Using Aadhaar for Continuous Test-Taker Presence Verification in Online Exams

N. Sethu Subramanian, Sankaran Narayanan, M. D. Soumya, Nitheeswar Jayakumar and Kamal Bijlani

Abstract In the context of Indian higher education, deployment of online exams for summative assessments is hampered by the lack of a reliable e-assessment system that can guarantee high degree of examination integrity. Current methods for maintaining integrity of online exams largely depend on proctor-based invigilation. This cumbersome method does not fully prevent test-taker impersonation. We propose leveraging the Aadhaar biometric data to verify the presence of the test-taker throughout the entire duration of the examination. Such a continuous presence verification technique is likely to be far more successful in preventing impersonation than the conventional methods. Our method can help eventually eliminate the need for a remote proctor. We identify a set of strategies to systematically validate the effectiveness of the proposed system.

Keywords LMS · Cloud · Exam cheating · Proctoring · e-Assessment Multimodal biometrics

1 Introduction

Online assessments are gaining increased acceptance in higher education as the preferred appraisal scheme, gradually replacing the manual paper-and-pen assessment

N. S. Subramanian (✉) · S. Narayanan · M. D. Soumya · N. Jayakumar · K. Bijlani
Amrita e-Learning Research Lab (AERL), Amrita School of Engineering, Amrita Vishwa Vidyapeetham, Amrita University, Amritapuri, India
e-mail: sethus@am.amrita.edu

S. Narayanan
e-mail: nsankaran@am.amrita.edu

M. D. Soumya
e-mail: soumyamd@am.amrita.edu

N. Jayakumar
e-mail: nitheeswar90@gmail.com

K. Bijlani
e-mail: kamal@amrita.edu

S. C. Satapathy et al. (eds.), *Information and Decision Sciences*,
Advances in Intelligent Systems and Computing 701,
https://doi.org/10.1007/978-981-10-7563-6_2

format for both formative and summative assessments [1]. Summative evaluations, such as final exams, are also transitioning from written to a blended assessment model [2] composed of a mix of open- and close-ended questions. These unified evaluations could very well be conducted in a proctored online setting obviating the need for the pen-and-paper option. However, there is a wide perception that online exams are inherently insecure despite being proctored [3, 4]. This perception hampers widespread adoption or constrains institutions, to conduct online exams in controlled settings under strict uninterrupted vigilance. These burdensome options motivate the development of practical alternative measures to administer online examinations, untainted by cheating and concomitant security violations.

Test-taker validation, identity verification, and impersonation prevention are major security goals that need to be achieved to ensure the integrity of summative e-assessments [5]. These three criteria need to be satisfied in any solution so that consumers of reliable, vetted academic grading systems such as educators, employers, public and private sector enterprises, and government agencies are assured of the authenticity and integrity of the examination process. Conventional methods such as usernames and passwords, hall tickets, or even biometrics provide only a partial security solution by meeting the initial validation criteria. But these checks are incapable to certify that the test-taker has not subsequently switched during the exam. Thus, frequent reports of compromised exams due to student–student or student–proctor collusions form part of the daily news headlines. These occurrences can be due to empathy, blackmail, bribery, or coercion. Test-taker impersonation is thus a key threat that needs comprehensive attention.

Impersonation occurs when someone other than the designated individual seeks all access privileges duly granted to the vetted person, whose identity is being claimed by the impersonator. In the case of online exams, this usually occurs when test-takers reveal deliberately their security credentials to the impersonating person who can then complete the exam on their behalf. Continuous presence verification [6] has been proposed as a means to reaffirm test-taker integrity throughout the examination process. The presence of the test-taker is verified continuously using biometric features such as fingerprints or keystroke dynamics [7] for the entire duration of the examination. Several factors serve to inhibit the wide deployment of sophisticated security technology such as these. First among these is the lack of a central repository database to collect and store test-taker demographic and security profile data during the enrollment/registration phase. Given the globally distributed test-taker body in large educational institutions and learning centers, building and maintaining an aggregated, real-time updated, and verifiable database poses a significant logistical and engineering challenge. The other security challenge is safeguarding such a database against attacks by hackers and terrorists.

