Enhancing security in Internet of Things using authentication techniques: A review survey

Mohit Goyal
Assistant Professor, Dept. of M.C.A., G.L. Bajaj Institute of Technology and Management, Greater Noida

e-mail: mohitims84@gmail.com

Abstract. Internet of Things (IoT) is an interrelation of heterogeneous physical devices over the network. It can assist the people by utilizing the latest technology through machine-to-machine (M2M) communication everywhere throughout the world. In general, IoT is connected with millions of individuals and computers and also provides the services among these with the help of sensors and actuators, etc. Actually, providing security to all users and its supported devices is a daunting task because as technology continues to grow, similarly various types of security threat and challenges are developing. The main objective is to enhance the security in the Internet of Things so that the existing system can be made more reliable as per user perspectives. To make more secure systems, have to use reliable security techniques and latest standards as per present era development since the old security standard is not sufficient for the user which uses the equipment’s according to the latest technology in IoT. So, biometric-based authentication is considered as the solution from preventing the new security threats in the IoT system. In any IoT system, biometric-based authentication can be implemented by using two approaches; one physical-based biometric authentication and another is behavioural-based authentication. In this paper, behavioural-based biometrics is the estimation and recording of personal behaviour patterns and also their utilization to check and validate an individual computer user using some machine learning algorithms to authenticate the IoT devices.

Keywords: Internet of things (IoT), security, privacy, biometric, authentication, and machine learning.

1. INTRODUCTION
The IoT is a collection of inter-connected sensor-enabled devices where all devices/objects are exchanged data and information on the network without human intervention. The development in sensor electronics, wearable technology, and mobile computing/communication devices has brought a phenomenal growth of data in the area of Internet-of-Things (IoT) [1, 2]. In other words, the involvement of the Internet of Things into various applications and fields, for example, smart homes, smart cities, smart health monitoring systems, and industrial control, etc, also shows the fast growth of its usage [1, 2]. Given its greater use in the present, it would not be wrong to say that in the future the counting of its connected devices is expected to increase largely, that approximately which will be between 100 and 200 billion. Because of their inborn dynamic nature, these devices perpetually work
under untrusted ecological conditions and may be in touch with various possibly malicious attacks [2, 3]. IoT security is a more emerging topic in the current scenario. The provision of a secure environment for various connected devices over the network is the main task of IoT security. To make the secure IoT system from a user perspective have to enhance security using authentication techniques is the main aim. Authentication is the technique to identify the users and various connected devices on the network so that only the authenticated users and non-manipulated devices can access the IoT system. In general, various authentication techniques exist for example, knowledge-based, possession-based, and biometric-based authentication. Biometric authentication is sub-classified into two categories: physiologic and behavioral [6,8,9]. In behavioral-based biometric authentication, many approaches are used to identify the users.

Nowadays, the smart phone is considered one of the most important IoT devices because it plays a large role to communicate with other connected devices over the network. In other words, you can say that various other IoT devices can be effectively handled by installing the required app on a smart phone [13]. The dependence on Smartphone’s / IoT devices is increasing day by day so as a result security threats are also increasing [1, 8]. The data received from Smartphone users can be related as an input to the gait model which shows the user’s walking style as well as their physical attributes which are used for access any IoT device [11]. IoT device (smart phone) has various sensors and small computer processors that work on the data gathered by the sensors with the help of machine learning for performing the desired task. Machine learning is a variant of artificial intelligence that assists computers in learning without being programmed by someone [10, 16]. Here in this paper, the author will present the existing technologies of the present system and discover the remaining essentialities to make secure the IoT and based on these needs present the structure of those authentication techniques that can be used to make more reliable the IoT system.

The rest of this paper is arranged out as follows: Section 2 describes the security challenges threats can affect on security of IoT device time to time. Section 3 represents the various methods which are used in IoT authentication for enhancing reliability. Section 4 specifies the proposed approach for gait-based authentication. Section 5 discuss the conclusion and also mention few upcoming challenges of this paper.

