ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΕΣΣΑΛΙΑΣ

ΣΧΟΛΗ ΘΕΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ

# ΔΙΑΒΑΘΜΙΣΜΕΝΗ ΠΡΟΣΒΑΣΗ ΣΕ ΑΡΧΕΙΑ ΠΡΟΣΩΠΙΚΗΣ ΠΛΗΡΟΦΟΡΙΑΣ

ΝΙΚΟΛΑΟΣ ΜΑΡΙΝΗΣ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

ΥΠΕΥΘΥΝΟΣ

Γεώργιος Λιουδάκης
Λέκτορας (βάσει ΠΔ407/80)

Λαμία 20/10 έτος 2022


ΠΑΝΕΠΙΣΤΗΜΙΟ
ΘΕΣΣΑΛΙΑΣ

ΣΧΟΛΗ ΘΕΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ

# ΔΙΑΒΑΘΜΙΣΜΕΝΗ ΠΡΟΣΒΑΣΗ ΣΕ ΑΡΧΕΙΑ ΠΡΟΣΩΠΙΚΗΣ ΠΛΗΡΟΦΟΡΙΑΣ

ΝΙΚΟΛΑΟΣ ΜΑΡΙΝΗΣ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

ΥΠΕΥΘΥΝΟΣ

Γεώργιος Λιουδάκης
Λέκτορας (βάσει ΠΔ407/80)

Λαμία 20/10 έτος 2022


UNIVERSITY OF
THESSALY

SCHOOL OF SCIENCE

DEPARTMENT OF COMPUTER SCIENCE & TELECOMMUNICATIONS

# GRADED ACCESS IN PERSONAL INFORMATION FILES

NICHOLAOS MARINIS

FINAL THESIS

ADVISOR

Georgios Lioudakis
Lecturer (based on PD407/80)

Lamia 20/10 year 2022

*«Με ατομική μου ευθύνη και γνωρίζοντας τις κυρώσεις [(1)], που προβλέπονται από της διατάξεις της παρ. 6 του άρθρου 22 του Ν. 1599/1986, δηλώνω ότι:*

*1. Δεν παραθέτω κομμάτια βιβλίων ή άρθρων ή εργασιών άλλων αυτολεξεί **χωρίς να τα περικλείω σε εισαγωγικά** και χωρίς να αναφέρω το συγγραφέα, τη χρονολογία, τη σελίδα. Η αυτολεξεί παράθεση χωρίς εισαγωγικά χωρίς αναφορά στην πηγή, είναι λογοκλοπή. Πέραν της αυτολεξεί παράθεσης, λογοκλοπή θεωρείται και η παράφραση εδαφίων από έργα άλλων, συμπεριλαμβανομένων και έργων συμφοιτητών μου, καθώς και η παράθεση στοιχείων που άλλοι συνέλεξαν ή επεξεργάσθηκαν, χωρίς αναφορά στην πηγή. Αναφέρω πάντοτε με πληρότητα την πηγή κάτω από τον πίνακα ή σχέδιο, όπως στα παραθέματα.*

*2. Δέχομαι ότι η αυτολεξεί **παράθεση χωρίς εισαγωγικά**, ακόμα κι αν συνοδεύεται από αναφορά στην πηγή σε κάποιο άλλο σημείο του κειμένου ή στο τέλος του, είναι αντιγραφή. Η αναφορά στην πηγή στο τέλος π.χ. μιας παραγράφου ή μιας σελίδας, δεν δικαιολογεί συρραφή εδαφίων έργου άλλου συγγραφέα, έστω και παραφρασμένων, και παρουσίασή τους ως δική μου εργασία.*

*3. Δέχομαι ότι υπάρχει επίσης περιορισμός στο μέγεθος και στη συχνότητα των παραθεμάτων που μπορώ να εντάξω στην εργασία μου εντός εισαγωγικών. Κάθε μεγάλο παράθεμα (π.χ. σε πίνακα ή πλαίσιο, κλπ), προϋποθέτει ειδικές ρυθμίσεις, και όταν δημοσιεύεται προϋποθέτει την άδεια του συγγραφέα ή του εκδότη. Το ίδιο και οι πίνακες και τα σχέδια*

*4. Δέχομαι όλες τις συνέπειες σε περίπτωση λογοκλοπής ή αντιγραφής.*

Ημερομηνία: 29/9/2022

Ο Δηλ.

