Ασφαλείς Υπολογισμοί Πολλών Μερών σε περιβάλλοντα νέφους και Διαδικτύου των Πραγμάτων

Κωνσταντίνα Παϊταρίδου
ΑΜ: mai20048

Επιβλέπουσα καθηγήτρια: Δρ. Πετρίδου Σοφία
Π.Μ.Σ. στην Εφαρμοσμένη Πληροφορική, Πανεπιστήμιο Μακεδονίας, Νοέμβριος 2021

Περιεχόμενα

- Ασφαλής Υπολογισμός Πολλών Μερών (SMC)
- Διαφορετικές προσεγγίσεις για την εφαρμογή του SMC
- Υπολογιστική στις Παρυφές του Δικτύου
- Ενσωμάτωση της Υπολογιστικής στις Παρυφές του Δικτύου στο 5G
- Μελέτη Περίπτωσης του πρότζεκτ SUNFISH για ασφαλή αποθήκευση δεδομένων στο cloud
- Μελέτη Περίπτωσης ανάλυσης δεδομένων με διατήρηση απορρήτου για αξιολόγηση και αντιμετώπιση οικονομικών ανισοτήτων
- Παρουσίαση της μελέτης περίπτωσης για την αντιμετώπιση οικονομικών ανισοτήτων

Ασφαλής Υπολογισμός Πολλών Μερών

$$f(x_1,\ldots,x_n) = y$$

Ιδιωτικές είσοδοι των οντοτήτων $P_1,\ldots,P_n$

Δημόσιο αποτέλεσμα της συνάρτησης

Διαφορετικές προσεγγίσεις για την εφαρμογή του SMC

- Πρωτοεμφανίστηκε ως Ασφαλής Υπολογισμός δύο Μερών (2PC) το 1982 από τον Andrew Yao, το λεγόμενο ‘Πρόβλημα των Εκατομμυριούχων’.
- Το 1987, οι Goldreich, Micali και Widgerson περιγράφουν λεπτομερώς την πρώτη γενική λύση του Ασφαλούς Υπολογισμού Πολλών Μερών. Η λύση τους βασίζεται στο Διαμοιρασμό Απορρήτων (Secret Sharing).
- Η ολοκληρωμένη λύση παρουσιάστηκε από τον Adi Shamir το 1979 και έκτοτε θεωρείται μια θεμελιώδης κρυπτογραφική τεχνική.

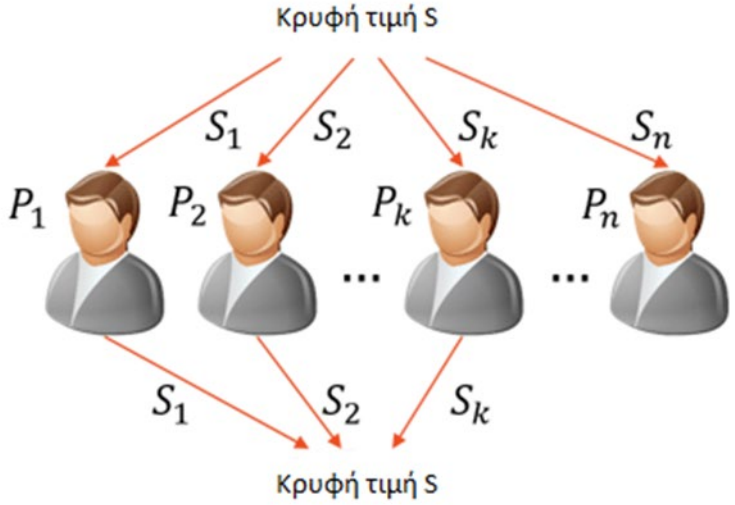
Έστω ότι S: κρυφή ακέραια τιμή που θέλουμε να διαμοιράσουμε στα άτομα P_1,P_2

