DESIGN AND EVALUATION OF A LOW-COST BIOMETRIC WORK ACTIVITY REGISTRATION SYSTEM

Marta Menéndez Álvarez-Cofiño, Pelayo Nuño Huergo, Francisco González Bulnes, y Juan Carlos Granda Candás
Universidad de Oviedo (España)

DOI: https://doi.org/10.52152/11101 | Received: 27jan/2022 Reviewing: 17/may/2022 • Accepted: 17/oct/2022

To cite this article: NUÑO-HUERGO, Pelayo, MENENDEZ-ALVAREZ, Marta, GONZALEZ-BULNES, Francisco; GRANDA-CANDÁS, Juan-Carlos. DESIGN AND EVALUATION OF A LOW COST BIOMETRIC TIME TRACKING SYSTEM. DYNA, July August 2024. vol. 99, n. 4, pp. 400-404. DOI: https://doi.org/10.52152/11101

1. INTRODUCTION

The recording of work activity is a common problem in companies, especially in larger ones, where it can be difficult to keep track of employees' activities. This problem is exacerbated in the case of employees who do not work within a company-owned facility. Absence from the workplace, as well as non-compliance with working hours or excessively long breaks, lead to a decrease in productivity as well as economic losses for companies. There are also situations where employees work more hours than agreed without being paid for it. To address these issues, on 13 February 2019, the Spanish Government approved Royal Decree-Law 8/2019, which, in its tenth article, establishes the obligation for companies to record employees' work hours on a daily basis. This decree also allows for the regulation of extensions or limitations on work hours and breaks, and establishes that the recorded data must be kept for four years [1]. This measure aims to improve transparency and address job insecurity.

Currently, there is no standardised system for complying with the requirement to record working time, leaving many companies without guidance on how to deal with this provision. This problem is exacerbated in cases where employees work all or part of their working day away from the company facilities. Commercial agents or staff working remotely from home are examples of such situations.

In addition, companies already using solutions to record work activity face the challenge of fraudulent registrations, where an employee logs in on behalf of a colleague. To address this, it is crucial to adopt methods that ensure the unique identity of the employee. Biometrics, which use unique and non-transferable physical characteristics such as two [2] or three-dimensional fingerprints [3], voice [4], iris [5], retinal vascular pattern [6] or face [7], offer an effective solution. Although more reliable, these systems are also more expensive than conventional card readers. Therefore, the cost of implementing these solutions can have a negative impact on business economics.

In this paper, a low-cost solution to address the problems mentioned above is presented. The proposal is to take advantage of the corporate computer network using *Voice over IP* (VoIP) technologies. From their workstations, employees can dial a *Private Branch Exchange* (PBX) extension to check-in, check-out or take a break from work. This method is also accessible to employees outside the corporate network who call the PBX from external locations. In addition, to prevent registrations from being made by a third party, the employee is asked to repeat a passphrase so that the system can verify his or her identity by voice. The verification process is text-independent (TI), so the passphrases posed to employees are unrestricted. To avoid impersonation, the passphrase is proposed randomly, so the solution is robust even if a voice sample of the employee to be impersonated is available. When the identification is successful, the time of the call is stored in a database, recording the start or end of the working day or break.

For companies without VoIP infrastructure, open-source solutions can be deployed enabling a conventional computer to become a VoIP PBX. In this work, the Asterisk PBX has been used. Moreover, there is no need to purchase compatible physical phones, as calls can be made from a software phone (softphone) installed on the employee's computer or from a mobile device if the employee is out of the office.

2.- MATERIALS AND METHODS

The recording of work hours is the subject of analysis in the scientific literature, with proposals arising that seek the most appropriate approach and technology to carry out this task.

In [8], a system using *Radio-Frequency IDentification* (RFID) tags is proposed to automate staff check-in and check-out. Other studies perform automatic check-in using workers' mobile devices instead of a token [9] [10]. The first is based on *Address Resolution Protocol* (ARP) requests that devices send through the corporate WiFi network, using the MAC address of the mobile to detect the arrival of an employee at the workstation. The second study uses *Near- Field Communication* (NFC), present in many modern mobile phones, to detect the presence of employees on the network. While these studies improve usability compared to manual or token-based systems, they can pose problems for employees without smartphones and lack reliability against spoofing or fraudulent registrations via applications that generate ARP or NFC requests.