*(1) «Όποιος εν γνώσει του δηλώνει ψευδή γεγονότα ή αρνείται ή αποκρύπτει τα αληθινά με έγγραφη υπεύθυνη δήλωση*
*του άρθρου 8 παρ. 4 Ν. 1599/1986 τιμωρείται με φυλάκιση τουλάχιστον τριών μηνών. Εάν ο υπαίτιος αυτών των πράξεων*
*σκόπευε να προσπορίσει στον εαυτόν του ή σε άλλον περιουσιακό όφελος βλάπτοντας τρίτον ή σκόπευε να βλάψει άλλον, τιμωρείται με κάθειρξη μέχρι 10 ετών.»*

# ΠΕΡΙΛΗΨΗ

Η προσωπική πληροφορία αποτελεί σημαντικό κομμάτι στην διατήρηση αλλά και ανάπτυξη προσωπικών σχέσεων. Ως μελέτη περίπτωσης στα πλαίσια της πτυχιακής εργασίας επιλέχθηκε η επιτήρηση μέσω καμερών κλειστού κυκλώματος. Επομένως, κρίνεται απαραίτητη η διασφάλισή της με τεχνολογίες ελέγχου πρόσβασης. Έτσι λοιπόν, έγινε ανάπτυξη ενός συστήματος θόλωσης προσώπων σε πραγματικό χρόνο με όνομα «RT_FaceBlur», το οποίο παρέχει διαβαθμισμένη πρόσβαση στην πληροφορία όποτε χρειάζεται, βασισμένο στο μοντέλο ελέγχου πρόσβασης βάσει ιδιοτήτων. Με το πέρας της προδιαγραφής του συστήματος, χρησιμοποιήθηκε ήδη υπάρχουσα τεχνολογία για την αναγνώριση προσώπων βασισμένη στον αλγόριθμο Viola-Jones και γύρω από αυτήν αναπτύχθηκε τεχνολογία ελέγχου πρόσβασης πάνω στην γλώσσα προγραμματισμού Python, με την χρήση κατάλληλων εργαλείων που αυτή προσφέρει. Το σύστημα θα παρέχει στον χρήστη την πληροφορία που καταγράφεται από τα συστήματα παρακολούθησης μόνο όποτε γίνει ορθή επαλήθευση των απαραίτητων χαρακτηριστικών του χρήστη. Ακόμη και με ορθή επαλήθευση του βαθμού εξουσιοδότησης, το σύστημα είναι σε θέση να αναγνωρίζει και να καταγράφει τις πληροφορίες του συνδεδεμένου χρήστη έτσι ώστε να πραγματοποιηθεί επίτευξη ευθύνης και διασφάλιση της ακεραιότητας της προσωπικής πληροφορίας των ατόμων που καταγράφονται.

## ABSTRACT

Personal information is an important part of maintaining and developing personal relationships. In the confines of this thesis, surveillance through closed-circuit television was chosen as a case study. It is therefore deemed necessary to protect it with the use of access control technologies. As a result, a real-time face blurring system named “RT_FaceBlur” was developed, which provides graded access to information whenever needed, based on the attribute-based access control model. After the system specifications were defined, an already existing technology for face recognition was used based on the Viola-Jones algorithm, and along with that, an access control technology was developed based on the Python programming language, using the appropriate tools it offers. The system will provide the user with the information recorded by the surveillance systems only when the necessary user attributes are verified. Even with authentication of the necessary clearance level, the system is able to recognize and record the information of the logged-in user so as to achieve accountability and ensure the integrity of the personal information of the people being recorded.

Table of Contents

# ΠΙΝΑΚΑΣ ΣΧΗΜΑΤΩΝ

# ΠΙΝΑΚΑΣ ΣΥΝΤΟΜΟΓΡΑΦΙΩΝ

| Συντομογραφίες | Ορισμός |
|---|---|
| DAC | Discretionary Access Control |
| MAC | Mandatory Access Control |
| RBAC | Role-Based Access Control |
| ABAC | Attribute-Based Access Control |
| Η.Π.Α | Ηνωμένες Πολιτείες Αμερικής |
| CCTV | Closed-Circuit Television |
| A.I. | Artificial Intelligence |
| HLM | Hierarchical Linear Modelling |
| WDQ | Weighted Displacement Quotient |
| ΓΚΠΔ | Γενικός Κανονισμός Προστασίας Δεδομένων |
| OOPSLA | Object-Oriented Programming, Systems, Languages and Applications |
| UML | Unified Modelling Language |
| GUI | Graphical User Interface |
| BSD | Berkeley Software Distribution |
| API | Application Programming Interface |
| IP | Internet Protocol |
| CSV | Comma-Separated Values |
| HDF5 | Hierarchical Data Format 5 |
| SQL | Structured Query Language |
| ID | Identification |

