Συγκριτική Συνάθροιση Ηλεκτρονικών Αξιολογήσεων στην Ανοικτή και εξ Αποστάσεως Εκπαίδευση

Comparative e-Evaluations Gathering in Open and Distance Learning

Γεράσιμος Κ. Μελετίου
Α.Τ.Ε.Ι. Ηπείρου
gmelet@teiep.gr

Σταμάτιος-Άγγελος Ν. Αλεξανδρόπουλος
Πανεπιστήμιο Πατρών
Τμήμα Μαθηματικών
alekst@math.upatras.gr

Μιχαήλ Ν. Βραχάτης
Πανεπιστήμιο Πατρών
Τμήμα Μαθηματικών
vrahatis@math.upatras.gr

Abstract

Evaluation plays an important role in education, as it enables to extract qualitative and quantitative conclusions by the purpose of upgrading the educational process. In open and distance learning web technologies have been used quite enough. Moreover, the usage of various computer systems enables efficient processing of large amounts of data. In this context online techniques have been proposed for educational evaluation, emanating from the area of cryptography, which ensures the integrity of the evaluation process, providing anonymity to all participants. In this paper, we propose the usage of e-evaluation protocols in order to perform comparative e-evaluations gathering.

Περίληψη

Η αξιολόγηση παίζει σημαντικό ρόλο στην εκπαίδευση, καθώς δίνει τη δυνατότητα να εξάγουμε ποιοτικά και ποσοτικά συμπεράσματα με γνώμονα την αναβάθμιση της εκπαιδευτικής διαδικασίας. Στην ανοικτή και εξ αποστάσεως εκπαίδευση χρησιμοποιείται αρκετά η τεχνολογία του διαδικτύου. Επίσης, η χρήση διάφορων υπολογιστικών συστημάτων παρέχει τη δυνατότητα για αποτελεσματική επεξεργασία μεγάλου όγκου δεδομένων. Σε αυτά τα πλαίσια έχουν προταθεί τεχνικές για την απ' ευθείας (online) εκπαιδευτική αξιολόγηση, που προέρχονται από το χώρο της κρυπτογραφίας, κάτι που εξασφαλίζει το αδιάβλητο της διαδικασίας της αξιολόγησης, παρέχοντας ανωνυμία σε όλους τους συμμετέχοντες. Σε αυτή την εργασία προτείνουμε τη χρήση πρωτοκόλλων ηλεκτρονικής αξιολόγησης με στόχο την συγκριτική συνάθροιση των ηλεκτρονικών αξιολογήσεων.

Εισαγωγή

Ο ρόλος της αξιολόγησης για τη σύγχρονη εκπαίδευση είναι δεδομένος. Δεν νοείται εκπαιδευτική διαδικασία χωρίς αξιολόγηση. Αυτό φυσικά ισχύει και για την Ανοικτή και εξ Αποστάσεως Εκπαίδευση (ΑεξΑΕ). Αν λάβουμε υπόψη μας τη γεωγραφική απόσταση εκπαιδευτικών (Σ.Ε.Π.)-φοιτητών, την ανομοιογένεια του φοιτητικού σώματος του Ανοικτού Πανεπιστημίου (εργαζόμενοι σε διάφορους τομείς, άτομα με οικογενειακές υποχρεώσεις, ηλικιωμένοι, απόφοιτοι μέσης εκπαίδευσης με διαφορετικές υποδομές, άτομα με ειδικές ανάγκες κλπ.), συμπεραίνουμε ότι είναι απαραίτητη η λεπτομερής καταγραφή της απόδοσης του εκπαιδευτικού έργου. Τα πράγματα είναι πιο απλά στη συμβατική εκπαίδευση μέσα στην αίθουσα ή στο αμφιθέατρο, όπου ο έλεγχος και η αξιολόγηση της εκπαιδευτικής διαδικασίας είναι ευκολότερος. Στην εργασία (Laskari

