Design a Novel User based Authentication System that Identify by User and Device

B. Bamleshwar Rao
Research Scholar
AKS University, Satna, M.P

Akhilesh A. Waoo, PhD
Associate Professor
AKS University, Satna, M.P

ABSTRACT
Smart City is promising to improve working environments in terms of quality, competitiveness and amenities. However, new data security problems emerge as a result of the evolving capabilities of Smart Cities. One of the main problems is the use of continuous and non-invasive authentication techniques, since conventional authentication approaches have major limitations. Thus, to overcome these shortcomings, the key contribution of this paper is the design and implementation of a continuous and intelligent authentication architecture for Smart City in the IOT environment. The architecture is cloud computing focused and users are authenticated by machine learning approaches based on the behaviours. To design a modern user-based authentication method, where user and device recognition.

Keywords
Authentication, classification approach, identify by user and device, Internet of Things (IoT).

1. INTRODUCTION
Data security is very critical for the Internet of Things (IoT) framework. One of the key security concerns is the correct and secure identification and authentication of users in an IoT environment. This paper suggests a cluster-based Identity and Authentication Architecture for the IoT platform. The contribution of this research work involves a dynamically configurable system architecture capable of ensuring the identification and authentication of all connected devices on the IoT network, regardless of their type; Place and a number of criteria. The proposed mechanism guarantees a central security to each cluster-based IoT service, which is locally or in the cloud, through the recognition and authentication of intelligent objects. This cluster-based method makes our system more stable and flexible, enabling small-scale and ensemble devices Eventually, it guarantees continuous safe contact with all established and approved members of the cluster and also continuously prevents all unauthorised members from causing any disruption. Finally, we conducted a comparative study of the efficiency and feasibility of the proposed method, representing the various important strengths of the job.

The rest of the article is organised as follows: Section 2 provides a brief description of the related work. Section 3 includes a comprehensive overview of the device authentication of IntelliAuth. Section 4 discusses the approach used in this study work for the identification of events and user authentication. A detailed analysis of the findings is presented and discussed in Section 5. Section 6 concludes the results of the study.

2. RELATED WORK
Kaburu, D.M. et al[1] The cognitive solution suggested integrates the usability consistency attribute for the primary activities of users in the system by applying cognitive psychology outcomes. The methodology helps the designer to consider the effect of a specific re-authentication process on user success and satisfaction in a continuous user authentication context.

Nixon K.W et al[2] User feedback patterns are obtained by embedded sensors on an Android smartphone. A learning algorithm is programmed to uniquely identify the user during their regular interaction with the system while embracing hardware and biometric capabilities that are continuously evolving. Our experimental findings reveal a great potential for our gesture-based protection scheme to achieve adequate recognition precision with an undetectable effect on user experience.

Sales, T. et al.[3] As a result, control points, devices operating as clients on behalf of the customer, and UPnP devices can not communicate on the basis of user knowledge. This paper proposes an expansion of the UPnP standard called UPnP-UP that enables user authentication and authorization mechanisms for UPnP devices and applications. These frameworks provide the basis for creating personalised and stable UPnP services around the board, retaining backward compatibility with previous iterations of UPnP.

Xue Q et al[4] This paper contains an analysis on the This paper analyses the current image of inter-device user identity authentication in the IoT and suggests an inter-device biometric authentication approach for the IoT that is intended to work with larger devices to resolve the limitations of conventional user identity authentication solutions, including security and reliability concerns. A plan for more optimization of solutions is also included. This paper elaborates on the basic method of user identity verification conducted by users on devices and within devices making use of fingerprints. We will illustrate the protection of this solution against current attack methods and, in the last section, we will list numerous potential implementations of this solution in smart homes.

Rajawat A.S et al[5] This research paper focuses on designing an algorithm to avoid and diagnose uncertainties in these applications. The developed algorithm is based on a deep learning model, a consolidated method used to forecast ambiguity in mobile computing. The challenge of estimating this uncertainty calculation is to learn both the target output and the associated variance. A comparable approximation is then rendered in a newly developed outcome model comprising one network for goal performance and another for variance. This technique avoids error from happening at a higher percentage than other usable algorithms.