# ΚΕΦΑΛΑΙΟ 1 Εισαγωγή

Η κοινή διαχείριση προσωπικών δεδομένων έχει γίνει ένα σημαντικό ζήτημα στην κοινωνία μας. Τα υποκείμενα των δεδομένων αυτών είναι σχεδόν πάντα απρόθυμα ως προς τον διαμοιρασμό των δεδομένων τους, για λόγους ασφάλειας και απορρήτου. Υπάρχει φόβος κατάχρησης των δεδομένων τους εις βάρος της προσωπικής τους ζωής, θέτοντας σε κίνδυνο ένα από τα βασικά ανθρώπινα δικαιώματά τους. Αυτή η ανησυχία των υποκειμένων έχει πολλαπλασιαστεί στην σύγχρονη εποχή λόγω της ραγδαίας ανάπτυξης νέων τεχνολογιών για την ακόμα ποιο βελτιωμένη συλλογή και διαχείριση προσωπικών δεδομένων (Chatterjee & Sreenivasulu N.S., 2019).

Με την εμφάνιση όλο και περισσότερων εξελισσόμενων τεχνολογιών όπως το Δικτύο των Πραγμάτων, τα «Μεγάλα Δεδομένα» και την Τεχνητή Νοημοσύνη, οι διάφοροι οργανισμοί είναι πλέον σε θέση να εξάγουν αναρίθμητα ψηφιοποιημένα δεδομένα προσωπικής πληροφορίας (Cavoukian, Chibba, Williamson and Ferguson, 2015). Αυτή η συλλογή και ανταλλαγή των δεδομένων είναι αναπόφευκτη στην σύγχρονη εποχή, οπότε αποτελεί επιτακτική ανάγκη η ορθή διαχείριση των δεδομένων αυτών με την εξέλιξη και την εφαρμογή μοντέλων ελέγχου πρόσβασης καθώς και με την ενσωμάτωση πολιτικών προστασίας απορρήτου από τον σχεδιασμό των διάφορων τεχνολογιών. Οι πολιτικές αυτές οφείλουν να είναι προληπτικές, να έχουν το απόρρητο ως προεπιλεγμένη ρύθμιση με ενσωμάτωση αυτού στον σχεδιασμό καθώς και να παρέχουν ορατότητα και διαφάνεια τις λειτουργίας τους με επίκεντρο τον χρήστη (Cavoukian, 2010). Επιπρόσθετα, η διαβαθμισμένη πρόσβαση κρίνεται αναγκαία για κάθε σύστημα συλλογής πληροφορίας ώστε να ελαχιστοποιηθεί η κακομεταχείριση των δεδομένων, «Οποιαδήποτε παραβίαση και ρήξη ασφάλειας, περιλαμβάνει παράνομη πρόσβαση σε ορισμένους πόρους, συστήματα, δεδομένα ή λειτουργίες. Σε αυτό το πλαίσιο, η εξέλιξη των πολιτικών ασφάλειας έχει φέρει τον έλεγχο πρόσβασης στον πυρήνα της ασφάλειας, αλλά και της προστασίας της ιδιωτικής ζωής» (Papagiannakopoulou et al., 2014). Έλεγχος πρόσβασης είναι η διαδικασία με την οποία ο χρήσης θα αποκτήσει πρόσβαση σε διάφορους πόρους που παρέχει το σύστημα, μόνο αν αυτός έχει την κατάλληλη εξουσιοδότηση. Βασικές ομάδες ελέγχου πρόσβασης αποτελούν (Capitani di Vimercati, Samarati and Sandhu, 2014):

- Διακριτός έλεγχος πρόσβασης ή DAC.
- Υποχρεωτικός έλεγχος πρόσβασης ή MAC.
- Έλεγχος πρόσβασης βάσει ρόλων ή RBAC.
- Έλεγχος πρόσβασης βάσει ιδιοτήτων ή ABAC.