To guarantee the authenticity of the employees' record, the current trend is shifting towards systems that employ biometric elements, from traditional methods such as fingerprint identification [11], to more advanced techniques such as facial recognition [12]. Although effective, these systems require the installation of dedicated devices for this purpose and are vulnerable to counterfeiting through moulds or photographs. A more robust biometric system, presented in [13], is based on radio frequency, identifying individuals by how they distort radio signals. This approach, transparent to the employee, virtually eliminates the possibility of fraudulent registrations. However, its effectiveness is limited if employees work away from the company facilities and may require updates in the case of sudden and noticeable physical changes.

2.1 VOICE RECOGNITION BASED BIOMETRIC SYSTEMS

The use of voice as a biometric element to register work activity has also been analysed in the literature. In [14] they make use of an Asterisk PBX with which the user interacts by answering various questions until they obtain sufficient voice samples to determine their identity from a catalogue of employees' audios stored in the system. However, it is not verified that the answers are consistent, with the risk of impersonation if an employee has recorded voice samples from a third party that he/she replays when interacting with the PBX. This work was extended in [15] and [16], where more voice-based identification mechanisms are incorporated, one of them being text-independent. However, in that case the system requires a three-minute audio sample from the user, which makes it difficult to implement in a real environment.

An alternative to the use of the Asterisk PBX is presented in [17] using the Alexa voice assistant to perform attendance control in an educational environment. Likewise, in [18] and [19] two biometric attendance control systems are presented, based on voice and fingerprint recognition, using respectively an Arduino and a Raspberry Pi as devices to capture the user's voice. These alternatives prove to be perfectly viable, but would be costly if implemented in a business environment as they do not take advantage of the existing infrastructure, either the PBX itself, or the VoIP hardware/software terminals and mobile devices.

2.2 PROPOSED SOLUTION

The architecture of the biometric activity registration system, shown in fig. 1, consists of five elements. Firstly, the VoIP phone terminal from which the employee dials the PBX to register his work activity. Second, the Asterisk PBX, which controls the registration process. Third, the audio-to-text transcription service, which in the scope of this work corresponds to the Google speech-to-text service [20], verifies the coincidence of the content of the passphrase repeated by the employee with the one proposed by the PBX. Fourth, the biometric analysis service, an API that evaluates the audio of the employee's passphrase together with a model audio of the same employee, returning a probability match value. Finally, the MySQL database where the employee’s actions are recorded: start and end of the working day or work break. The sample audios and passphrases are encoded using G.711 and stored in .wav format.

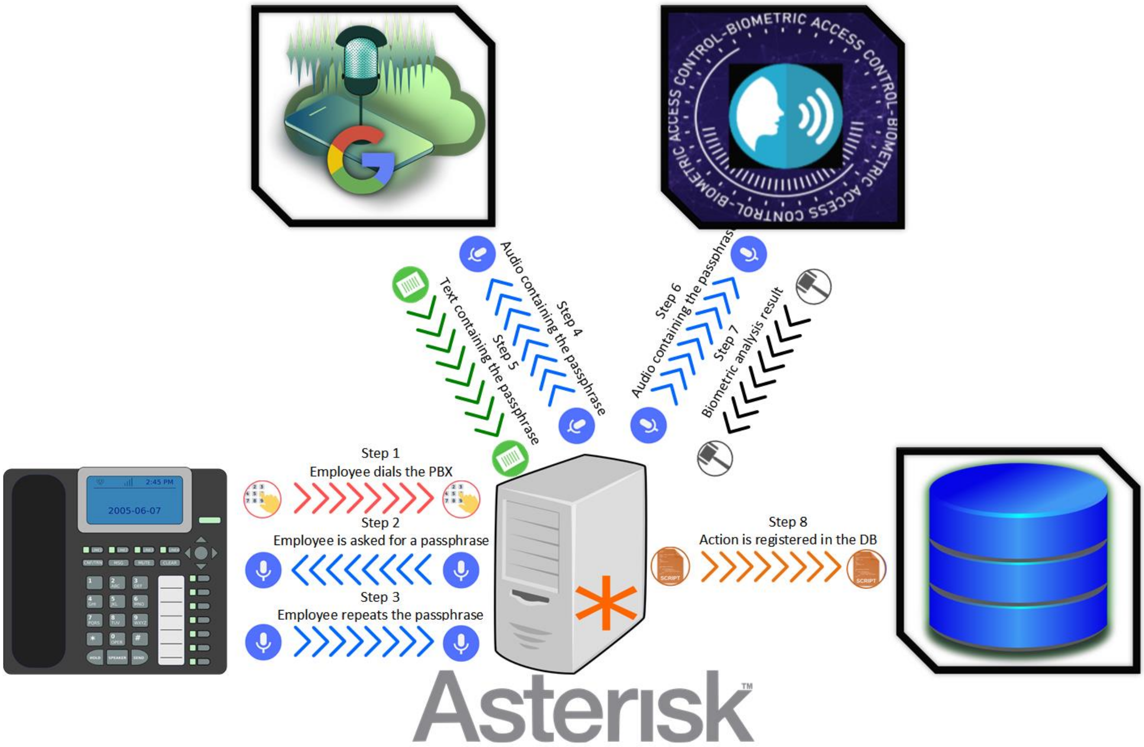
BIOMETRIC ACCESS CONTROL-BIOMETRIC ACCESS CONTROL-BIOMETRIC ACCESS CONTROL
Step 4
Audio containing the passphrase
Step 5
Text containing the passphrase
Step 6
Audio containing the passphrase
Step 7
Biometric analysis result
2:45 PM
2005-06-07
Step 1
Employee dials the PBX
Step 2
Employee is asked for a passphrase
Step 3
Employee repeats the passphrase
Step 8
Action is registered in the DB
SCRIPT
Asterisk