S. Dong et al[6] The findings of the experiment demonstrate

that the use of CPU graphs for our proposed comparative mechanism will achieve a high degree of uniqueness and stability of the extracted fingerprint relative to other fingerprint techniques. We are also developing a concept model based on the fingerprint device and the biological features to solve the drift problem.

Q. Wang et al., et al[7] Create a novel pop-noise identification scheme to distinguish pop-noises at the phonemic level, on the basis of which we develop a special relationship between phonemes and pop-noises to distinguish legitimate users and to protect against spoofing attacks. Our experimental findings with 18 participants and three forms of smartphones indicate that VoicePop achieves more than 93.5 percent detection accuracy at about 5.4 percent equivalent error rate. VoicePop needs no extra hardware, but rather built-in microphones in nearly all smartphones that can be quickly incorporated with current voice authentication systems for mobile devices.

3. AUTHENTICATION APPROACH

In this classification, the most applicable to the nature of this work, two solutions have been described in the literature. Suggested a continuous security system for Smart Homes. This approach uses various contextual information sources such as the user context (GPS position, records, calendar, etc.), the system context (position, tab, OS, apps, etc.), the network context (IP address, ping, communication speed, etc.) and the environmental context obtained from IoT devices spread over the house. However, contrary to our suggestion, this approach does not take into account the actions of the same consumer with different devices. In addition, the approach suggested is based around the use of ontologies and policies for authentication and authorisation. It uses IoT devices to collect information on the state of the situation that can be used to model the user and to allow the user to use or continue to use those resources. However, this approach is heavily reliant on the implementation context, requiring thorough preparation to better model user behaviour. As can be shown, there are various ideas for continuous authentication using different devices and ensuring successful efficiency during the authentication process. However, the current implementations do not integrate the behavioural details gathered from various devices used in our plan to authenticate the same user in several devices at the same time.

The Monitoring module shall acquire the data generated by the Smart Office devices in real time. – The Data Processing Module philtres, aggregates, and handles the previous data to produce the related attributes of user behavioural profiles. – The Judgment Module creates ML models to identify consumers by their behaviour. – The Reaction module sets various sensitivity thresholds to authenticate people, taking into account the performance of the previous modules. It also provides interfaces to allow a global authentication mechanism in the Smart Office The surveillance module will collect data produced by smart office devices from below if the users are using them. Table 1 offers an outline, for example, of the principal measurements to be tracked in a smart workplace. The data processing module collects raw data from the previous module on a daily basis. Filter, aggregate and process the raw behavioural data in the Feature Extraction Portion, for the measurement of features which model the user 's behaviour. It also takes frequent account of raw data collected over a period called time window. This aggregation is performed regularly. The architecture manager establishes this time span.

MULTI-FACTOR AUTHENTICATION USER

Authentication schemes are generally divided into three types. Awareness element is the first form that includes a password or a Lock. Possession-based authentication means the physical proof of one's identity. It can be a Multimedia Messaging Service (ATM) card or a token. In recent times, phone numbers and e-mail addresses are highly favoured because they are unique and available to all users.The OTP[8] is forwarded to the user during the transaction and users should enter the same on the transaction page. Although this will make it easy for users to hold any extra authentication codes such as a card, authentication will be weakened if a cell phone is robbed or misplaced. The inherence aspect is based on certain physical characteristics of a person that are special and can not be impersonated. Biometric schemes based on finger printing, iris, ears, etc. are in use. Multi-factor authentication is a mixture of more than one authentication scheme to improve the authentication process and maximise its success rate[9].

Client applications For user compliance monitoring, an application that implements the Client applications of the Monitoring Module is hosting Smart Office devices with sufficient computing capacities. The Client app is housed with third-party[10] or proxy in the case of resource-constricted devices. This application recalls periodically data generated by the interaction of the user. The durations are specified by the architecture administrator in the data processing module. We have developed customer applications for two devices: PCs and mobile devices (smartphones and tablets), as proof of concept.