## Σκοπός της Πτυχιακής Εργασίας 1.1

Σκοπό αυτής της εργασίας αποτελεί η ανάπτυξη ενός συστήματος, το οποίο θα διασφαλίζει την ακεραιότητα της ιδιωτικότητας των πολιτών που καταγράφονται από κάμερες παρακολούθησης, μέσω της ικανοποίησης απαιτήσεων και διαβαθμισμένης πρόσβασης. Το σύστημα θα αναπτυχθεί βάσει του μοντέλου ελέγχου πρόσβασης ABAC, ώστε να επιτευχθεί διαβαθμισμένη πρόσβαση στην προσωπική πληροφορία βάσει δύο κύριων χαρακτηριστικών, την εξουσιοδότηση του χρήστη και τον περιβαλλοντικό παράγοντα. Ειδικότερα, θα γίνεται αίτηση από τον χρήστη για να αποκτήσει πρόσβαση στην προσωπική πληροφορία των πολιτών που καταγράφονται από το σύστημα, μόνο όταν έχει καταγραφεί ένα περιστατικό και αφού γίνουν οι κατάλληλοι έλεγχοι και ο χρήστης έχει επαρκή εξουσιοδότηση θα πραγματοποιηθεί πρόσβαση στην πληροφορία. Βασικά κομμάτια αυτού του μοντέλου ελέγχου πρόσβασης αποτελούν το Policy Enforcement Point και Policy Decision Point (Capitani di Vimercati, Samarati and Sandhu, 2014). Στα πλαίσια της πτυχιακής εργασίας υλοποιήθηκε Policy Enforcement Point στο σύστημα που αναπτύχθηκε, το οποίο είναι μια λογική οντότητα ή ένα μέρος στο σύστημα, το οποίο πραγματοποιεί τον έλεγχο αποδοχής όταν ο χρήστης κάνει αίτηση για να αποκτήσει πρόσβαση στα δεδομένα.

# Κάμερες Παρακολούθησης 1.2

Η εποπτεία στον χώρο εργασίας υπήρχε πάντα με διάφορες μορφές και σκοπούς, όμως οι καινούργιες τεχνολογίες επιτρέπουν ένα νέο είδος ηλεκτρονικής επιτήρησης, πιο αδιάκριτο από πριν (Doberstein, Charbonneau, Morin and Despatie, 2021). Τέτοιες τεχνολογίες αποτελούν η τεχνητή νοημοσύνη, μέσω της οποίας δίνεται η δυνατότητα παρακολούθησης της χρήσης του διαδικτύου, καθώς και η ανάγνωση μηνυμάτων ηλεκτρονικού ταχυδρομείου (Doberstein, Charbonneau, Morin and Despatie, 2021). Όμως το κλασικό εργαλείο παρακολούθησης, η βιντεοκάμερα, συνεχίζει να επεκτείνεται σε χώρους εργασίας με ολοένα μεγαλύτερη ανάλυση και δυνατότητες, όπως είναι η αναγνώριση προσώπου. Γεγονός που διευκολύνει την συλλογή πληροφοριών ενός ατόμου, την κακομεταχείριση και κατάχρηση αυτών των δεδομένων (Cavallaro, 2007).

Κύριο και πρόσφατο παράδειγμα τέτοιας συλλογής πληροφορίας και κακομεταχείρισης αποτελούν οι πράξεις της εταιρίας «Clearview AI». Η εταιρία εδρεύετε στις Η.Π.Α και αποτελεί πλατφόρμα αναγνώρισης προσώπων, επιτρέποντας έτσι στους χρήστες της να κάνουν αναζήτηση και μέσω της βάσης δεδομένων της εταιρίας να βρίσκουν εικόνες τους που υπάρχουν στο διαδίκτυο (ΑΠΔ, 2022). Η εταιρία «Clearview AI» χρησιμοποιεί τεχνολογία «web scrapping» για την συλλογή δημοσιευμένων εικόνων από το διαδίκτυο, καθώς και άλλων πληροφοριών όπως η γεωμετρική τοποθεσία των ατόμων (ΑΠΔ, 2022). Επιπρόσθετα, έκανε επεξεργασία και χρήση των δεδομένων, χωρίς να ενημερώσει τα άτομα των οποίων συλλέγει τις πληροφορίες (ΑΠΔ, 2022). Λόγω αυτών, η Αρχή Προστασίας Δεδομένων έκανε καταγγελία κατά της εταιρίας με την απόφαση 35/2022, επίβαλε πρόστιμο αξίας 20.000.000 ευρώ, απαγόρευσε την συλλογή πληροφορίας των ατόμων εντός της ελληνικής επικράτειας και την διαγραφή των προϋπάρχων δεδομένων που αφορούν αυτούς (ΑΠΔ, 2022).