2. SECURITY CHALLENGES AND THREATS IN IOT

As all know very well in the coming year many more IoT devices will be connected with the network. At that time security and privacy will become two mandatory factors for working in any commercial environment. To provide a safe environment for any commercial organization in the future, have to focus on current security threats and challenges, so that can study future security threats and challenges. IoT security is considered very weak because available standards are not as per Industry. Although many security frameworks are available, yet no single standard on which agreed by all. Due to a lack of accepted single standards [7], large industries have their own special standard. The use of a weak password is the most important issue which leads to security breaches in the IoT system [1,2,5]. Although the password is can be changed from time to time, they are not much efficient in controlling IoT security.

3. METHODS FOR AUTHENTICATION

The user authentication method demonstrates the whole procedure where a user, who politely urges his perspective to the system so that verified himself as a user after checking his own identity or authority or capability with which itself can retrieve any information in the system easily whenever required. The whole authentication procedure is made of 1) identification proof that a user claims as his identity, 2) confirmation through an authentication server to proof that user who urges get to is permitted, and 3) an access control mechanism-based authority in which the server permits the user to utilize the system assets [8]. Especially, the authentication process is a compulsory requirement to allow a user to get services delivered by the service provider. In general, authentication techniques are categorized into three major kinds. They are: 1. Memory-based authentication 2. Object - based authentication 3. Identity - based authentication.
3.1 Memory-based authentication

Memory-based authentication is also known as knowledge-based authentication. In this type of authentication, you have to remember parts of information that you know as passwords and PINs, etc. In general, sometimes the user experiences difficulty remembering random and strong passwords. Due to this, the user uses a short and simple password which becomes very easy to guess. Therefore, it becomes unable to provide high authentication to any system, that's why it does not be considered good for a security point of view [12].

3.2 Object-based authentication

Object-based authentication is also known as possession-based authentication. In this type of authentication, the user holds token, etc. to authenticate the system or any device. The Object-based authentication method is more advantageous than memory-based authentication because the user does not need to remember anything. During the authentication process, the presence of the token is mandatory, which become sometimes a disadvantage because the token can be missed or somebody can take, due to this an attacker can use it for authentic access [8, 10].

3.3 Identity-based authentication

Identity based-authentication is also known as biometric-based authentication. In this type of authentication, users can be authenticated with the concept of “something you are” and “something you do” [3, 4,5]. The identity-based authentication method is divided into sub-categories on the basis of its usage or technique. These are: physical -based biometric authentication and behaviour-based biometric authentication techniques that depend on the user's physicality (e.g., fingerprints, facial features) or specificity of behaviour (e.g., handwriting, gait, etc.) as you can see in given figure 1[14 ,17].

![Figure 1. Various types of Identity based authentication](image)

Biometric-based authentication has several advantages compared to other authentication methods. Some of these are given below:

- The user does not need to remember or take anything.
- Authentication of the user is done at the place where the biometric device/sensor is located [9].

The above statements show that biometric techniques seem to be an extremely beneficial technique of authentication available. These days, because it has integrated the capacities of sensors and mobile applications side by side collected. Behaviour-based biometric authentication encompasses various technologies to implement authentication, for example, signature, gait, etc. [11]. But the Gait technique has been considered an important technique for user authentication. Nowadays various IoT device is available in the market but by seeing the majority of user’s opinion, the smart phone has
been considered one of the most suitable and popular IoT devices because smart phone can provide the support to various others device by installing required applications, for example, you can control your home AC by installing a required application on your smart phone [13]. Now, will look at how can provide authentication to the smart phone or any related IoT device. Nowadays, Technology will be changing day to day basis. So, before applying authentication on any IoT device (for example, smart phone) will mention the technological changes. The three main technology changes are noticeable in the context of smart phone (IoT devices) security [11, 13]. These are given: a. Mobility b. Sensor c. Constant connectivity.

