A Survey on Remote IoT User Authentication Systems

Hima Mohan[1], Professor Usha Gopalakrishnan[2]

[1]P G Scholar, Department of CSE, Musaliar College of Engineering & Technology, Pathanamthitta, Kerala, India
[2]Associate Professor, Department of CSE, Musaliar College of Engineering & Technology, Pathanamthitta, Kerala, India,

---***---

Abstract - *Authenticating users and devices in IoT (Internet of Things) - based systems is a major challenge where standard authentication methods such as login-password can no longer be enabled. Remote user authentication is a process in which a user's legitimacy over an insecure communication channel is checked by the remote server. Authentication is a security mechanism designed to ensure that a network, site or service can be linked to only approved devices. The technique is also known as authentication of computers. Two-factor authentication can be provided by authenticating both the user and the device. The most popular form of authentication is passwords. The significant part of stable IoT systems is mutual authentication between IoT devices and IoT servers. Single password-based authentication mechanisms are susceptible to side-channel and dictionary attacks and are commonly used. Password-based authentication, multi-factor authentication, certificate-based authentication, biometric authentication, token-based authentication are some common authentication methods used to secure modern systems. The aim of this paper is to give overview and comparison of remote IoT user authentication techniques for young learners and researchers.*

***Key Words*:** **RFID, LiSA-G, Gait Recognition, Accelerometer**

1. INTRODUCTION

The IoT is an evolving technology that focuses on interconnecting things or devices with each other and with people or users in order to achieve some common goals. Many current technologies, such as wireless sensor and actuator networks (WSAN) and radio frequency identification (RFID) are operated by IoT. The definition of the Internet of Things was conceived by Kevin Ashton of Auto ID-Center MIT [16]. Many researchers around the world are using their efforts to tackle different IoT security issues. In communication and information strategies, the IoT is the most common field at present. It is still a challenge, however, to develop a safe and secure authentication scheme for IoT-based architectures. A lightweight IoT-based authentication scheme is proposed and an IoT-based authentication scheme is proposed that can resist different types of attacks and realize key security features such as user audit, shared authentication, and security of sessions. The idea of the IoT has become a hot topic for research, with the rapid advancement of computer science and network technology. This definition was introduced by Ashton in 1991. Several sensors in the IoT have the ability to collect data and communicate with each other or to provide human beings with data through the Internet. In smart power grids, smart houses and other areas, technology can also be widely used. Sensors monitor electrical energy usage and time-of-use rates for power stations within a smart grid. Then, the stations can maximize the supply of electricity. To improve navigation, sensors track traffic in an intelligent transportation system. Users can remotely manage, track, and access objects inside the smart home. Although IoT is close to our lives, due to the wireless nature of the communication channel [12], it suffers from security challenges. To defend against these IoT security threats, authentication is important. Authentication ensures that the messages the recipient receives come from the sender of a legal document. This acts as the first line of defence against potential assailants. The main requirement for IoT is authentication [14]. Because of the limited resources of most IoT devices, conventional asymmetric encryptions do not support IoT devices, giving rise to lightweight authentication schemes. There is a very particular pattern in the human gait which can be used for recognition and verification. Traditional wearable sensor-based gait recognition gains gait data by bundling dedicated sensors into the fixed portion of the human body [17]. With the rapid popularization of smartphones and the continuous improvement of their functions in recent years, it has become possible for users to use the built-in smartphone accelerometer for gait detection in circumstances that do not affect the usual work, study and life of users [5]. Factors such as the variety of smartphones and very large performance discrepancies of the built-in accelerometers, however, contribute to major differences in the data obtained, raising the complexity of recognizing individuals and directly impacting the accuracy and credibility of the identification. The two key Fields are authentication and access control security problems that need to be addressed to secure information computing infrastructure and computer systems against unauthorized access. Authentication has become more critical for an entity to have an effective and reliable means of authentication due to recent incidents of fraud and terrorism. An example of the security interface used by electronic commerce (e-commerce) websites is the authentication interface [18]. This paper explores five different methods of remote user authentication in IoT, technologies used and their advantages and disadvantages.