# ΚΕΦΑΛΑΙΟ 2 Ο Έλεγχος της Ιδιωτικότητας και το Νομικό της Πλαίσιο.

## Έλεγχος Πρόσβασης 2.1

Αποτελεί επιτακτική ανάγκη, για οποιαδήποτε σύστημα διαχείρισης πληροφοριών, η προστασία των πληροφοριών αυτών και η διασφάλιση της εμπιστευτικότητας και της ακεραιότητας (Capitani di Vimercati, Samarati and Sandhu, 2014). Με την τεχνολογία ελέγχου πρόσβασης γίνεται δυνατή η επίτευξη αυτού του στόχου. Χρησιμοποιώντας διαβαθμισμένη πρόσβαση, το σύστημα είναι σε θέση να προστατεύσει την πληροφορία από μη εξουσιοδοτημένη αποκάλυψη των προσωπικών δεδομένων, καθώς και από τις μη εξουσιοδοτημένες ή ακατάλληλες τροποποιήσεις, ενώ ταυτόχρονα διασφαλίζει την διάθεση της πληροφορίας στους εξουσιοδοτημένους χρήστες. Ένα σύστημα υλοποιημένο με έλεγχο πρόσβασης ελέγχει κάθε αίτημα πρόσβασης και καθορίζει εάν αυτό πρέπει να χορηγηθεί ή να απορριφθεί (Capitani di Vimercati, Samarati and Sandhu, 2014). Γενικά, στα συστήματα ελέγχου πρόσβασης, γίνεται διάκριση μεταξύ των πολιτικών, των μοντέλων και των μηχανισμών. Οι πολιτικές καθορίζουν πως θα πραγματοποιείται ο έλεγχος πρόσβασης στο σύστημα, ενώ το μοντέλο θα επισημοποιήσει αυτήν την πολιτική που θα επιβάλλεται από τους μηχανισμούς ελέγχου. Το σύστημα λειτουργεί ως μεσολαβητής ο οποίος συμβουλεύεται μια βάση δεδομένων εξουσιοδότησης για να προσδιορίσει αν ο χρήστης που επιχειρεί να πραγματοποιήσει μια λειτουργία έχει πράγματι την εξουσιοδότηση να την εκτελέσει. Ειδικότερα, οι εξουσιοδοτήσεις σε αυτή τη βάση δεδομένων ορίζονται συνήθως σε σχέση με την ταυτότητα των χρηστών, δηλαδή απαιτείται αρχικά έλεγχος ταυτότητας με σωστή επαλήθευση του χρήστη. Τα διαφορετικά μοντέλα ελέγχου πρόσβασης διακρίνονται σε τέσσερις διαφορετικές ομάδες, DAC, MAC, RBAC και ABAC (Capitani di Vimercati, Samarati and Sandhu, 2014).

### Διακριτός έλεγχος πρόσβασης 2.1.α

Στον διακριτό έλεγχο πρόσβασης, οι πολιτικές πραγματοποιούν τους ελέγχους με βάση την ταυτότητα του χρήστη καθώς και τους κανόνες πρόσβασης που δηλώνουν τις δυνατότητές του (Samarati and Capitani di Vimercati, 2001). Ειδικότερα, οι πολιτικές αυτές αποφασίζουν τι είδους πρόσβαση θα έχει ο χρήστης στην πληροφορία, βάσει της ταυτότητας και της εξουσιοδότησής του, όπου αυτά τα χαρακτηριστικά προσδίδουν για κάθε χρήστη και αντικείμενο στο σύστημα ξεχωριστά, τον τρόπο με τον οποίο επιτρέπεται η πρόσβαση στο σύστημα (Capitani di Vimercati, Samarati and Sandhu, 2014). Επομένως, κάθε αίτημα ενός χρήστη για την πρόσβαση σε πληροφορία, ελέγχεται με μια βάση προκαθορισμένων εξουσιοδοτήσεων και αν ο χρήστης έχει την κατάλληλη εξουσιοδότηση η οποία δίνει σε αυτόν την δυνατότητα πρόσβασης στη πληροφορία σε συγκεκριμένη λειτουργία, τότε το σύστημα χορηγεί την πρόσβαση, αλλιώς την αρνείται. Ύστερα περιγράφεται το μοντέλο του πίνακα πρόσβασης, το οποίο είναι χρήσιμο για την κατανόηση των βασικών αρχών πίσω από τις πολιτικές διακριτού ελέγχου πρόσβασης. Ο πίνακας πρόσβασης είναι ένα εννοιολογικό μοντέλο που προσδιορίζει τα δικαιώματα που έχει κάθε υποκείμενο για το κάθε προστατευόμενο αντικείμενο. Υπάρχει μία γραμμή στον πίνακα για κάθε υποκείμενο και μία στήλη για κάθε αντικείμενο, με κάθε κελί του πίνακα να καθορίζει την πρόσβαση που επιτρέπεται στον χρήστη για το συγκεκριμένο αντικείμενο της στήλης (Capitani di Vimercati, Samarati and Sandhu, 2014). Τέλος ο έλεγχος της πρόσβασης θα πραγματοποιείται βάση των λειτουργιών που προσδίδονται από τον πίνακα πρόσβασης.