E.C., *et al.* 2005a) έχει διατυπωθεί η ιδέα της χρήσης σχημάτων ηλεκτρονικών εκλογών (e-voting) για την ηλεκτρονική αξιολόγηση (e-evaluation) για την ΑεξΑΕ και προβάλλονται τα πλεονεκτήματα της ηλεκτρονικής αξιολόγησης, ο ασύγχρονος χαρακτήρας της και η συμβατότητα της με την ΑεξΑΕ, αφού πρόκειται για αξιολόγηση από απόσταση. Επίσης περισσότερα αποτελέσματα αναφέρονται στις εργασίες (Galanis V.I., *et al.* 2009, Meletiou G.C., *et al.* 2011). Η ηλεκτρονική αξιολόγηση (e-evaluation) αποδεικνύεται ότι αποτελεί μια σύγχρονη αξιολογητική διαδικασία για την κοινωνία της πληροφορίας και γενικότερα των επικοινωνιών και του διαδικτύου. Στην παρούσα εργασία περιγράφεται ένα σχήμα ηλεκτρονικής αξιολόγησης με πολλούς αξιολογητές και πολλούς αξιολογούμενους, που προσφέρεται για σύγκριση μεταξύ των αξιολογήσεων. Στηρίζεται σε κρυπτογραφικά πρωτόκολλα που επιτρέπουν τη Στατιστική Ανάλυση και την Εξόρυξη Δεδομένων σε κρυπτογραφημένα δεδομένα (privacy preserving Statistical Data Analysis, privacy preserving Data Mining) (Drosatos G. & Efraimidis P.S. 2011, Du W., *et al*. 2004, Du W. & Atallah M.J., 2001, Agrawal R. & Srikant R., 2000, Laskari E.C., *et al*. 2005b, Lindell Y. & Pinkas B., 2002). Τέλος, για τη σύγκριση ανάμεσα στα αντικείμενα αξιολόγησης προτείνεται η Order Preserving Encryption (Agrawal R., *et al.* 2004, Boldyreva A., *et al.* 2009, Boldyreva A., *et al.* 2011).

Αντικείμενα Ηλεκτρονικής αξιολόγησης

Σύμφωνα με την εργασία (Laskari E.C., *et al.* 2005b) έχουμε αξιολογητές και αντικείμενα αξιολόγησης. Χαρακτηριστικά αναφέρουμε:

- Οι φοιτητές αξιολογούν το εκπαιδευτικό υλικό κάποιας Θεματικής Ενότητας (Θ.Ε).
- Οι εκπαιδευτικοί κρίνουν το εκπαιδευτικό έργο ενός καθηγητή (Μέλους Σ.Ε.Π.) σε κάποια Θ.Ε.
- Οι εκπαιδευτικοί αξιολογούν το πολυμεσικό εκπαιδευτικό υλικό.
- Οι φοιτητές αξιολογούν την ποιότητα των διοικητικών υπηρεσιών σε κάποιο Α.Ε.Ι.
- Ένας εξωτερικός κριτής (Επιστήμονας διεθνούς κύρους) αξιολογεί ο εκπαιδευτικό έργο ενός τμήματος ή μιας σχολής Α.Ε.Ι.
- Ένα μέλος εκλεκτορικού σώματος αξιολογεί το ερευνητικό και διδακτικό έργο ενός υποψηφίου μέλους Δ.Ε.Π. ή Σ.Ε.Π.

Ηλεκτρονική αξιολόγηση (e-evaluation)

Κατά κάποιον τρόπο έχουμε ένα σύνολο αξιολογητών (π.χ. τα μέλη ενός εκλεκτορικού) και ένα σύνολο αντικειμένων αξιολόγησης (π.χ. υποψήφια μέλη Σ.Ε.Π.). Τα αντικείμενα αξιολόγησης $\{X_1,\ldots,X_N\}$ είναι γραμμές σε κάποιο δημόσιο πίνακα ανακοινώσεων (Public Board) και οι αξιολογητές $\{A_1,\ldots,A_M\}$ οι στήλες του ίδιου πίνακα.

	A_1	A_2	A_3	…	A_M
X_1	V_{11}	V_{12}	V_{13}	…	V_{1M}
X_2	V_{21}	V_{22}	V_{23}	…	V_{2M}

…	…	…	…	…	…
X_N	V_{N1}	V_{N2}	V_{N3}	…	V_{NM}

Κάθε γραμμή του πίνακα περιέχει όλες τις αξιολογήσεις για το ίδιο αντικείμενο αξιολόγησης (π.χ. τις απόψεις των κριτών $\{A_1,\ldots,A_M\}$ για το ερευνητικό έργο του Χημικού τμήματος). Με V_{ij} παριστάνουμε την κρίση του A_j κριτή για το X_i αντικείμενο αξιολόγησης. Σύμφωνα με το (Laskari E.C. *et al.* 2005b) το V_{ij} μπορεί να περιέχει:

- Ποσοτικά Δεδομένα (π.χ. βαθμολογίες, αριθμό εργασιών, h-factor κλπ.).
- Αξιολογήσεις τύπου ΝΑΙ/ΟΧΙ (δηλαδή ένα bit).
- Επιλογή μεταξύ 1,2,…,L περιπτώσεων.
- Κ επιλογές από L περιπτώσεις.
- Ταξινομημική επιλογή Κ μεταξύ L περιπτώσεων.
- Επιλογή 1-L-K. Οι κριτές επιλέγουν ένα σύνολο από L περιπτώσεις και εν συνεχεία από αυτό το σύνολο επιλέγουν Κ περιπτώσεις.
- Δομημένη επιλογή. Υπάρχουν n πιθανά επίπεδα και οι αξιολογητές μετακινούνται από το πρώτο επίπεδο στο τελευταίο.
- Επιλογή με καταγραφή. Πρόκειται για την προαναφερθείσα περίπτωση, σύμφωνα με την οποία ο κάθε αξιολογητής απλώς καταγράφει μια άποψη.

Με άλλα λόγια το V_{ij} είναι μια ποσότητα πληροφορίας σε μορφή «πίνακα» ή «διανύσματος» που περιέχει αριθμητικά δεδομένα, ποιοτικά δεδομένα, δεδομένα διάταξης κλπ. Για το αντικείμενο αξιολόγησης X_i είναι λογικό να γίνει συμψηφισμός των αξιολογήσεων $V_{i1},V_{i2},\ldots,V_{iM}$ και να καταλήξουμε στο S_i που προκύπτει από στατιστική ανάλυση των $V_{i1},V_{i2},\ldots,V_{iM}$. Το S_i είναι ο «μέσος» βαθμός που αντιστοιχεί στο X_i. Είναι μια ποσότητα πληροφορίας που περιέχει μέσους όρους, διαμέσους, διακυμάνσεις, στατιστικά συμπεράσματα, με άλλα λόγια είναι η συνολική εικόνα του αντικειμένου αξιολόγησης.

Κρυπτογραφημένα πρωτόκολλα ηλεκτρονικής αξιολόγησης

Προφανώς η εξαγωγή του S_i πρέπει να ικανοποιεί τις προϋποθέσεις που αναφέρονται στο (Laskari E.C. *et al.* 2005a):

- Η κατάθεση κάθε άποψης να είναι μυστική.
- Μόνο εξουσιοδοτημένοι αξιολογητές μπορούν να καταθέσουν άποψη.
- Κάθε αξιολογητής αξιολογεί μόνο μια φορά.
- Τα αποτελέσματα της αξιολόγησης παραμένουν μυστικά μέχρι το τέλος της αξιολογητικής διαδικασίας.
- Ο αξιολογητής δεν εκχωρεί το δικαίωμα για αξιολόγηση σε τρίτους.

Κατά συνέπεια, μπορεί να γίνει e-evaluation με τη χρήση κάποιου πρωτοκόλλου ηλεκτρονικής ψηφοφορίας (e-voting). Στην προκειμένη περίπτωση είναι προτιμότερο να χρησιμοποιηθούν σχήματα από «ομομορφική κρυπτογράφηση» (homomorphic encryption) (Sako K. & Kilian J. 1994, Hirt M. & Sako K. 2000). Κατ' αυτόν τον τρόπο είναι εφικτή η στατιστική ανάλυση σε κρυπτογραφημένα δεδομένα. Η διαδικασία περιλαμβάνει τα εξής βήματα:

1) Κάθε αξιολογητής A_j αξιολογεί το X_i και διαμορφώνει την άποψη V_{ij}.
2) Ο A_j κρυπτογραφεί την V_{ij}, $W_{ij}=Encr(V_{ij})$ και στη συνέχεια υπογράφει την W_{ij} με την ψηφιακή του υπογραφή. Την υπογεγραμμένη κρυπτογραφημένη άποψη $\mathbf{W_{ij}}=(W_{ij}, Sign_{Aj}, (W_{ij}))$ την ανακοινώνει στην i-γραμμή και j-στήλη του δημόσιου πίνακα ανακοινώσεων (Public Board).
3) Με τη βοήθεια του δημοσίου αλγορίθμου υπολογίζονται τα $Ti=Encr(S_i)$, όπου S_i είναι η συνολική άποψη των M αξιολογητών για τον Ai. Το Si προκύπτει από τη στατιστική ανάλυση δεδομένων πάνω στα V_{ij} και υπολογίζεται σε κρυπτογραφημένη μορφή σαν $T_i=Encr(S_i)$ από τα W_{ij}. Αυτά καταχωρούνται σε μια επί πλέον στήλη στον πίνακα ανακοινώσεων αμέσως μετά τις στήλες των αξιολογητών.
4) Κάθε αξιολογούμενος επαληθεύει όλες τις ψηφιακές υπογραφές των αξιολογητών στον πίνακα ανακοινώσεων. Επίσης, επαληθεύει όλες τις τιμές T_k που υποτίθεται ότι προκύπτουν από τα W_{kj}.
5) Κάθε αξιολογούμενος X_i υπολογίζει το S_i από το T_i και βλέπει τη συνολική άποψη των αξιολογητών γι' αυτόν.