3.3.1 Mobility

Mobility generates uncertainty regarding the ecological conditions around smart phones. The device can be accessed either in a safe environment or a public environment, so the diversity in surroundings creates a chance to attacks a mobile device.

3.3.2 Sensors

A sensor is can be a device or any machine whose aim is to explore the events or changes that happen in its surrounding environment and also send the information to another electronic device, generally a computer processor. Accelerometers, gyroscopes are the two most important sensors found in modern smart phones [13]. The accelerometer sensor is the most used sensor, which is capable to record the variation in acceleration according to time. The smart phone uses the built-in tri-axial accelerometer sensor to measures the proper acceleration. Nowadays, wearable devices use only those accelerometer sensors which are made by a single silicon chip along with an integrated electronic circuit. These silicon chips are used in the Micro-Electro-Mechanical-Systems category and are very micro, as like a match tip. Second, the Gyroscope sensor is non-pivoting sensors which essentially utilize the Coriolis Effect on a mass to distinguish inertial angular rotation. The gyro sensors have been utilized in physical action identification or in body pose analysis [11].

3.3.3 Constant connectivity

Constant connectivity means to establish constant access in between the various devices through the network.

4. PROPOSED APPROACH FOR GAIT BASED AUTHENTICATION

A new behavioral-based biometric authentication technique which is used to authenticate the user is known as Gait biometric. The main objective of Gait biometric is to recognize and verify the users on the basis of their own walking style, for example, how an individual goes ahead in a general or fast walk. As per the above discussion, the smart phone is known as the most popular IoT device, so, here will discuss only how to authenticate to smart phone (IoT device) Gait based authentication has three techniques to implement biometric based authentication [19,20]. These are: a. Machine vision-based b. Floor sensor-based c. Wearable Sensor based.

![Figure 2. Gait authentication techniques](image)
The various gait authentication techniques with different sensors are used for behavioral-based authentication. As shown in figure 2 these approaches can be used to implement gait-based authentication. But the first two techniques cannot implement to on the smart phone, here wearable accelerometer sensor techniques or approach is used for implementing gait-based authentication in IoT devices (for example: smart phone), because this approach does not require too much additional equipment, like floor sensor technology, etc. Wearable sensors-based approach is those approach in which sensors are closely attached to the human body to collect various types of information either directly or indirectly. The sensors can be kept any place on the human body, for example, belt, jeans pockets, hand, and waist, etc. Generally, a user prefers to keep a smart phone in a trouser pocket, so that the sensor can collect all related information. The various important types of sensors are required to collect the information effectively, such as gyroscope, accelerometer, and speed sensors, etc. Here, the proposed method for implementing the behavioral-based biometric authentication system is used 'Gait based technique and machine learning algorithm'. By applying both concepts, the existing system becomes more reliable. Machine learning is an application of artificial intelligence that confer system the capability to learn automatically and better from past experience without giving training to the computer program explicitly. The main aim of machine learning is the development of computer programs so that can learn and access the data without human intervention and which also capable to make forecasting from the data. The main steps required to implement the proposed ‘Gait based authentication approach’ are given below:

4.1 Collection of gait- based data
4.2 Data pre-processing
4.3 Data extraction
4.4 Selection of features
4.5 Classification

4.1 Collection of gait- based data

To implement a proposed authentication approach data must be collected effectively in a well-defined format. With the help of various sensors, we can obtain gait-based data, for example, GPS, gyroscope, and accelerometer sensor. Gait based data can vary according to device mode or motion mode. A device mode means where the device is kept. For example, generally, the smart phone device can be kept either in hand or in the pocket. A motion mode means the user's position while holding the device. For example, a user's motion mode could be either standing still or walking/running [15]. At the time of collection of gait data, these factors must be taken under consideration.

4.2 Data per-processing

It is the procedure of taking out an object (human) shadow from back surroundings. By which we can calculate our gait-related calculation in a simple way. After that we separate an individual shadow which is main objective of this step.