**Πίνακας 1.** Παράδειγμα Πίνακα Πρόσβασης. [1]

| | File 1 | File 2 | File 3 | Program 1 |
|---|---|---|---|---|
| **Ann** | own<br>read<br>write | read<br>write | | execute |
| **Bob** | read | | read<br>write | |
| **Carl** | | read | | execute<br>read |

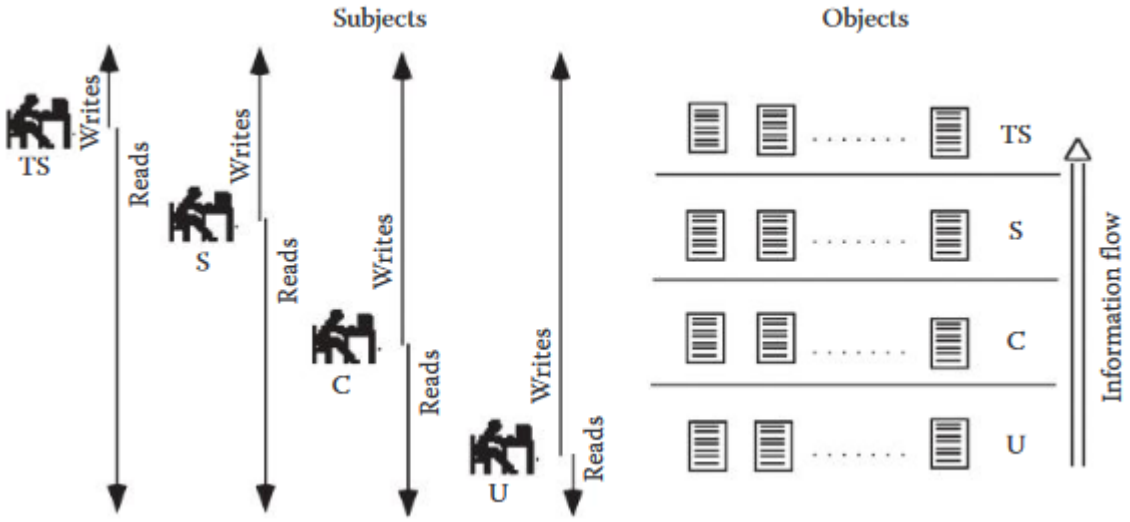
Το διακριτό μοντέλο ελέγχου πρόσβασης παρέχει ευέλικτες πολιτικές διάκρισης, επομένως το καθιστά κατάλληλο για διάφορα συστήματα και εφαρμογές, ειδικά σε εμπορικά και βιομηχανικά περιβάλλοντα (Capitani di Vimercati, Samarati and Sandhu, 2014). Όμως σε αυτού του είδους πολιτικές, δεν διασφαλίζεται πραγματικά η ροή πληροφορίας σε ένα σύστημα. Αποτελεί μειονέκτημα το γεγονός ότι ένας χρήστης έχει την δυνατότητα να παρακάμψει τους περιορισμούς πρόσβασης, καθώς ένας εξουσιοδοτημένος για ανάγνωση χρήστης έχει την δυνατότητα να διαβιβάσει την πληροφορία σε άλλους χρήστες, οι οποίοι δεν έχουν κατάλληλη εξουσιοδότηση (Capitani di Vimercati, Samarati and Sandhu, 2014).

## Υποχρεωτικός έλεγχος πρόσβασης 2.1.β

Ο υποχρεωτικός έλεγχος πρόσβασης βασίζεται σε πολιτικές οι οποίες ελέγχουν την πρόσβαση βάσει κανονισμών οι οποίοι έχουν καθοριστεί από μια κεντρική αρχή (Samarati and Capitani di Vimercati, 2001). Αντίθετα από το διακριτό μοντέλο πρόσβασης, στον υποχρεωτικό έλεγχο η διάδοση πληροφοριών ελέγχεται σε υποχρεωτικά συστήματα αποτρέποντας τη ροή της πληροφορίας από χρήστη με εξουσιοδότηση σε χρήστες χωρίς (Capitani di Vimercati, Samarati and Sandhu, 2014). Στον υποχρεωτικό έλεγχο πρόσβασης, υποκείμενα είναι διαδικασίες που λειτουργούν στην θέση του χρήστη. Κάθε υποκείμενο και κάθε αντικείμενο σε ένα υποχρεωτικό σύστημα έχει μια κλάση πρόσβασης, το οποίο αποτελείται από ένα επίπεδο ασφάλειας και ένα σύνολο κατηγοριών. Το επίπεδο ασφάλειας έχει ιεραρχική δομή, όπου κάθε επίπεδο κυριαρχεί στον εαυτό του καθώς και σε όλα τα επίπεδα κάτω από αυτό στην ιεραρχία. Το σύνολο των κατηγοριών είναι ένα υποσύνολο ενός μη ταξινομημένου συνόλου, του οποίου τα στοιχεία αντικατοπτρίζουν λειτουργίες ή αρμοδιότητες. Αν για παράδειγμα έχουμε σε ένα σύστημα δύο κλάσεις πρόσβασης, τις x1 και x2, όπου η x1 έχει μεγαλύτερο ή ίσο επίπεδο ασφάλειας από την x2, και το σύνολο κατηγοριών της x1 περιλαμβάνουν αυτές της x2 τότε λέμε πως η x1 κυριαρχεί της x2 (Capitani di Vimercati, Samarati and Sandhu, 2014). Ο υποχρεωτικός έλεγχος πρόσβασης έχει δύο κύριες πολιτικές, την πολιτική απορρήτου και την πολιτική ακεραιότητας.