Ο P_1 λαμβάνει έναν τυχαίο αριθμό $s_1 = r$

Ο P_2 λαμβάνει $s_2 = S - r$

$S = s_1 + s_2 \Rightarrow$

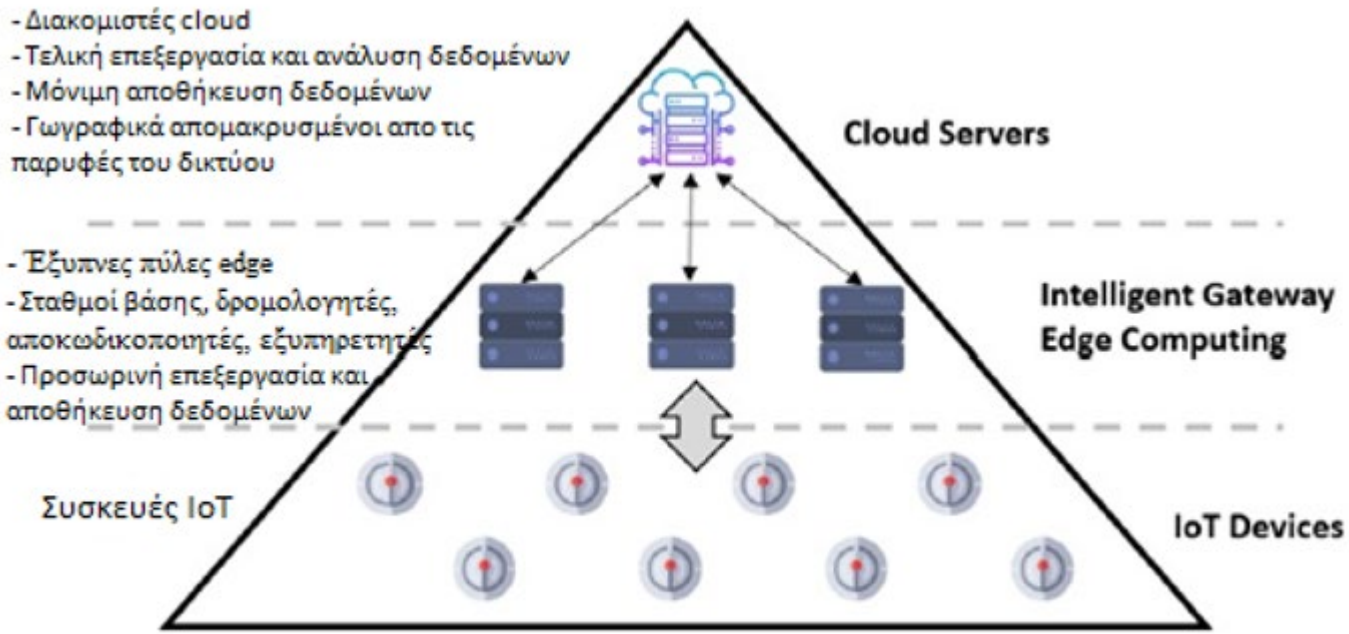
$S = r + S - r = S$



Υπολογιστική στις Παρυφές του Δικτύου

- Ο SMC είναι μια τεχνική που μπορεί να χρησιμοποιηθεί για την υιοθέτηση της ασφαλούς επεξεργασίας δεδομένων σε ένα υπολογιστικό νέφος.
- Η διαδεδομένη εφαρμογή του IoT έχει δημιουργήσει μια κατάσταση στην οποία οι συσκευές που βρίσκονται στις παρυφές του δικτύου να δημιουργούν τεράστιες ποσότητες δεδομένων αυξάνοντας τη χρήσης του δικτύου για τη μεταφορά των δεδομένων αυτών για επεξεργασία στο cloud, που μέχρι την προηγούμενη δεκαετία επεξεργάζονταν από το υπολογιστικό νέφος (Cloud Computing - CC).
- Επίλυση αποτελέσει η Υπολογιστική στις Παρυφές του Δικτύου (Edge Computing - EC) η οποία διαφέρει από το CC. Φέρνει τις υπηρεσίες και τις εφαρμογές του CC πιο κοντά στον τελικό χρήστη καθώς πραγματοποιεί τις διαδικασίες επεξεργασίας των δεδομένων στις παρυφές του δικτύου, που ουσιαστικά αποτελούν την πηγή των παραγόμενων δεδομένων.