4. PROPOSED METHODOLOGY

Cloud computing application In a cloud platform hosted by Smart Office data collection, decision-making and response modules have been installed. These modules require a significant number of storage and processing tasks, as the data generated by Smart Office devices are collected and stored. A REST API for the receipt of data from client applications is provided by the data processing moducle. In order to generate a dataset, the obtained data is handled one by IoT system following the following steps : 1. In time windows, process and connect the raw data (configurable) for 1 minute, to create the functionality of various users. 2. Mark the patented ID vector functions. 3. Use one hot encoding strategy to substitute text fields with values that the ML algorithm can recognise. 4. Filter functions with a value of 0 on all vectors. Once you have datasets with vector attributes, the Decision Module uses the Random Forest as a classification algorithm to classify and authenticate the various users. In this context, we use the implementation of the Random Forest given by Scikit-learn[11], which is capable of classifying users in a computational order that is lower than other solutions. 12]. Furthermore, Scikit-learns to train and incorporate ML modelling and pandas [13] to manipulate and process data are the most appropriate libraries used in this module. Thus, by training the algorithm with the data of the various monitored users, a Random Forest model is created for each type of IoT unit. After that, the Classification part periodically evaluates the function vectors created by a user with the various Random Forest models in a time window to get the odds of being each of the trained users for each IoT unit. Eventually, the Reaction component is implemented in Python and uses rules that consider the probabilities given by the Classification component (one value per model associated with the device). The rules are specified by the system administrator and the user's authentication level is the consequence. This degree of

authentication can be determined on the basis of one or more versions (belonging to various devices). Below are some guidelines, an example of a potential rule collection to calculate the degree of authentication: – Level 1: The user is correctly categorised and there is a high difference in the probability of belonging to other classes (users). This scenario represents normality and the typical user is the user who uses the computer. Stage 2: The consumer is accurately identified, but all users with a similar chance (±0.10) are assessed. This condition often represents normality but with more complexity, such that some system functionality, such as allowing administrator rights in some applications or closing critical applications, may be disabled at this stage. – Level 3: The user is not properly categorised, but the likelihood of a user class is similar to the class chosen (±0.10). This condition is suggestive that someone else might be the person using the equipment and not its owner. At this stage, it is agreed to submit an email notifying the user that there might be a potential anomalous condition. – Level 4: The user is not properly identified and the probability allocated to the user to whom the computer belongs is very low relative to the probability assigned to the chosen class. In this scenario, the computer will be blocked immediately and an email will be sent to the owner. In addition, the Reaction module implements the REST API to connect with the various Smart Office devices [14]. This API sends the level of user authentication and activities to be done to the Smart Office computers.