Figure 1: Architecture of the proposed solution

The operation of the system is exemplified by an employee, Alice, who wants to register the start of her working day. The process begins by dialling extension 1000 of the PBX from her phone terminal. The PBX answers the call, randomly selects a passphrase from those stored in the system and plays it back to Alice. The system developed has dozens of passphrases stored in the database. To play them back, all of them are pre-recorded by the system administrator. However, the system could also dynamically generate these recordings using third-party text- to-speech services. When Alice hears the passphrase, she repeats it, and the PBX records her speech in an audio file.

This is followed by two sequential verifications. First, the audio file with Alice's passphrase is sent to the transcription service, which returns her speech in text format. The PBX then checks whether the passphrase dictated by Alice matches the original passphrase. This prevents the impersonation of Alice by a third party, since, without this verification, it would be enough to obtain a recording of Alice repeating a passphrase in order to impersonate her during the biometric analysis.

If the above check is correct, the biometric analysis is carried out, consisting of sending the audio file with Alice's passphrase, together with its audio model, to the biometric service. For this purpose, an audio template is stored in the database for each employee who has an account registered in the PBX. The response of the biometric service provides a match probability value. Based on this value, the PBX allows Alice access to an interactive response menu (IVR), indicating the actions to be performed.

In the IVR, Alice selects the extension associated with the start of the day, which in this system is 1. The PBX then obtains the date and time from the system and runs a script that updates the database to reflect Alice's start time. For other actions available in the system (end of working day, start and end of work break), the process is similar, changing only the extension (2, 3 and 4 respectively) that the employee selects after accessing the IVR. It is important to note that in the IVR, consistency checks are carried out on the actions that the employee tries to register, avoiding, for example, starting a new working day if one is already in progress, ending a break without it having been started previously, etc.

Finally, it should be noted that the proposed system also has an alternative identification mechanism for cases where the biometric service is unable to detect legitimate users due to temporary circumstances affecting their voice, for example if an employee is suffering from a speech impediment.

After detecting a number of consecutive unsuccessful identification attempts -three in the proposed system, although it is configurable- the PBX poses a question to the user regarding some personal data as a token. Specifically, in the scope of this project, the user is asked for his or her ID. Once the user pronounces his or her personal data, this is verified using the speech-to-text transcription service with respect to the value stored in the database. Therefore, in this alternative mechanism, the analysis by the biometric service is omitted. If the verification is successful, the PBX redirects the user to the IVR presented above. In addition, when the user performs the corresponding action, the system reflects by means of a flag in the database that this action has been performed after an identification in the system through the alternative mechanism. In this way, it is possible to keep a traceability of the use of this mechanism, and identify possible users who are making a continuous and potentially fraudulent use of it.

3.- RESULTS

During the experimentation of the proposed system, two test scenarios have been analysed. In the first scenario, the performance of the biometric analysis service is studied based on the length of the passphrase to be repeated by the employee. The objective of this scenario, whose results are shown in Table I, is to determine how the length of the passphrase affects the probability of successful employee identification.