Στην πολιτική απορρήτου, κρίνεται απαραίτητη η προστασία του απορρήτου της πληροφορίας. Σε αυτήν την πολιτική το επίπεδο ασφάλειας που σχετίζεται με ένα αντικείμενο καθορίζει την ευαισθησία της πληροφορίας που εμπεριέχεται σε αυτό, δηλαδή την πιθανή ζημία που θα μπορούσε να προκύψει από την μη εξουσιοδοτημένη πρόσβαση. Επίσης, το επίπεδο ασφαλείας που σχετίζεται με ένα χρήστη, το οποίο ονομάζεται επίσης επίπεδο εξουσιοδότησης προσδίδει την αξιοπιστία του χρήστη όσο αφορά την διαχείριση ευαίσθητης πληροφορίας (Capitani di Vimercati, Samarati and Sandhu, 2014).

[1] Πίνακας από: Samarati and Capitani di Vimercati, (2001).



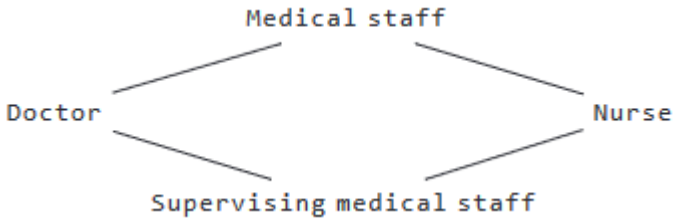

**Σχήμα 1.** Έλεγχος ροής πληροφορίας για την προστασία απορρήτου.[2]

Η πολιτική προστασίας της ακεραιότητας της πληροφορίας, έχει επίπεδα ακεραιότητας τα οποία αντικατοπτρίζουν τον βαθμό εμπιστοσύνης που μπορεί να αποδοθεί στην πληροφορία που είναι αποθηκευμένη αλλά και στον χρήστη, τα οποία καθορίζουν την πιθανή ζημιά που θα προκύψει από την μη εξουσιοδοτημένη πρόσβαση και την αξιοπιστία του χρήστη για την εισαγωγή, τροποποίηση ή και διαγραφή της πληροφορίας αντίστοιχα (Capitani di Vimercati, Samarati and Sandhu, 2014).