Για την επιτυχία του παραπάνω σχήματος απαιτείται για κάθε αξιολογούμενο Xi ένα σχήμα με κλειδιά $PRIV_i$, PUB_i που να επιτρέπει την ομομορφική κρυπτογράφηση. Ο υπολογισμός του W_{ij} γίνεται με το δημόσιο κλειδί PUB_i και ο υπολογισμός του Si με το ιδιωτικό κλειδί $PRIV_i$. Μέσα στις απαιτήσεις για το σχήμα θα είναι φυσικά το ανέφικτο της ανάκτησης του V_{ij} από το W_{ij} καθώς και το εφικτό του υπολογισμού του S_i από το T_i. Τέλος, η πιστοποίηση του T_i γίνεται είτε από την επαλήθευση όλων των υπογραφών στα W_{ij} είτε από κάποιο σχήμα του τύπου homomorphic signature scheme. Υπολογίζεται έτσι μια υπογραφή σ_i από τα $\{Sign_{Aj}(W_{ij})\}_{1\le j\le M}$ που επαληθεύεται στο T_i, δηλαδή το $\mathbf{T_i}=(T_i,\sigma_i)$ είναι υπογεγραμμένο κείμενο. Μπορούμε αν θέλουμε στην τελευταία στήλη να έχουμε τα $\mathbf{T_i}$ αντί τα T_i. Για βιβλιογραφία αναφορικά με τις homomorphic signatures παραπέμπουμε στην εργασία (Boneh D. & Freeman D. 2011).

	A_1	A_2	A_3	…	A_M	
X_1	$\mathbf{W_{11}}$	$\mathbf{W_{12}}$	$\mathbf{W_{13}}$	…	$\mathbf{W_{1M}}$	$\mathbf{T_1}$
X_2	$\mathbf{W_{21}}$	$\mathbf{W_{22}}$	$\mathbf{W_{23}}$	…	$\mathbf{W_{2M}}$	$\mathbf{T_2}$
…	…	…	…	…	…	…
X_N	$\mathbf{W_{N1}}$	$\mathbf{W_{N2}}$	$\mathbf{W_{N3}}$	…	$\mathbf{W_{NM}}$	$\mathbf{T_N}$

Πιθανά προβλήματα

Αναφέρουμε τα παρακάτω προβλήματα:

1) Δύο αντικείμενα αξιολόγησης X_{i1} και X_{i2} θέλουν να συγκριθούν χωρίς να αποκαλυφθούν οι αντίστοιχες συνολικές αξιολογήσεις S_{i1} και S_{i2} (π.χ. το ερευνητικό έργο του τμήματος Χημείας του Πανεπιστημίου Πατρών με το ερευνητικό έργο του τμήματος Χημείας της Αθήνας).
2) Από $X_{i1},\ldots,X_{iL}$ αντικείμενα αξιολόγησης θέλουμε να επιλέξουμε αυτό που έχει τα πιο πολλά προσόντα και παράλληλα να μη δώσουμε το δικαίωμα στα υπόλοιπα

να πουν ότι έχουν αδικηθεί χωρίς να αποκαλύψουμε τα προσόντα τους $S_{i1},\ldots,S_{iL}$ (από L υποψήφια μέλη Δ.Ε.Π. θέλουμε να επιλέξουμε έναν).

3) Το παραπάνω πρόβλημα αν θέλουμε να εκλέξουμε από L αξιολογούμενους τους K καλύτερους, $1 \leq K < L$.

Όμως τα παραπάνω προβλήματα μπορούν επιτυχώς να αντιμετωπιστούν χρησιμοποιώντας ένα Order Preserving Encryption Scheme (Agrawal R., *et al.* 2004, Boldyreva A., *et al.* 2009).