In addition, it is analysed whether the length of the passphrase has any consequence on the response time during the identification process, which is presented in Table II. To calculate the response time, the time difference between the response obtained from the biometric analysis service and the time when the audio samples were sent to be compared is determined.

In this scenario, three audios were taken from each participant for each passphrase length of between one and seven words. All of them were compared with the model audio that each participant has stored in the system. Four participants, two males and two females, took part in this test scenario with a mean age of 38.75 years ($siggma$=18.19).

USER	PROBABILITY						
	1 word	2 words	3 words	4 words	5 words	6 words	7 words
User1	0.731375	0.840355	0.937976	0.978122	0.999799	0.993866	0.999584
User2	0.249712	0.538086	0.769614	0.968933	0.999180	0.997671	0.999866
User3	0.751507	0.981764	0.992965	0.999876	0.999839	0.999934	0.999898
User4	0.995329	0.999600	0.999910	0.999962	0.999974	0.999993	0.999998
Average	0.681981	0.839952	0.925116	0.986723	0.999698	0.997866	0.999837
Std. deviation	0.312152	0.213480	0.107306	0.015692	0.000354	0.002877	0.000177

Table I: Performance depending on the length of the audios.

USER	TIME (S)						
	1 word	2 words	3 words	4 words	5 words	6 words	7 words
User1	0.430132	0.645371	0.530916	0.295924	0.298949	0.354206	0.339351
User2	0.519569	0.520047	0.575357	0.535810	0.532469	0.522709	0.532750
User3	0.352124	0.300450	0.341765	0.317621	0.310864	0.295339	0.374444
User4	0.394671	0.372388	0.676807	0.741798	0.636347	0.563229	0.680680
Average	0.424124	0.459564	0.531211	0.472788	0.444657	0.433871	0.481806
Std. deviation	0.071174	0.153947	0.140282	0.209520	0.166920	0.129310	0.157021

Table II: Processing time depending on the length of the audios.

The results of the first test scenario are summarised in fig. 2. The clear influence of the length of the passphrase on the identification of employees stands out. Specifically, it is observed that a passphrase consisting of three words achieves a match probability of more than 0.9. However, for the use of the biometric analysis service within the activity registering system, a minimum length of 5 words would be recommended for accurate voice identification, since probabilities very close to the maximum (1) are achieved. As for the response time, it can be stated that it does not increase as a function of the length of the passphrase.

The second test scenario analyses the reliability of the identification of the biometric analysis service. Thirty participants, thirteen males (43.33%) and seventeen females (56.66), took part in this scenario, with a mean age of 31.97 years ($siigma$=15.5). The probability threshold at which an identification is considered to be a match was selected based on the results in Table I for a 5-word length, being set at 0.9996. This passphrase length is chosen because the shorter the passphrase length, the less effort it is for the participant to repeat it when interacting with the PBX, which results in an increase in the usability of the system.

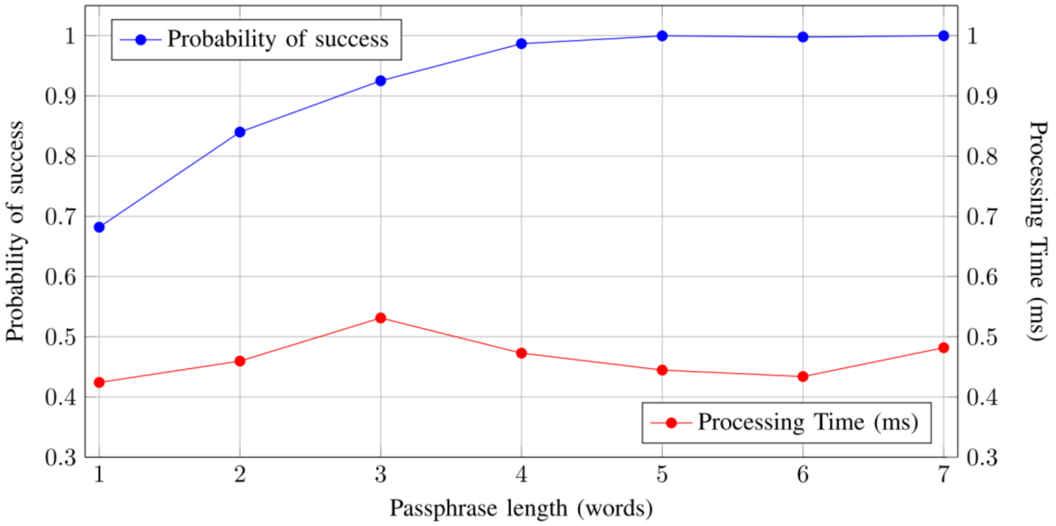

Figure 2: Performance as a function of passphrase length.