2. METHODS FOR REMOTE USER AUTHENTICATION IN IoT

2.1 Authentication of Remote IoT users based on Deeper Gait analysis of sensor data

This method implements a user authentication system based on specific walking patterns [1] for remote IoT users to extract gait-related features [9]. The method suggested applies to a wide variety of IoT devices, such as Cell phones, wearable sensors and smart watches. Deeper gait analysis with the least number of features and data for authentication purposes are the key contributions of this technique. The user need not authenticate with the userid and password to get any data through IoT. Instead, they can use the gait movement directly to authenticate. We have a server, we used to take data from the server. But we must be legal users. The gait movement can be used to authenticate the user without giving userid and password. On the receiver side they can monitor if it is an authorized user or not. If they are an unauthorized user, they will block the data. There is a hub, data source and at a time five users are allowed. They usually give a userid and password for authenticated users. All the activity related information stored in the server. When someone is waiting to authenticate, their activities will match with the template, which is already stored in the server. If the system says OK to the individual waiting for his activities to be authenticated, he is an authorized person; otherwise he is an unauthorized person.

2.2 Securing IoT based RFID systems: A Robust Authentication protocol using Symmetric Cryptography

The RFID (Radio Frequency Identification) system is another technology used for authentication instead of identifying activities. There is a small tag in RFID, which can be used to store the information. While reading the tag information using RFID reader we can identify whether it is authorized or unauthorized. Different people use different RFID tags. When the authentication key shows the RFID tag, it reads the information coming from the RFID [6][4] and compares it with the already existing dataset. In the database if that particular information containing the person is available then we can say that it is authenticated, otherwise it is not authenticated. There is no need of sensors and identifying movements, just one tag is required.

2.3 Lightweight Seamless Authentication based on Gait in wearable IoT Systems

It is based on single activity focus only on walking. Gait, which is the pattern of limb movements during locomotion, achieved through the movements of human limbs. A lightweight gait-based seamless authentication system (LiSA-G)[2] that can authenticate and identify users on commercial smart watches that are widely available. Unlike existing works, extracts not only the statistical characteristics but also the human action-related characteristics from the collected sensor. In the traditional authentication method, by typing a password or presenting biometric tests, a user needs to authenticate himself. In other words, direct user interaction is required by the current authentication scheme, which can impede seamless authentication. However, we can authenticate users without requiring their direct or active involvement when activated to automatically analyse user sensor data collected in real-time via wearable IoT devices [7]. We propose a gait-based authentication system for wearable IoT devices to authenticate users [8] automatically by analyzing their sensor data to strive for such seamless authentication. The workflow of our frame work consists mainly of three steps:

(1) Collection of information
(2) Pre-processing of data
(3) Authentication

A customer-side LiSA-G G in the data collection phase, implemented in the smart watch, it collects and transmits to the server the sensor data stream. Then, the data pre-processing is run by a server-side LiSA-G that removes undesirable glitches and noises in the data stream received and obtains a consistent data sampling rate by applying linear interpolation. The server-side LiSA-G extracts not only statistical characteristics (e.g. mean, standard deviation) but also physical characteristics in the authentication stage such as arm movement features (e.g., pitch, yaw, and roll) from the details. Then, the server-side LiSA-G authenticates users via machine learning techniques, based on the extracted features.

2.4 Gait Recognition of Acceleration Sensor for Smart Phone Based on multiple classifier Fusion

A recognition approach based on multiple classifier fusion (MCF) [3] is suggested on the basis of the Smartphone accelerometer. In order to obtain the final classification results, Multiple Scale Voting (MSV) is proposed to combine the results of multiple classifiers. Noise or unwanted signals can be removed in the data acquisition and pre-processing section. Period can be divided in to two groups, one based on gait feature related to activities and other based on motion feature related to movements. Then it is passed on to two or three classifiers. These classifier outputs can be combined using fusion algorithm [13] as shown in Fig 1. If any one of the classifiers is negative we will get different output. For three classifiers, if the output of the two classifier is same then that output can be taken as the final output. Hence misclassification rate can be reduced. If we use a single classifier, it depends only on that single classifier. But if we use a multiple classifiers sometimes, one or two classifiers will perform better. So will get better classification accuracy.