In this paper, we propose a simple, efficient, and cost-effective architectural approach to continuous test-taker presence verification in the mega-sized Indian educational context. Our concept incorporates the field-proven Aadhaar database [8, 9] with a collection of biometric data of over a billion Indian citizens. Mobile devices have facilitated increased awareness of biometrics, such as fingerprint scanning technology, especially among the younger citizens. Moreover, inexpensive USB-based

fingerprint scanning devices are gaining wide adoption in a variety of commercial settings for use with Aadhaar and other biometric systems. The confluence of these factors renders the proposed architecture ideal for continuous test-taker presence verification in large-scale distributed e-assessment applications.

2 Related Work

Authentication of an initial user (i.e., test-taker) can be accomplished via several mainstream techniques [7]. Knowledge-proof methods require the user to demonstrate knowledge of a secret possessed only by that user such as usernames–passwords, security questions–answers, etc. As standalone authentication factors, these methods are susceptible to inter test-taker collusion. Possession proof methods require the user to possess a physical entity such as an ID card. These are generally used when the exam is conducted in a proctored environment such as a university examination hall or an accredited exam center but vulnerable as the card can be cloned. Biometric methods rely on the user's unique physical characteristics such as fingerprint [10] or iris recognition [11]. By far, biometric methods are the most reliable for initial authentication but they do not provide continuous presence verification by themselves.

Proctoring methods using a remote proctor observing test-takers via webcams [12] or centralized video cameras is a widely accepted practice to minimize the likelihood of malpractices in exam centers. This method is generally good at capturing abnormal activities in an examination center. However, these and other video-camera-based methods are storage-greedy and bandwidth-intensive [13] that do not scale well when there is large number of test-takers involved. Observing the test-taker's face via an individualized webcam by the remote proctor could be a reasonable method for continuous presence verification. Currently, this approach has a few problems that limits its practical effectiveness. First of all, it requires an alert proctor, undistracted for the entire duration of the exam. Second, each proctor is able to monitor only a few test-takers effectively. Lastly, there is a paucity of inexpensive off-the-shelf proctoring solutions that can be readily deployed.

Several methods have been proposed to reduce the dependency on remote proctor. Swathi et al. [14] propose a method to perform feature extraction for automated face understanding. Their work was geared to ensure presence of the examinee throughout the examination session, with the assumption that if the face is not present it could indicate malicious activity. Krishnamoorthy et al. [15] used image recognition to automatically recognize the test-taker's face. These measures remain under the domain of active research.

Flior et al. [7] proposed keystroke dynamics for biometric authentication. By detecting the keystroke typing patterns of the pre-authenticated users, a model is constructed to provide continuous presence verification. Although keystroke detection has been shown to have low error rates in lab conditions [5], its availability and technical maturity for mass-scale deployment such as the heterogeneous test-taker

population in India is far from clear [16]. The same can be said for other types of advanced biometrics like Iris recognition, too expensive to be established on a mass-scale.

Fingerprint biometrics [10] are used ubiquitously all over India in various public and private sector enterprises like military, banking, etc. They are easy to use, have fast response time, and impose minimal technology training and deployment overhead. Most modern mobile phones are equipped with a built-in fingerprint sensor that can unlock a phone by recognition of the human fingerprints. USB-based fingerprint scanning devices are also available that scan fingerprints with greater details and higher levels of accuracy. Studies have shown that among the domain biometric options, the fingerprint biometric option is the least intrusive and most reliable [17]. Gil et al. [10] have proposed the design of a middleware that links up a fingerprint identification system with the university learning management system (LMS). Their solution requires a computer connected with a biometric reader for every test-taker.

Clarke et al. [13] outline a generic e-invigilation methodology that can utilize several methods to provide continuous presence verification. They envisage extensive use of facial recognition as it can be implemented naturally by placing a webcam on top of the test-taker's monitor. Their prototype performed fingerprint authentication by uploading fingerprints to a central server.

The goal of the present work is to transform the fingerprint scanning option into an efficient, practical method approach for continuous presence verification of test-takers (such as students) in e-assessment sessions.