Επίλογος

Η εκπαιδευτική αξιολόγηση διαδραματίζει σημαντικό ρόλο στη σύγχρονη εκπαίδευση, καθώς συμβάλλει στην ποιοτική αναβάθμιση και εξέλιξη της εκπαιδευτικής διαδικασίας. Ο μεγάλος όγκος πληροφοριών που επεξεργάζονται τα σύγχρονα υπολογιστικά συστήματα καθώς και το διαδίκτυο, δίνουν τη δυνατότητα μέσω της ηλεκτρονικής αξιολόγησης να μπορεί να προσεγγιστεί σε μεγάλο βαθμό η κλασική συμβατική αξιολόγηση. Επίσης, διασφαλίζοντας μέσω της ανωνυμίας όλους τους συμμετέχοντες κάνουν τη διαδικασία αρκετά αποδοτικότερη σε σχέση με την κλασική αξιολόγηση. Έτσι είμαστε σε θέση να δώσουμε στην ανοικτή και εξ αποστάσεως εκπαίδευση τη δυνατότητα για συγκριτική συνάθροιση αξιολογήσεων, προσδίδοντας ένα ακόμα πλεονέκτημα ούτως ώστε να βελτιωθεί το παρεχόμενο εκπαιδευτικό έργο.

Αναφορές

Agrawal, R., Srikant, R. (2000). Privacy-preserving data mining. In *Proc. of the ACM SIGMOD Conference on Management of Data,* pp. 439-450, ACM Press.

Agrawal, R., Kiernan, J., Srikant, R., Xu, Y.-R. (2004). Order Preserving Encryption for Numeric Data. In *Proc. of the ACM SIGMOD Conference on Management of Data,* pp. 3-11, ACM Press.

Boldyreva, A., Chenette, N., Lee, Y., O'Neill, A. (2009). 'Order-Preserving Symmetric Encryption', A. Joux, (eds), *Eurocrypt 2009*, LNCS 5479, pp. 224-241.

Boldyreva, A., Chenette, N., Lee, Y., O'Neill, A. (2011). 'Order-Preserving Symmetric Revisited: Improved Security Analysis and Alternative Solutions', P. Rogaway, (eds), *CRYPTO 2011*, LNCS 6841, pp. 578-595.

Boneh, D., Freeman, D. (2011). 'Homomorphic Signatures for Polynomial Functions', K.G. Paterson, (eds), *Eurocrypt 2011*, LNCS 6632, pp.149-168.

Drosatos, G., Efraimidis, P.S. (2001). Privacy-Preserving Statistical Analysis on Ubiquitous Health Data. In *Proc. of 8th international conference on Trust, privacy and security in digital business*, pp. 24-36.

Du, W., Atallah, M.J., (2001). Privacy-Preserving Cooperative Statistical Analysis. In *Proc. of Computer Security Applications Conference*, ACSAC, pp. 102-110.

Du, W., Han, Y.S., Chen, S. (2004). Privacy-Preserving Multivariate Statistical Analysis: Linear Regression and Classification. In *Proc. of 4th SIAM International Conference on Data Mining*, pp. 222-233.

Galanis, V.I., Laskari, E.C., Meletiou, G.C., Vrahatis, M.N. (2009). E-evaluation in open and distance learning environments. In *Proc. of the International Conference on Information Technologies, (InfoTech 2009)*, Varna, Bulgaria, pp. 28-33.

Hirt, M., Sako, K. (2000). 'Efficient receipt-free voting based on homomorphic encryption'. In *Proc. of Advances in Cryptology--EUROCRYPT'00*, pp. 539-556.

Laskari, E.C., Meletiou, G.C., Stergiou, E., Vrahatis, M.N. (2005a). Electronic eva-luation in open and distance education (in Greek). In *Proc. of the Third International Conference on Open and Distance Learning (ICODL '05)*, Hellenic Open University, A. Lionarakis, (eds), Vol. 1, pp. 497-507, Propobos, Greece.

Laskari, E.C., Meletiou, G.C., Tasoulis, D.K., Vrahatis, M.N. (2005b). Privacy preserving electronic data gathering. *Mathematical and Computer Modelling*, Vol. 42, pp. 739-746.

Lindell, Y., Pinkas, B. (2002). Privacy preserving data mining. *Journal of Cryptology,* 15 (3), pp. 177-206.

Meletiou, G.C., Vasileiadis, D., Stergiou, E., Vrahatis, M.N. (2011). Dynamic Self-Evaluation in O.D.L., (in Greek). In *Proc. of the Sixth International Conference on Open and Distance Learning (ICODL '11),* Hellenic Open University, Loutraki, Greece A. Lionarakis, (eds), 'Alternative Forms in Education', pp. 85-90.

Sako, K., Kilian, J. (1994). 'Secure voting using partially compatible homomorphisms'. Advances in Cryptology - CRYPTO '94, Lecture Notes in Computer Science, Springer-Verlag.