Two audio samples were taken from each participant containing passphrases of a length of five words. Then, for the thirty available users, all possible combinations of their two samples were made, allowing for repetitions but no permutations. The identifications were classified as fraudulent (positive samples) or legitimate (negative samples) out of the total of the 1830 possible combinations of audios that can be made under the above assumption. The confusion matrix with the classifier results is presented in Table III. In addition, several key metrics that allow determining the identification performance of the biometric analysis service were evaluated, as shown in Table IV.

The results in this second test scenario give an accuracy of 99.7% with an precision of 99.89% and an F1-score of 99.86%, which proves that the identification of the biometric service is reliable. Focusing on fraudulent identification attempts, the system achieves a recall of 99.8%, indicating that it is able to detect almost all fraudulent identification attempts. The FNR (False Negative Rate) value of 0.17% indicates that less than 2 out of 100 fraudulent identification attempts go undetected by the system.

In the case of samples with legitimate identification attempts, a specificity value of 97.8% is obtained. This implies that in 2.2% (FPR, False Positive Rate) of the occasions an employee's identification is rejected, which should not be a problem due to the three possible attempts and the alternative identification mechanism offered.

		Predicted	
		Positive (fraud)	**Negative (non fraud)**
Current	**Positive (fraud)**	1737	3
	Negative (non fraud)	2	88

Table III.- Confusion matrix

Accuracy	Precision	Recall	Specificity	FPR	FNR	F1
0.99727	0.99885	0.99828	0.97778	0.02222	0.00172	0.99856

Table IV.- Performance metrics

4.- DISCUSSION

The feasibility of the system presented to carry out the registration of the work activity with the use of voice biometric analysis is remarkable. It is an alternative that can be easily deployed in various work environments without excessive economic costs. The system is based on an open-source PBX supporting convergent LANs with VoIP technology along with hardware VoIP phones. In addition, it can be deployed on conventional LANs by installing software VoIP phones on employees' computers. In both scenarios, the only relevant cost is the licensing of voice-to-text transcription and biometric analysis services, together with the cost of the computer hosting the Asterisk PBX. However, in the case of using open APIs for the above services, the costs would be even lower.

The proposed system proves to be reliable according to the results obtained. Remarkable levels of prediction accuracy, precision and recall have been achieved by using significantly shorter sample lengths as passphrases than existing solutions in the literature. Furthermore, the use of independent text-based speech analysis allows the use of random passphrases for each employee, thus reducing the risk of impersonation by third parties. To improve the precision metric, it would be desirable to consider extending the length of the passphrase along with an increase in the probability threshold value for identification. This tuning would not negatively impact the response time of the system and would contribute to decrease the false positive rate. However, it is crucial to ensure that the length of the passphrase does not interfere the usability of the system. Nevertheless, the three attempts offered to the user to identify himself/herself, coupled with identification via an alternative mechanism, minimises the impact of false positives.

In terms of limitations of the proposed system, it is worth considering the fraudulent registrations that could be made in the system through the use of software that allows the cloning of a third party's voice based on artificial intelligence (AI voice cloning). The use of random passphrases makes it very difficult to use such applications to impersonate third parties. These applications are not yet capable of cloning a user's voice in real time. Under these conditions, the system is robust, as it sets a configurable time limit of a few seconds during which the PBX listens for the user's passphrase. However, once voice cloning applications are able to operate in real time, they will pose a real threat to the reliability of the proposed system that will need to be studied.

REFERENCES

[1] Spanish Government approved Royal Decree-Law 8/2019, https://www.boe.es/boe/dias/2019/03/12/pdfs/BOE-A-2019-3481.pdf Last access: 3/11/2023.