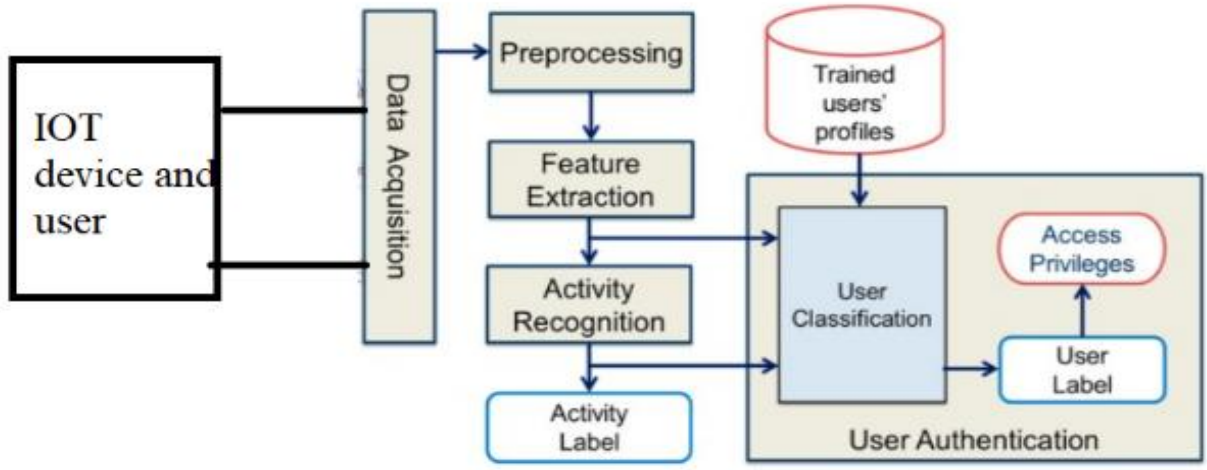

Fig 1: IOT based Authentication approach

5. COMPARISION ANALYSIS

The Comparison and Evaluation Eight performance assessment components were compared in order to evaluate the performance of the proposed system and the current system. These include non-repudiation, long password, user monitoring, blocking of mobile devices, user and mobile phone verification, prevention of re-use of user records, prevention of re-use of mobile phones, and type of credential. Non-repudiation: As the proposed process functions to authenticate the user and his or her cell phone (IMEI plus mobile number), all relevant user information, such as ID card number, mobile number and IMEI, is unique to the proposed system. The proposed method should then promise that the person who misuses the method is liable. Long password: Typically, a long authentication password is known to be better than a short one. Complex or useless codes, though, are hard to recall. A long password for authentication is generally considered safer than a short one. However, complex or meaningless passwords are difficult to remember. The user is only expected to rewrite long passwords (such as an IMEI, telephone number or ID card number) which they already have during the validation process. The password can also be accessed from the user ID card or cell phone by the user, although other programmes enable users to recall this key. User tracking: Most authentication schemes that produce OTPs from the server and send OTPs to the user via SMS cannot detect the user's tampering with the system because, in addition to the user's username and password, the authentication system only has the mobile number.

The device may be tampered with by a person who receives an OTP via SMS and then adjusts or discards the SIM card. The proposed system may decide the responsibility of the person who misuses the system or tampers with the system by the user's ID card number, which is a unique number, in addition to the mobile number (each user has a unique mobile number and a unique IMEI number). Mobile device blocking: You should use the IMEI to find the mobile device. The system can also be rendered unusable by blacklisting in any network. The proposed framework allows the IMEI to authenticate the computer and to take the appropriate measures against framework tampering. The administrator of the proposed system who detects any attempt to tamper with the system could cancel the user's account and prohibit the user and the related mobile device from registering on the system. If the OTP system cannot prohibit the same programme from being used, the illegal user can return and register (if the administrator detects illegal attempts by the user) as a legitimate user and obtain access to the system. Authentication of users and cell phones: These systems authenticate the user and ignore all parties that are used for electronic verification, such as the user's cell phone, contrasted with other authentication systems that use mobile phones to produce OTPs or accept text messages. Even so, to ensure the confidentiality of transactions on the Internet, the customer is not the only entity who has to be authenticated. In addition to mutual authentication between the user and the server via the Protected Socket Layer (SSL), the proposed framework authenticates both the user and the mobile device.

6. CONCLUSION

This thesis introduces a continuous and intelligent cloud computing paradigm-oriented authentication architecture. The system uses ML techniques to identify and authenticate users located in IOT Smart City Application and users. For the identification and authentication of various users using

classification algorithms. As a potential job, we expect to test our approach with a higher number of customers. In addition, we expect to use other ML algorithms, such as anomaly detection systems. Finally, we plan to expand the proof of concept to other IoT computers and operating systems such as Linux and iOS.

7. REFERENCES

[1] Kaburu, D.M., Sansa-Otim, J., Mayanja, K. *et al.* A usability based approach to designing continuous user biometric authentication system. *Qual User Exp* **3,** 8 (2018). https://doi.org/10.1007/s41233-018-0021-1

[2] Nixon K.W., Chen Y., Mao ZH., Li K. (2014) User Classification and Authentication for Mobile Device Based on Gesture Recognition. In: Pino R. (eds) Network Science and Cybersecurity. Advances in Information Security, vol 55. Springer, New York, NY. https://doi.org/10.1007/978-1-4614-7597-2_8

[3] Sales, T., Sales, L., Almeida, H. *et al.* A UPnP extension for enabling user authentication and authorization in pervasive systems. *J Braz Comput Soc* **16,** 261–277 (2010). https://doi.org/10.1007/s13173-010-0022-2