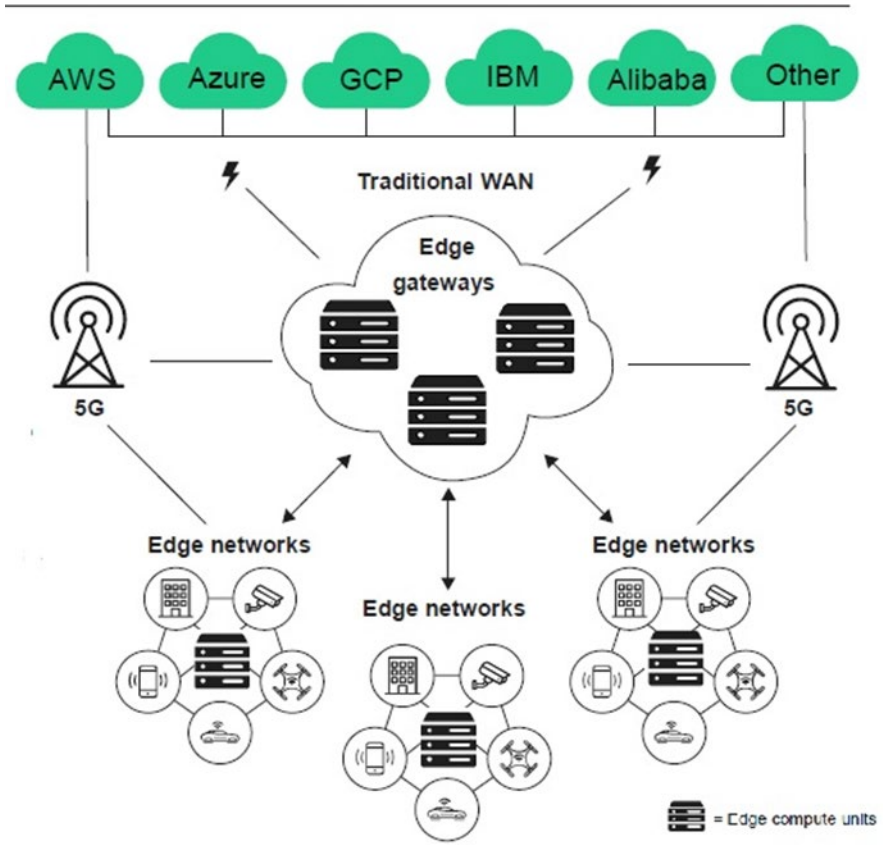
Υπολογιστική στις Παρυφές του Δικτύου



Αρχιτεκτονική της επικοινωνίας IoT συσκεύων που βασίζεται στην τεχνολογία EC

Ενσωμάτωση της Υπολογιστικής στις Παρυφές του Δικτύου στο 5G

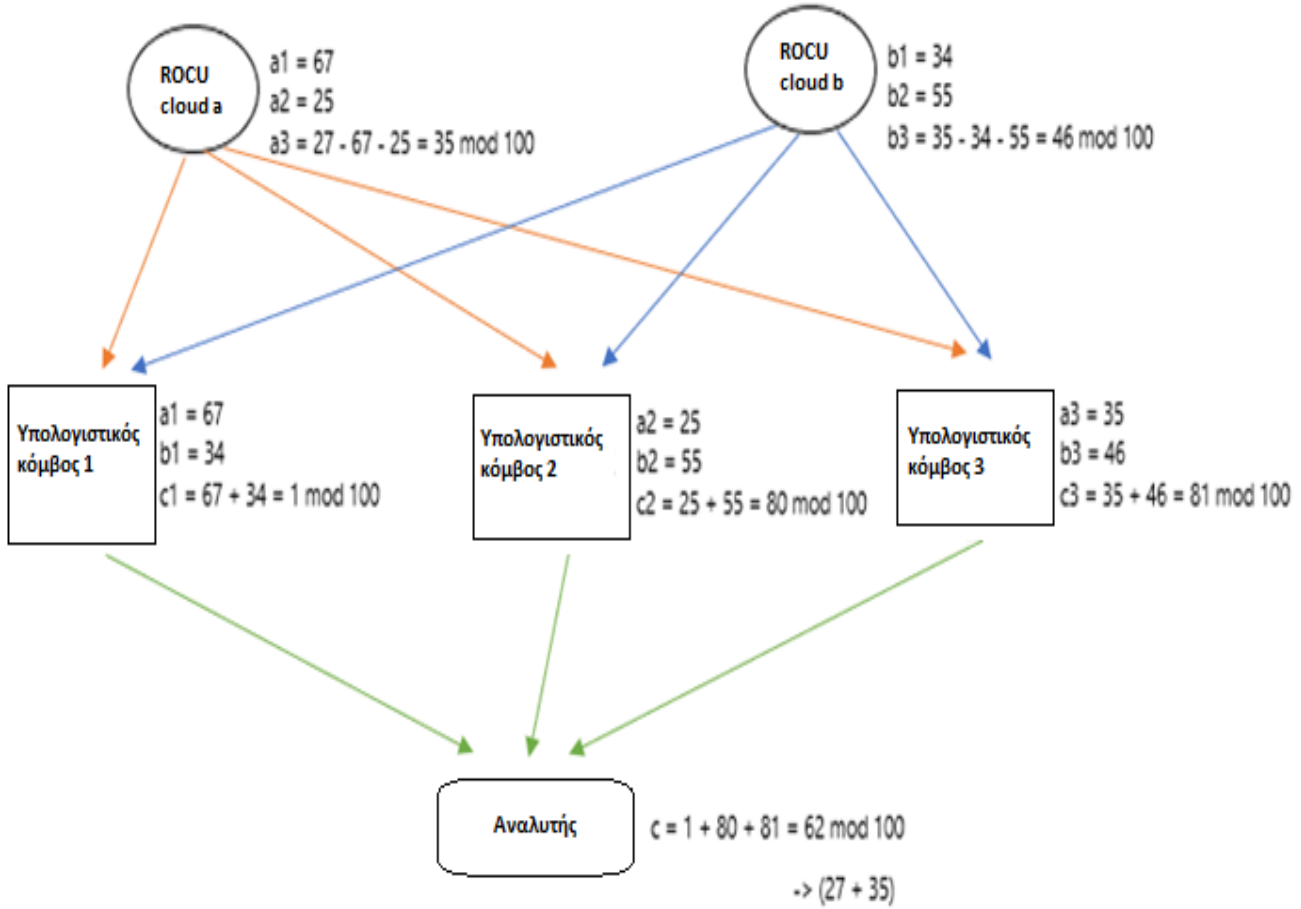
- Αλληλεπίδραση σε πραγματικό χρόνο
- Τοπική επεξεργασία δεδομένων
- Υψηλές ταχύτητες μεταφοράς δεδομένων
- Υψηλή διαθεσιμότητα



Αρχιτεκτονική δομή δικτύου ενσωμάτωσης των τεχνολογιών EC και 5G

Μελέτη Περίπτωσης του πρότζεκτ SUNFISH για ασφαλή αποθήκευση δεδομένων στο cloud

- Το SUNFISH αναπτύσσει μια πλατφόρμα για τις εννέα Περιφερειακές Μονάδες Κυβερνοεγκλήματος (ROCU) που λειτουργούν σε ολόκληρο το Ηνωμένο Βασίλειο και συνεργάζονται σε εθνικό επίπεδο με μεγάλες εγκληματικές μονάδες, για τη δίωξη των παραβατών με έδρα την Ευρώπη.
- Αναπτύσσεται για την ασφαλή ενοποίηση διαφορετικών Cloud διατηρώντας τον έλεγχο στα δεδομένα, αποθηκεύει με ασφάλεια μεγάλες ποσότητες αποδεικτικών στοιχείων για εγκλήματα στον κυβερνοχώρο και ευαίσθητα δεδομένα, με τη χρήση του Ασφαλούς Υπολογισμού Πολλών Μερών (SMC).



Μελέτη Περίπτωσης ανάλυσης δεδομένων με διατήρηση απορρήτου για αξιολόγηση και αντιμετώπιση οικονομικών ανισοτήτων

Μισθολογικό χάσμα της Βοστώνης

1. Συμμετέχουσες εταιρείες που συνεισφέρουν τα ιδιωτικά τους δεδομένα για τον υπολογισμό.
2. Ένας πάροχος υπηρεσιών (διακομιστής) που ονομάζεται και αθροιστής ο οποίος βλέπει μόνο κρυπτογραφημένα δεδομένα, τα αθροίζει και τα αποθηκεύει.
3. Ένας αναλυτής που ονομάζεται και ως έμπιστη οντότητα ο οποίος υπολογίζει το τελικό συνολικό άθροισμα – την έξοδο του υπολογισμού.