[2] Ramya, K.R.; Josephine, B. M.; Praveen, K. D.; Maruthi, M. B., Kumar, C. S. An efficient and secured biometric authentication for IoT. *International Journal of Emerging Trends in Engineering Research*, 2019, vol. 7, nº. 11, p. 604-609. ISSN: 2347-3983. DOI: http://doi.org/10.30534/ijeter/2019/327112019

[3] Cheng, K.H.M.; Kumar, A. Contactless Biometric Identification Using 3D Finger Knuckle Patterns. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 2020, vol. 42, nº. 8, p. 1868-1883. ISSN: 0162-8828. DOI: http://doi.org/10.1109/TPAMI.2019.2904232

[4] Hollien, H. An Approach to Speaker Identification. *Journal of Forensic Sciences*, 2016, vol. 61, nº. 2, p. 334-344. ISSN: 0022-1198. DOI: http://doi.org/10.1111/1556-4029.13034

[5] Abdul, W.; Alzamil, A.; Masri, H.; Haq, Q.E.U.; Ghouzali, S.; Hussain, M.; Alzuair, M. Fingerprint and iris template protection for health information system access and security. *Journal of Medical Imaging and Health Informatics*, 2017, vol. 7, nº. 6, p. 1302-1308. ISSN: 2156-7018. DOI: http://dx.doi.org/10.1166/jmihi.2017.2149

[6] Abrishami-Moghaddam, H.; Farzin, H.: Moin, M.S. A novel retinal identification system. *EURASIP Journal on Advances in Signal Processing*, 2008, vol. 2008, p. 1-10. ISSN: 1687-6180. DOI: http://dx.doi.org/10.1155/2008/280635

[7] da Silva Nieto, J.G.; Caldeira, J.L.M.; Ferreira, D.D. Face Recognition based on Higher-Order Statistics. *IEEE Latin America Transactions*, 2018, vol. 16, nº. 5, p. 1508-1515. ISSN: 1548-0992. DOI: http://doi.org/10.1109/TLA.2018.8408448

[8] Jyothi, K.; Karthik, R.; Anusha, B.; Annapurna, B.; Kiran, A.; Soumya, K.; Harini, N. Design and implementation of RFID based attendance system. *International Journal of Innovative Technology and Exploring Engineering*, 2019, vol. 9, nº. 1, p. 853-855. ISSN: 2278-3075. DOI: http://dx.doi.org/10.35940/ijitee.A4353.119119

[9] Prabowo, O.M.; Saputra, D.E. Design and Implementation of Automatic Attendance System using ARP Request Detection. *International Conference on Information Technology Systems and Innovation*, 2018, p. 139-142. DOI: http://dx.doi.org/10.1109/ICITSI.2018.8695933

[10] Oo, S.B.; Oo, N.H.M; Chainan, S.; Thongniam, A.; Chongdarakul, W. Cloud-based web application with NFC for employee attendance management system. *International Conference on Digital Arts, Media and Technology*, 2018, p. 162-167. http://dx.doi.org/10.1109/ICDAMT.2018.8376516

[11] Santoso, B.; Sari, M.W. Design of Student Attendance System Using Internet of Things (IoT) Technology. *Journal of Physics: Conference Series*, 2019, vol. 1254, nº. 1, p. 1-11. ISSN: 1742-6588. DOI: http://dx.doi.org/10.1088/1742-6596/1254/1/012064

[12] Pooja, I.; Gaurav, J.; Yamuna Devi, C.R.; Aravindha, H.L.; Sowmya, M. Smart Attendance System Using Deep Learning Convolutional Neural Network. *International Conference on Remote Engineering and Virtual Instrumentation*, 2019, vol. 80, p. 343-356. ISSN: 2367-3370. DOI: http://dx.doi.org/10.1007/978-3-030-23162-0_31

[13] Miao, Q.; Xiao, F.; Huang, H.; Sun, L.; Wang, R. Smart attendance system based on frequency distribution algorithm with passive RFID tags. *Tsinghua Science and Technology*, 2020, vol. 25, nº. 2, p. 217-226. ISSN: 1007-0214. DOI: http://doi.org/10.26599/TST.2018.9010141

[14] Dey, S.; Barman, S.; Bhukya, R.K.; Das, R.K.; Haris, B.C.; Prasanna, S.R.M.; Sinha, R. Speech biometric based attendance system. *Twentieth National Conference on Communications*, 2014, p. 1-6. DOI: http://dx.doi.org/10.1109/NCC.2014.6811345

[15] Das, R.K.; Jelil, S.; Prasanna, S.R.M. Development of Multi-Level Speech based Person Authentication System. *Journal of Signal Processing Systems*, 2016, vol. 88, p. 259-271. ISSN: 1939-8018. DOI: http://doi.org/10.1007/s11265-016-1148-z