3 Proposed Methodology

In this paper, we propose a simple architecture to enable continuous authentication by means of the Indian government's Aadhaar database [8, 9]. Our first observation is that the biometric data collection and management process is simplified significantly by the presence of the Aadhaar database. Aadhaar Web Services make available a portal interface that can be dedicated to biometric verification by third-party service providers.

Modern smartphones and laptop personal computers (PCs) are built-in with a fingerprint sensor that can be configured as a login mechanism. These built-in sensors are designed for single-user identity verification scenarios. Devices with these sensors do not allow export of the private biometric information beyond that device to protect the user's privacy. Thus, these sensors are of no use in public, multiuser identity verification settings. In contrast to fingerprint sensors, fingerprint scanning devices are designed for public, multiuser identify verification scenarios. These devices can be interfaced to a PC or a smartphone via USB. They are widely available, inexpensive, and easy to train and deploy. Coupled with image recognition-based fingerprint detection technology, these scanning devices serve as an effective mechanism to identify fingerprints in large multiuser identity verification settings.

Test-taker information stored in a profile database (such as LMS in academic environments) is normally the starting point for exam authentication and launch of the exam sessions and storing of results. This is most commonly done using a Web Portal that the test-takers connect to from their Browsers. To bring the benefits of Biometrics to an academic environment, integration with such profile databases is necessary.

Integrating Aadhaar with student profile databases (such as Learning Management Systems) can be easily achieved via a cloud service. This architecture provides a seamless channel for large-scale dispensation of benefits of biometric authentication to the online exam environment.

3.1 Aadhaar Service Overview

Aadhaar identity management system was originally intended as a mechanism that can efficiently enable reliable large-scale delivery of various social services and entitlement programs. It has since become the largest biometric verification system in the world. Aadhaar service supports hundreds of millions of verification requests per day with sub-second latencies. Aadhaar exposes open services to help verify identity of the claimant using a combination of biometrics and demographic data. Aadhaar service is being used for fraud detection in near real time, in a variety of application domains.

The Aadhaar system architecture is shown in Fig. 1. The Authentication User Access Server (AUA) is an application-domain-specific server that receives requests for authentication from client agents and forward it to the Aadhaar Authentication Service (AAS). The authentication service returns a simple Boolean response to the identity verification request. The client agent supplies the biometrics data collected from the user along with the user information data to the AUA. The AUA responds with the Boolean answer received from the AAS verifying the claimant (whether "the user is who he/she claims to be").

3.2 System Architecture

Our system for continuous presence verification involves capturing test-taker fingerprints at random unpredictable intervals using a fingerprint scanning device. These fingerprints are processed by a cloud service. The cloud service acts as an AUA that can leverage Aadhaar service for biometrics verification. Further, it contains a broker component to read/write information from the profile database. This architecture allows seamless integration of fingerprint authentication to any standard online exam web portal. This architecture is shown in Fig. 2.

