F Quatieri, and Robert B Dunn. Speaker verification using adapted Gaussian mixture models. Digital Signal Processing, 10(1–3): 19–41, 2000. DOI: 10.1006/dspr.1999.0361.
48. Mohamed Soltane, Noureddine Doghmane, and Noureddine Guersi. Face and speech based multi-modal biometric authentication. International Journal of Advanced Science and Technology, 21(6): 41–56, 2010.
49. Girija Chetty and Michael Wagner. Multi-level liveness verification for face- voice biomet-ric authentication. In Biometrics Symposium: Special Session on Research at the Biometric Consortium Conference, pp. 1–6. IEEE, 2006. DOI: 10.1109/BCC.2006.4341615.
50. Yi-Pin Liao and Chih-Ming Hsiao. A novel multi-server remote user authentication scheme using self-certified public keys for mobile clients. Future Generation Computer Systems, 29(3): 886–900, 2013. DOI: 10.1016/j.future.2012.03.017.
51 Yi Liu, Jie Ling, Zhusong Liu, Jian Shen, and Chongzhi Gao. Finger vein secure bio-metric template generation based on deep learning. Soft Computing, 22(7): 2257–2265, 2018. DOI: 10.1007/s00500-017-2487-9.
52. Manmohan Chandraker, Xiang Yu, Eric Lau, and Wong Elsa. Login access control for secure/private data, 2019. US Patent App. 10/289,825.
53. Ilkyu Ha. Security and usability improvement on a digital door lock system based on internet of things. International Journal of Security and Its Applications, 9(8): 45–54, 2015. DOI: 10.14257/ijsia.2015.9.8.05. 192
54. Mrutyunjaya. Sahani, Chiranjiv Nanda, Abhijeet Kumar Sahu, and Biswajeet Pattnaik. Web-based online embedded door access control and home security system based on face recognition. In International Conference on Circuits, Power and Computing Technologies [ICCPCT-2015], pp. 1–6, 2015.
55. Junjue Wang, Brandon Amos, Anupam Das, Padmanabhan Pillai, Norman Sadeh, and Mahadev Satyanarayanan. A scalable and privacy-aware IoT service for live video ana-lytics. In Proceedings of the 8th ACM on Multimedia Systems Conference, pp. 38–49. ACM, 2017. DOI: 10.1145/3083187.3083192.

Cite this article:

Dr G Yashodha, "A conceptual view of biometric usage in IOT", Journal of Multidimensional Research and Review (JMRR), Vol.2, Iss.2, pp.61-75, 2021.