[4] Xue Q., Ju X., Zhu H., Zhu H., Li F., Zheng X. (2019) A Biometric-Based IoT Device Identity Authentication Scheme. In: Han S., Ye L., Meng W. (eds) Artificial Intelligence for Communications and Networks. AICON 2019. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, vol 287. Springer, Cham. https://doi.org/10.1007/978-3-030-22971-9_12

[5] Rajawat A.S., Upadhyay P., Upadhyay A. (2021) Novel Deep Learning Model for Uncertainty Prediction in Mobile Computing. In: Arai K., Kapoor S., Bhatia R. (eds) Intelligent Systems and Applications. IntelliSys 2020. Advances in Intelligent Systems and Computing, vol 1250. Springer, Cham. https://doi.org/10.1007/978-3-030-55180-3_49

[6] S. Dong, F. Farha, S. Cui, J. Ma and H. Ning, "CPG-FS: A CPU Performance Graph Based Device Fingerprint Scheme for Devices Identification and Authentication," 2019 IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress (DASC/PiCom/CBDCom/CyberSciTech), Fukuoka, Japan, 2019, pp. 266-270, doi: 10.1109/DASC/PiCom/CBDCom/CyberSciTech.2019.00056.

[7] Q. Wang et al., "VoicePop: A Pop Noise based Anti-spoofing System for Voice Authentication on Smartphones," IEEE INFOCOM 2019 - IEEE Conference on Computer Communications, Paris, France, 2019, pp. 2062-2070, doi: 10.1109/INFOCOM.2019.8737422.

[8] Khan R., Islam M. (2020) Cluster Based User Identification and Authentication for the Internet of Things Platform. In: Bohlouli M., Sadeghi Bigham B., Narimani Z., Vasighi M., Ansari E. (eds) Data Science: From Research to Application. CiDaS 2019. Lecture Notes on Data Engineering and Communications Technologies, vol 45. Springer, Cham. https://doi.org/10.1007/978-3-030-37309-2_14

[9] Sánchez Sánchez P.M., Huertas Celdrán A., Fernández Maimó L., Martínez Pérez G., Wang G. (2019) Securing Smart Offices Through an Intelligent and Multi-device Continuous Authentication System. In: Wang G., El Saddik A., Lai X., Martinez Perez G., Choo KK. (eds) Smart City and Informatization. iSCI 2019. Communications in Computer and Information Science, vol 1122. Springer, Singapore. https://doi.org/10.1007/978-981-15-1301-5_7.

[10] Z. Dou, I. Khalil and A. Khreishah, "A Novel and Robust Authentication Factor Based on Network Communications Latency," in IEEE Systems Journal, vol. 12, no. 4, pp. 3279-3290, Dec. 2018, doi: 10.1109/JSYST.2017.2691550.

[11] M. Wachs, Q. Scheitle and G. Carle, "Push away your privacy: Precise user tracking based on TLS client certificate authentication," 2017 Network Traffic Measurement and Analysis Conference (TMA), Dublin, 2017, pp. 1-9, doi: 10.23919/TMA.2017.8002897.

[12] A. Singh Rajawat and S. Jain, "Fusion Deep Learning Based on Back Propagation Neural Network for Personalization," 2nd International Conference on Data, Engineering and Applications (IDEA), Bhopal, India, 2020, pp. 1-7, doi: 10.1109/IDEA49133.2020.9170693.

[13] Lavanya R., Sundarakantham K., Mercy Shalinie S., Divya R., Selvamani K. (2020) User Authentication of IoT Devices for Decentralized Architecture Using Blockchain. In: M. Thampi S. et al. (eds) Applied Soft Computing and Communication Networks. ACN 2019. Lecture Notes in Networks and Systems, vol 125. Springer, Singapore. https://doi.org/10.1007/978-981-15-3852-0_2

[14] A. S. Rajawat and A. R. Upadhyay, "Web Personalization Model Using Modified S3VM Algorithm For developing Recommendation Process," 2nd International Conference on Data, Engineering and Applications (IDEA), Bhopal, India, 2020, pp. 1-6, doi: 10.1109/IDEA49133.2020.9170701.

[15] Srinivasan Rajarajan and Ponnada Priyadarsini," UTP: A Novel PIN Number Based User Authentication Scheme" The International Arab Journal of Information Technology, Vol. 16, No. 5, September 2019