Μελέτη Περίπτωσης ανάλυσης δεδομένων με διατήρηση απορρήτου για αξιολόγηση και αντιμετώπιση οικονομικών ανισοτήτων

2 συμμετέχουσες εταιρείες, A και B.

dA = 33 και dB = 14 και προχωρούν ως εξής:

Οι εταιρείες δημιουργούν μια τυχαία μάσκα mA = 63 και mB = 70. Και οι 2 υπολογίζουν τις τιμές των καλυμμένων δεδομένων τους:

rA = dA + mA = 33 + 63 = 96

rB = dB + mB = 14 + 70 = 84

και τα υποβάλλουν στον αθροιστή.

Ο αθροιστής υπολογίζει το R = rA + rB = 96 + 84 = 180 και αποθηκεύει αυτή την ποσότητα.

Η έμπιστη οντότητα μπορεί στη συνέχεια να υπολογίσει το άθροισμα:

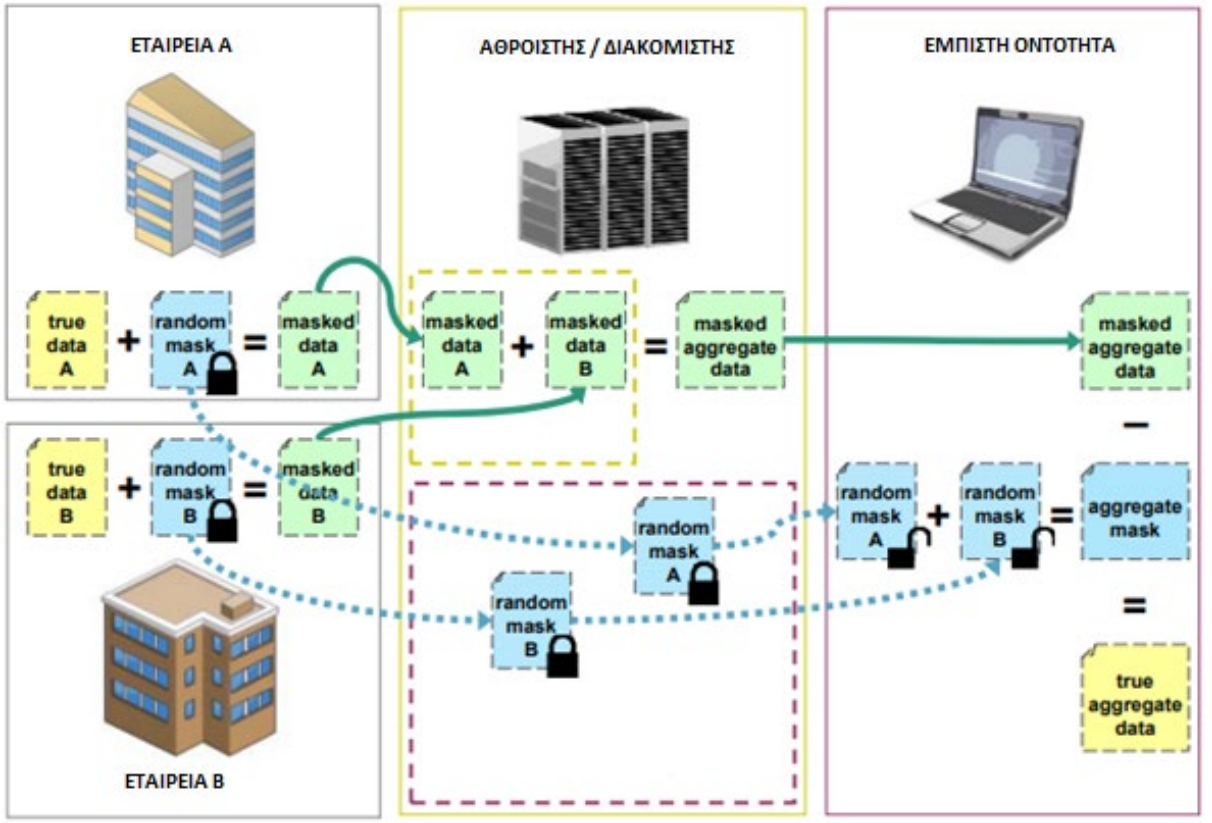
dA + dB = (rA − mA) + (rB − mB)

= (rA + rB) − (mA + mB)

= R − (mA + mB)

= 180 − (63 + 70) = 180 − 133 = 47

Επειδή 33 + 14 = 47, η έμπιστη οντότητα έχει υπολογίσει το άθροισμα.



Ευχαριστώ πολύ για τον χρόνο σας