4.3 Data Extraction

Extraction means a reduction in data size. A gait sequence has many gait cycles. The gait cycle is a recurring pattern consisting of steps and stride. A step means one single step walk. A stride denotes a whole gait cycle. So, a one gait cycle has all essential gait-related features. Now extraction is required to find a unique gait style. Gait based data can be extracted by applying various machine learning algorithms (like KNN, SVM, etc.) for the purpose of storing unique gait data.

4.4 Selection of feature

The main aim is to select the most important features because a large number of features make a model bulky and time taking process and so the model becomes difficult to implement. The selection of feature basically used to choose the best appropriate model to make a classification. By discarding the non-related feature, the data size is decreased, so that the execution time of the model can be reduced. Now, it can help to upgrade the performance of the system by decreasing the various errors. To apply the classification algorithm, it selects a part of the extracted data or features. It is also known as variable selection or attributes selection. There are various ways in which can select the feature, but according to their importance the feature selection methods are divided into three main types, which are listed below:

- Filter based feature selection method
• Wrapper-based feature selection method
• Embedded feature selection method

These methods used such algorithms that have the predefined methods for feature selection. For example, Lasso and RF have their personal feature selection methods.

4.5 Classification

Classification is the procedure of estimating a given mapping function to map the input variable to the output variable. In standard terminology, this mapping function is called the model that forecasts the class for the available sets of data. If the input variables are real-valued or discrete, then a classifier can categorize the given data values into one or more classes. For solving the classification problem used various types of supervised machine learning algorithms like KNN, and SVM, etc. [16,18]. In various classification algorithm to find best from the others is not easy because it depends on its application and nature of its available data. Some machine learning algorithms which is used in classification are given below:

4.5.1 K-Nearest Neighbor (KNN)

K-Nearest Neighbor is an example of a lazy learning algorithm that stores all objects and also trained these objects in n-dimensional space according to training data points. Whenever an unnamed discrete data is achieved then it analysis the nearest k number of objects stored and returns the widely recognized class as the forecast for actual esteemed data, it also returns the mean of k closest neighbors.

4.5.2 Logistic Regression

Logistic regression is an example of a supervised learning-based classification algorithm that is utilized to forecast the probability of a target variable. The tendency of the dependent and target variable is dual, that meaning is there will be just two feasible classes. In general terms, the target variable is the nature of binary in which data can be represented into two forms either yes (symbolic code is 1) or no (symbolic code is 0). In mathematical terms, it forecast P(Y=1) as a probability function of X.

4.5.3 Support vector machines (SVM)

Support vector machines (SVMs) are effective yet softly supervised machine learning algorithms that are utilized both for classification and regression. In general, these are utilized for classification related problems. SVM has an uncommon method of implementation as compared to other methods of the machine learning algorithm. Slowly, it becomes most popular due to its capability to tackle many categorical variables and multiple continuous variables. A SVM model is essentially a portrayal of various classes in a hyper plane in multidimensional space. The hyper plane would be produced in an iterative method for the purpose of minimizing the error. The objective of it is to partition the given dataset into class to search the maximum marginal hyper plane. The important approaches of SVM are given below:

4.5.3.1. Hyperplane

It is a decision plane and place (space) which is partitioned into a various group of objects having a number of classes.

4.5.3.2. Support vector

Data points that are nearest to the hyperplane are known as support vector. With the help of these data points, the splitting line will be explained.

4.5.3.3. Margin

It can be explained as the blank space between two lines of the closest data points of various classes. A good margin means a large margin but a bad margin is just adverse of good margin, as its name indicates. It means a small margin is known as a bed margin.
5. CONCLUSION AND FUTURE CHALLENGES

As the growth of someone technology increases then, as usual, the problem is increased on usage of these techniques just like happened in IoT. Slowly many new security threats were introduced in IoT along with their increased usage. So, considering various researcher put attention towards how they can make IoT network make more reliable. In this paper, the researcher presented behavioral-based authentication techniques to increase the reliability in IoT from the user perspective. Here, Gait-based authentication is considered the main technique for biometric based authentication. It is highly sufficient to provide security without giving any more difficulty to the use.