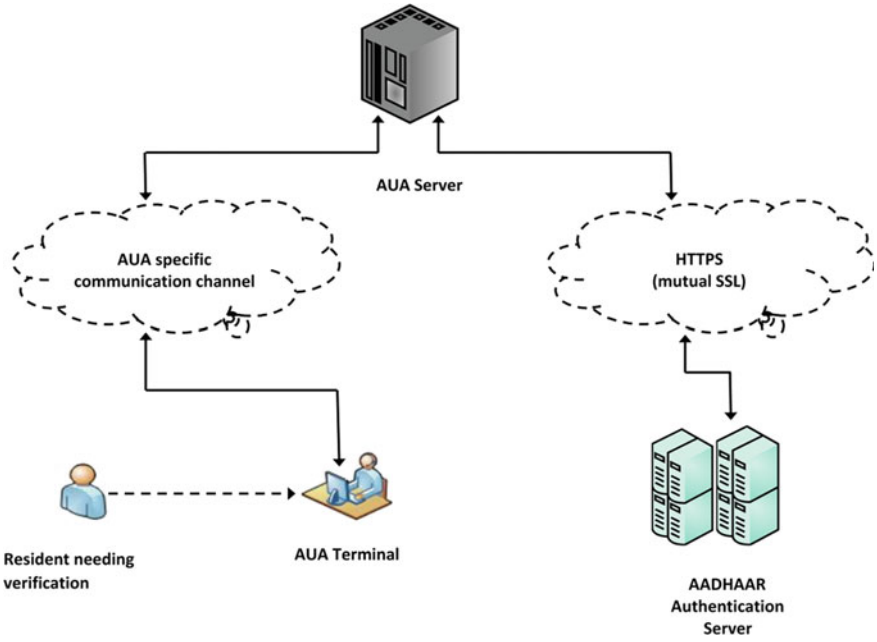

Fig. 1 Aadhaar system architecture

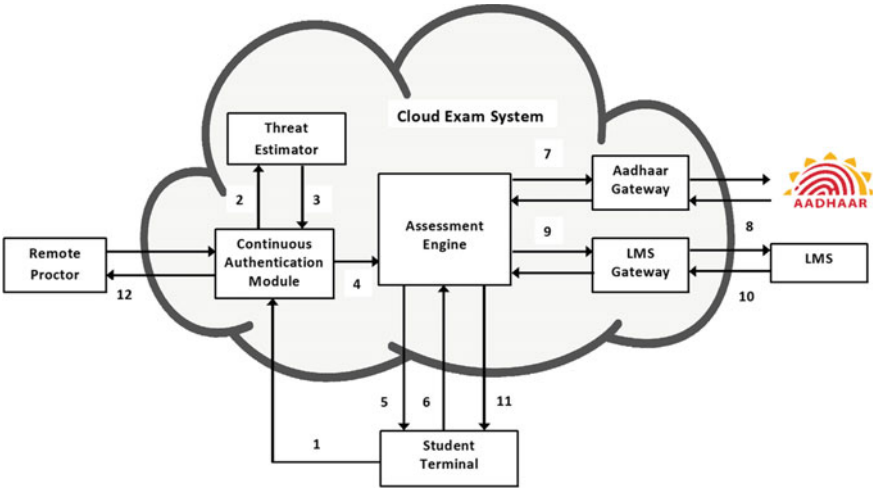

Fig. 2 Proposed system architecture

- Assessment Engine: Responsible for generating assessments that will be delivered to pre-authenticated and verified (by Aadhaar-LMS system) test-takers.
- Continuous Verification: Orchestrator for ensuring test-taker's continuous presence for the entire duration of the examination.
- Threat Estimator: Determines whether a re-verification request is necessary based on the client inputs.
- Aadhaar Gateway: Acts as the AUA middleware entity (ref. Fig. 1) responsible for managing the interaction with the Aadhaar cloud.
- LMS Gateway: Supplies the middleware necessary to connect to various test-taker profile databases (e.g., Moodle, A-VIEW [18], etc.).

The runtime interaction between the modules is as given below:

1. The video feed via webcam is fed into the continuous verification module by the client agent. Other parameters such as keystrokes or mouse movement pattern could also be used.
2. The Threat Estimator module builds a model of the test-taker's behavior obtained from the client agent. The threat estimator determines whether a re-verification request is needed. As explained before, in our current system, we have implemented this using a simple random interval to make the re-verification requests unpredictable.
3. When the continuous verification module determines re-verification is needed, it notifies the assessment engine to perform the actual verification step.
4. The user is prompted for a fingerprint scan by the client agent. In a proctored setting, we could use this step to alert the proctor to check the test-taker. The fingerprint scan method helps move toward a proctor-less examination solution.
5. The fingerprint data is passed back to the assessment engine by the client agent.
6. The assessment engine sends the obtained credential data to the Aadhaar Gateway acting as an AUA.
7. The Aadhaar Gateway makes a verification request to the Aadhaar Service (AAS). In the request, the test-taker's personal information obtained from the LMS is passed along with the biometric data collected for verification.
8. The return value is a Yes or No Boolean value which is passed back to the orchestrator.
9. Optionally, the assessment engine could notify the LMS about the re-verification and the results of re-verification.
10. The LMS system stores the supplied re-verification event as part of the test-taker's assessment history.
11. The client agent is notified of the result. If the re-verification request fails, and instructor/proctor alerting is issued for manual verification.