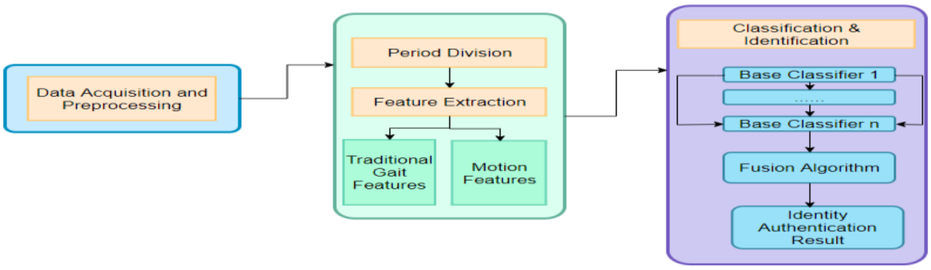
Data Acquisition and Preprocessing
Period Division
Feature Extraction
Traditional Gait Features
Motion Features
Classification & Identification
Base Classifier 1
......
Base Classifier n
Fusion Algorithm
Identity Authentication Result

Figure 1: Fusion Algorithm for Multiple Classifier Recognition.

2.5 Unobtrusive User-Authentication on Mobile Phones using Biometric Gait Recognition

Such an unobtrusive authentication mechanism [10] is biometric gait recognition [15] based on accelerometer data [11]. Based on his gait data, the phone can recognize him when the phone owner is walking, so that when the data is collected with a commercially accessible mobile system containing low-grade accelerometer [19], he can use the phone directly without any further authentication. To collect gait data, the mobile device was positioned on each volunteer at the hip.

3. COMAPRISON

Verifying the identity of someone who wants to access data, services, or applications is known as authentication. Validating the identity builds a foundation of confidence for future interactions. Authentication also facilitates transparency by allowing access and behavior to be linked to individual identities. The features and technologies used in the authentication methods are shown in Table 1.

Table 1: Features and Technologies used in Authentication Methods

Authentication Methods	Technology Used	Features Based on the Feature Extraction
1. Authentication of Remote IoT users based on Deeper Gait analysisof sensor data	Single Classifier	Median, Mean, Skew, Kurtosis

2. Securing IoT based RFID systems: A Robust Authentication protocol using Symmetric Cryptography	Radio Frequency Identification	RFID tag
3. Lightweight Seamless Authentication based on Gait in wearable IoT Systems	Using Gait, Locomotion achieved through the movement of human limbs	Mean, Standard Deviation, Skew, Kurtosis, Correlation, Roll, Pitch, Yaw, Force
4. Gait Recognition of Acceleration Sensor for Smart Phone Based on multiple classifier Fusion	Multiple Classifier Fusion Algorithm	Average, Standard Deviation, Mean Variation, Peak Interval, Energy, Zero crossing, Skewness, Kurtosis, Root mean square, DFT coefficient, DCT coefficient

The advantage and disadvantage of different authentication methods are shown in Table 2.

Table 2: Advantages and Disadvantages used in Authentication Methods

No	Authentication Methods	Advantages	Disadvantages
1.	Authentication of Remote IoT users based on Deeper Gait analysis of sensor data	▪ Robust authentication between user and device ▪ Unpredictable authentication ▪ Simple design	▪ It is not suitable for more users ▪ Imprint is the unique, difficult to change
2.	Securing IoT based RFID systems: A Robust Authentication protocol using Symmetric Cryptography	▪ RFID is the lightweight device to authenticate ▪ Symmetric key is used	▪ Loss of card leading insecure ▪ Possibility of loss of information inside the RFID tag
3.	Lightweight Seamless Authentication based on Gait in wearable IoT Systems	▪ No need of physical contact ▪ User can use in their pockets ▪ Computation complexity low	▪ Sensor fault still exist ▪ Heavy gait movements leads to misclassification of users

4.	Gait Recognition of Acceleration Sensor for Smart Phone Based on multiple classifier Fusion	▪ Multiclassifier increase the authentication accuracy ▪ Gait and Motion feature included	▪ Multifeature and fusion increase the computation time delay in the processing.
5.	Unobtrusive User-Authentication on Mobile Phones using Biometric Gait Recognition	▪ Enables Unobtrusive user authentication. ▪ User friendly.	▪ Difficult for an attacker to initiate another person.

4. CONCLUSIONS

Remote IoT user authentication system plays a vital role in IoT. In this paper a few remote authentication methods, comparison, advantages, disadvantages were discussed.

REFERENCES

[1] H.Donggu, "Human Gait Recognition and Application Based on Smart-Phone", Research Institute of Electronic Science and Technology, 2018.