Now as future challenges, generally talk about likely answers for some issues that must be overcome to make easy the utilization of behavioral-based biometrics.

5.1 Here, Android based smart phone is assumed by considering as most important IoT device to implement gait-based authentication due to its popularity in market, so generally proposed approached support only for android-based phone. This proposed approach cannot be support mobile platforms like window based mobile or iOs based mobile. In this way, to secure all mobile device users or expanding the proposed gait-based authentication mechanism, this approach should be applied on other platforms also.

5.2 In general, in this paper, the main focus is to develop gait- based authentication techniques, but along with should also gave attention towards proper utilization of resources, like, usage of processor, battery and memory, etc. Actually, as a researcher gave no attention towards this.

The future researchers can also mix two or more authentication techniques to provide easiness to the user

REFERENCES
[1] Suoa H, Wan J, Zoua C, and Liu J. (2012). Security in the Internet of Things: A Review. In international conference on Computer Science and Electronics Engineering, (648-651).
[2] Patel K K, & Patel M S. (2016). Internet of Things- IoT: Definition, Characteristics Architecture, Enabling Technologies, Application & Future Challenges. In International Journal of Engineering Science and computing. (6122-6133).
[3] Iqbal M A, Olaleye G O and Bayouni M A. (2016). A Review on Internet of Things (Iot): Security and Privacy Requirements and the Solution Approaches. In global journal of computer science and technology. (1-11).
[4] Porras J, Päkkäläinen J, Knutas A.(2018). Security in The Internet of Things – A Systematic Mapping Study. In Proceedings of the 51st Hawaii International Conference on System Sciences.
[5] Noor M B M, Hassan W H. (2018). Current research on Internet of Things (IoT) security: A survey. Article in computer network in Elsevier (283-294)
[6] Prabhakar S, Pankanti S, and Jain A K. (2003). Biometric recognition: Security and privacy Concerns.” In IEEE Security & Privacy Magazine. (33-42).
[7] Mahadi A N, Mohamad A M , Mohamad, I A, Mokhairi M, Kadir A F M, and Mamat M. (2018). A Survey of Machine Learning Techniques for Behavioral-Based Biometric User Authentication. In book Recent Advances in Cryptography and Network Security,Intech Open. (42-59).
[8] Vongsingthong S, and Boonkrong S. (2015). A survey on smartphone authentication. In Walailak Journal of Science and Technology. (1-19).
[9] Sahu S B, and Singh A. (2014). Survey on various techniques of user authentication and
graphical password. In International Journal of Computer Trends and Technology (IJCTT).

[19] Khaddar E, Boulmalf M, Smartphone: The Ultimate IoT and IoE Device.(137-162).
[20] Abdulaziz A and Kalita J, (2019). Authentication of Smartphone Users Using Behavioral Biometrics. (1-32).
[21] Janabi M, (2017). Human Gait identification System. (1574-1594).
[22] Xiao L, Lu X, Zhang Y, Wu D, (2018). IoT security techniques Based on Machine Learning. (1-21).
[23] Babich A, (2012). Biometric authentication Types of Biometric Identifiers. In HAAGA – HELIA University, as Bachelor’s Thesis Degree Programme. (1-56).
[24] Hussain,F, Hussain,R, Hassan A S and Hossain E (2019).Machine Learning in IoT Security:
[25] Current Solutions and Future Challenges. Article In arXiv.org. (1-24).
[26] Kececi A, Yildirak A, Ozyazici K, Ayluctarhan G, Agbulut O and Zincir I.(2020).
[27] Implementation of machine learning algorithms for gait recognition. In International Journal Engineering Science & Technology. (1-7).
[28] Hoang T, Choi D, and Nguyen T. (2015). Gait authentication on mobile phone using biometric cryptosystem and fuzzy commitment scheme. International Journal of Information Security (549–560).