4 Conclusion

In this paper, we have proposed a continuous presence verification system that can be reliably implemented to guarantee high degree of examination integrity. By capturing test-taker biometrics at unpredictable intervals and validating them via the national Aadhaar service, we have shown that it is possible to reduce and eventually completely eliminate the dependency on remote proctor. Our system can be implemented using off-the-shelf components. We are currently working to validate our prototype in several university-level trials.

5 Future Work

Instead of using random unpredictable intervals, a threat model [6] could be built to decide when a re-verification is really necessary. This could help reduce distraction. Behavior of the system under miscalibrated biometric devices is an area that deserves closer attention. Offline mode that can work with partial unavailability of Aadhaar Service is another interesting area of study.

References

1. Perera-Diltz, D., Moe, J.: Formative and summative assessment in online education. J. Res. Innovat. Teach. **7**(1), 130–142 (2014)
2. Ardid, M., Gómez-Tejedor, J.A., Meseguer-Dueñas, J.M., Riera, J., Vidaurre, A.: Online exams for blended assessment. study of different application methodologies. Comput. Educat. **81**, 296–303 (2015)
3. Fask, A., Englander, F., Wang, Z.: Do online exams facilitate cheating? an experiment designed to separate possible cheating from the effect of the online test taking environment. J. Acad. Ethics **12**(2), 101–112 (2014)
4. Harmon, O.R., Lambrinos, J., Buffolino, J.: Assessment design and cheating risk in online instruction. Online J. Dist. Learn. Administ. **13**(3), n3 (2010)
5. Apampa, K.M., Wills, G., Argles, D.: User security issues in summative e-assessment security. Int. J. Digit. Soc. **1**(2), 1–13 (2010)
6. Al Solami, E., Boyd, C., Clark, A., Islam, A.K.: Continuous biometric authentication: Can it be more practical? In: 2010 12th IEEE International Conference on High Performance Computing and Communications (HPCC), pp. 647–652. IEEE (2010)
7. Flior, E., Kowalski, K.: Continuous biometric user authentication in online examinations. In: 2010 Seventh International Conference on Information Technology: New Generations (ITNG), pp. 488–492. IEEE (2010)
8. Aadhar Unique Identification Authority of India (uidai)
9. Varma, P.: Building an open identity platform for India. In: 2015 Asia-Pacific Software Engineering Conference (APSEC), pp. 3–3. IEEE (2015)
10. Gil, C., Díaz, G., Castro, M.: Fingerprint identification in lms and its empirical analysis of engineer students' views. In: 2010 IEEE Education Engineering (EDUCON), pp. 1729–1736. IEEE (2010)

11. Wildes, R.P.: Iris recognition: an emerging biometric technology. Proc. IEEE **85**(9), 1348–1363 (1997)
12. Kryterion Global Testing Solutions. http://www.kryteriononline.com
13. Clarke, N.L., Dowland, P., Furnell, S.M.: e-invigilator: a biometric-based supervision system for e-assessments. In: 2013 International Conference on Information Society (i-Society), pp. 238–242. IEEE (2013)
14. Prathish, S., Bijlani, K., et al.: An intelligent system for online exam monitoring. In: International Conference on Information Science (ICIS), pp. 138–143. IEEE (2016)
15. Krishnamoorthy, S., Soman, K.: Implementation and comparative study of image fusion algorithms. Int. J. Comput. Appl. **9**(2) (2010)
16. Gonzalez, N., Calot, E.P., Ierache, J.S.: A replication of two free text keystroke dynamics experiments under harsher conditions. In: 2016 International Conference of the Biometrics Special Interest Group (BIOSIG), pp. 1–6. IEEE (2016)
17. Asha, S., Chellappan, C.: Authentication of e-learners using multimodal biometric technology. In: International Symposium on Biometrics and Security Technologies, 2008. ISBAST 2008, pp. 1–6. IEEE (2008)
18. Subramanian, N.S., Anand, S., Bijlani, K.: Enhancing e-learning education with live interactive feedback system. In: Proceedings of the 2014 International Conference on Interdisciplinary Advances in Applied Computing. p. 53. ACM (2014)
19. Apampa, K.M., Wills, G., Argles, D.: An approach to presence verification in summative e-assessment security. In: 2010 International Conference on Information Society (i-Society), pp. 647–651. IEEE (2010)