[16] Jelil, S.; Shrivastava, A.; Das, R.K; Prasanna, S.R.M.; Sinha, R. SpeechMarker: A voice based multi-level attendance application. *Proceedings of the Annual Conference of the International Speech Communication Association,* 2019, vol. 2019, p. 3665-3666. ISSN: 2308-457X. DOI: http://doi.org/10.21437/Interspeech.2019-8014

[17] Adithya Sanjeev Byalpi, A. Alexa based Real-Time Attendance System. *International Conference on Communication and Electronics Systems*, 2018, p. 121-124. DOI: http://doi.org/10.1109/CESYS.2018.8724006

[18] Priyadharshini, A.; Balakrishnan, R.; Shazuli, S.M.; Gunapriya, D.; Deepthi, J. Convolutional Neural Network for Speaker Recognition Embedding with Biometric System. *International Conference on Inventive Computation Technologies*, 2022, p. 896-900. DOI: http://doi.org/10.1109/ICICT54344.2022.9850483

[19] Becerra, A.; de la Rosa, J.I.; Velásquez, E.J.; Zepeda, G.; Escalante, N.I.; Pedroza, A.D. Portable student attendance management module for university environment by using biometric mechanisms. *Multimedia Tools and Applications*, 2023, p. 1-25. ISSN: 1380-7501. DOI: http://doi.org/10.1007/s11042-023-15482-y

[20] Speech-to-Text Conversion – Google API. https://cloud.google.com/speech-to-text. Last access: 3/11/2023.

ACKNOWLEDGEMENTS

This research has been partially funded by the project PID2021-124383OB-I00 of the National Plan for Research, Development and Innovation. Thanks also to the Instituto Universitario de Tecnología Industrial de Asturias (IUTA) for their support.

SUPPLEMENTARY MATERIAL: THE ASTERISK PBX

Asterisk is an open-source framework that allows a conventional computer to act as a telephone PBX. Asterisk configuration is based on multiple configuration files. Some configuration files are related to signalling protocols, such as the pjsip.conf file for *Session Initiation Protocol* (SIP), allowing to register accounts that can log in to the PBX using these signalling protocols. Authentication parameters such as user names, passwords, supported codecs, etc. can also be defined.

Asterisk functionality is programmed by means of a special configuration file (extensions.conf) that defines the dial plan. This configuration file defines the actions and services that are available to a user account and is specified declaratively by means of a proprietary scripting language. The dial plan is organised in contexts, which are independent sections corresponding to the minimum organisational unit of the dial plan. The purpose of using contexts is to group and separate functionalities within the dial plan, e.g. to provide a different set of services on a per-user basis. A context can be composed of one or more extensions that can be dialled from VoIP terminals. An extension is a set of related instructions that are executed sequentially to achieve the desired behaviour. Each instruction within an extension is numbered and referred to as a priority. In addition, each instruction executed performs an action in the dial plan. In the Asterisk environment, this action is called an application. An example of a dial plan is shown in fig. 3.

```
[MyContext]
exten => 1000,1,Answer()
;The call is answered
exten => 1000,2,AGI(./scripts/UpdateDB.sh)
;A bash script located in the PBX is invoked
exten => 1000,3,Playback(message)
;The "message" file containing an audio file is played
exten => 1000,4,Wait(2)
;A two-second pause
exten => 1000,5,Dial(PJSIP/Alice)
;A call is made to Alice's phone terminal
exten => 1000,6,Hangup()
;The call is hung up
```

Figure 3: Example of a dial plan in Asterisk

As can be seen, the fragment shows a context, called MyContext, composed of a single extension (1000). When this extension is dialled, six instructions (priorities) are executed step by step, invoking a different application in each of them. For example, the Playback application plays an audio stored in the PBX, while the Dial application calls a user registered in the PBX.

An interesting aspect of Asterisk is that it can be used to develop systems that go beyond the role of a telephone PBX. In the scope of this work, the Asterisk PBX plays the role of a user interface, whereby it receives commands from the user via a VoIP phone (software or hardware) and, as a response, executes actions on other systems via scripts written in languages such as Python, Bash and Perl. In this sense, the *Asterisk Gateway Interface* (AGI) application is the key component, as it allows more complex solutions to be developed. In the dial plan example illustrated in fig. 3, the AGI application is used to execute a script that updates the content of a database after the call is answered.