[2] Wu, F. Xu, Kumari.S, Li, X, Das, A.K., Shen.J, "A lightweight and anonymous RFID tag authentication protocol with cloud assistance for e-healthcare applications", J. Ambient Intel. Humanized Comput. Vol. 9, pp. 919–930, 2018.

[3] K.Wang, "Application and Research of Multiple Classifier Fusion Algorithm in Activity Recognition", Xi'an university of Posts & Telecommunications, 2017.

[4] Peris-Lopez.P. Hernandez-Castro.J.C., Estevez-Tapiador.J.M, Ribagorda.A, "Lightweight cryptography for low-cost RFID tags In Security in RFID and Sensor Networks", CRC Press: London, UK, pp. 121–150, 2016.

[5] M. Muaaz and R. Mayrhofer, "Accelerometer based gait recognition using adapted gaussian mixture models," in Proceedings of the 14th International Conference on Advances in Mobile Computing and Multi Media, pp. 288–291, ACM, New York, NY,USA, 2016.

[6] Gope.P, Hwang.T, "A realistic lightweight authentication protocol preserving strong anonymity for securing RFID system", Comput. Secur. Vol. 55, pp. 271–280, 2015.

[7] H.Yoon, S.Park, and K.Lee, "Exploiting ambient light sensor for authentication on wearable devices", in 2015 Fourth International Conference on Cyber Security, Cyber Warfare and Digital Forensic (CyberSec), pp. 95–100, Oct 2015.

[8] Gope.P, Hwang.T, "A realistic lightweight authentication protocol preserving strong anonymity for securing RFID system", Comput. Secur. Vol. 55, pp. 271–280, 2015.

[9] B.Sun, Y.Wang and J.Banda, "Gait characteristic analysis and identification based on the iPhone's accelerometer and gyrometer", Sensors, Vol. 14, No. 9, pp. 17037–17054, 2014.

[10] H. Lu, J. Huang, T. Saha, and L. Nachman, "Unobtrusive gait verification for mobile phones," in Proceedings of the 2014 ACM International Symposium on Wearable Computers, pp. 91 –98, ACM, New York, NY, USA, 2014.

[11] A.Bayat, M.Pomplun and D.A.Tran, "A study on human activity recognition using accelerometer data from smartphones", Procedia Computer Science, Vol. 34, pp. 450–457, 2014.

[12] Jing.Q, Vasilakos.A.V, Wan.J, "Security of the Internet of Things: Perspectives and challenges", Wirel. Netw, Vol. 20, pp. 2481–2507, 2014.

[13] L.Huang, J.Tang, D.Sun and B.Luo, "Feature selection algorithm based on multi-label Relief", Journal of Computer Applications, Vol. 32, No. 10, pp. 2888–2898, 2012.

[14] Atzori.L, Iera.A, Morabito.G, "The Internet of Things: A survey", Comput. Netw. Vol. 54, 2787–2805, 2010.

[15] D.Gafurov, "Performance and security analysis of gait-based user authentication", Ph.D. dissertation, Faculty of Mathematics and Natural Sciences, University of Oslo, 2008.

[16] K.Ashton, "That 'Internet of Things' thing", RFID Journal. [Online] June 2009. Available: http://www.rfidjournal.com/article/view/4986.

[17] L.Rong, Z.Jianzhong, L.Ming et al., "A wearable acceleration sensor system for gait recognition", in Proceedings of the IEEE Conference on Industrial Electronics & Applications, pp. 2654–2659, IEEE, May 2007.

[18] Halpert.B.J, "Authentication Interface Evaluation and Design for Mobile Devices", 2005.

[19] J.Mantyj arvi, M.Lindholm, E.Vildjiounaite, S.M.Makel and H.Ailisto, "Identifying users of portable devices from gait pattern with accelerometers", IEEE International Conference on Acoustics, Speech and Signal Processing, Vol. 2, pp. ii/973 – ii/976, 2005.

BIOGRAPHIES

HIMA MOHAN is doing M Tech at Musaliar College of Engineering and Technology, Pathanamthitta, Kerala, India. She has received B Tech degree in Computer Science and Engineering from *Kerala University*, Thiruvananthapuram, Kerala.

USHA GOPALAKRISHNAN is working as an Associate Professor at Musaliar College of Engineering and Technology, Pathanamthitta, Kerala, INDIA. She has received M Tech Degree from Kerala University and B Tech Degree from Cochin University of Science and Technology.