## Έλεγχος πρόσβασης βάσει ρόλων 2.1.γ

Στον έλεγχο πρόσβασης βάσει ρόλων, οι πολιτικές ελέγχουν την πρόσβαση ανάλογα με τους ρόλους που έχουν οι χρήστες του συστήματος καθώς και με κανόνες που δηλώνουν τι επίπεδο πρόσβασης επιτρέπεται στον εκάστοτε χρήστη ανάλογα με τον ρόλο του (Samarati and Capitani de Vimercati, 2001). Απαιτείται ο προσδιορισμός των ρόλων στο σύστημα, όπου ένας ρόλος μπορεί να οριστεί ως ένα σύνολο ενεργειών και ευθυνών που σχετίζονται με μια συγκεκριμένη εργασιακή δραστηριότητα (Capitani di Vimercati, Samarati and Sandhu, 2014). Ύστερα, αντί να προσδιορίζονται όλες οι λειτουργίες που μπορεί να εκτελεί ο κάθε χρήστης ξεχωριστά, αυτές προσδιορίζονται στους ρόλους που θα λάβουν οι χρήστες. Αυτό απλοποιεί σημαντικά την διαδικασία επεξεργασίας των ιδιοτήτων του εκάστοτε χρήστη καθώς γίνεται μια απλή αλλαγή ρόλου ανάλογα με τις ιδιότητες που οφείλει να έχει ο χρήστης. Γενικά, ένας χρήστης μπορεί να αναλάβει διαφορετικούς ρόλους σε διαφορετικές περιπτώσεις, όπως επίσης γίνεται να έχουν πολλοί διαφορετικοί χρήστες τον ίδιο ρόλο ταυτόχρονα (Capitani di Vimercati, Samarati and Sandhu, 2014). Ανάλογα με το σύστημα ο χρήστης μπορεί να έχει πολλούς ρόλους ταυτόχρονα ή μόνο ένα ρόλο κάθε φορά. Ένα RBAC μοντέλο είναι οργανωμένο σε τέσσερα κομμάτια. Το βασικό RBAC, όπου πραγματοποιείται η ανάθεση των ρόλων. Το ιεραρχικό RBAC, το οποίο καθορίζει την ιεραρχία των ρόλων, όπου οι ρόλοι παραπάνω στην ιεραρχία κληρονομούν τις ιδιότητες κατώτερων ρόλων. Τον στατικό διαχωρισμό καθηκόντων, όπου επιβάλλονται περιορισμοί στην ανάθεση ρόλων στους χρήστες και τέλος, τον δυναμικό διαχωρισμό καθηκόντων, όπου επιβάλλονται περιορισμοί κατά το χρόνο εκτέλεσης (Capitani di Vimercati, Samarati and Sandhu, 2014).

[2] Σχήμα από: Samarati and Capitani di Vimercati, (2001).




**Σχήμα 2.** Παράδειγμα ιεραρχίας ρόλων.[3]

### Έλεγχος πρόσβασης βάσει ιδιοτήτων 2.1.δ

Σε σενάρια όπου ένα σύστημα παρέχει υπηρεσίες σε όποιον τις χρειάζεται, όπως είναι για παράδειγμα ένα υπολογιστικό νέφος, δεν επαρκεί η υιοθέτηση ενός βασικού μοντέλου ελέγχου πρόσβασης. Καθώς το αίτημα πρόσβασης μπορεί να προέρχεται από άγνωστους χρήστες, οι πολιτικές ελέγχου πρόσβασης που βασίζονται στην ταυτότητα του χρήστη δεν μπορούν να υλοποιηθούν. Επομένως υλοποιήθηκε ένα καινούργιο μοντέλο ελέγχου πρόσβασης, το ABAC, το οποίο παραχωρεί πρόσβαση ανάλογα με τα χαρακτηριστικά του πόρου ή της υπηρεσίας και τα χαρακτηριστικά του χρήστη που πραγματοποιεί την αίτηση (Capitani di Vimercati, Samarati and Sandhu, 2014). Δηλαδή δεν βασίζονται όλες οι αποφάσεις για την καταχώρηση πρόσβασης στην ταυτότητα του χρήστη, αλλά κρίνεται πως ο ρόλος του ή και πως ορισμένα χαρακτηριστικά του είναι πιο σημαντικά από την ταυτότητά του για την καταχώρηση πρόσβασης.

## Κάμερες παρακολούθησης κλειστού κυκλώματος 2.2

Ένα από τα πιο διαδεδομένα συστήματα διαχείρισης και συλλογής πληροφοριών στην σημερινή εποχή είναι οι κάμερες παρακολούθησης. Η ηλεκτρονική παρακολούθηση επεκτείνετε με ταχύς ρυθμούς στον δημόσιο καθώς και τον ιδιωτικό τομέα. Πολλές χώρες τις χρησιμοποιούν ως πρωταρχικό εργαλείο για την επίβλεψη των μετακινήσεων του πληθυσμού, καθώς και την πρόληψη του εγκλήματος και της τρομοκρατίας (IFSEC Global, 2021). Μέσω της τεχνολογίας Κλειστού Κυκλώματος Τηλεόρασης (CCTV), οι πολίτες καταγράφονται σε καθημερινή βάση σε δημόσια κτήρια, σιδηροδρομικούς σταθμούς, καταστήματα, ανελκυστήρες, ακόμη και σε σχολικούς διαδρόμους. Το Ηνωμένο Βασίλειο μόνο είχε περίπου 1.85 εκατομμύρια κάμερες το 2012 οι οποίες κατέγραφαν τον μέσω πολίτη έως και 70 φορές την ημέρα (We're watching you: 'Britons caught on CCTV 70 times a day', 2012) ενώ σήμερα αυτός ο αριθμός έχει ξεπεράσει της 5.2 εκατομμύρια κάμερες.

[3] Σχήμα από: Capitani di Vimercati, Samarati and Sandhu, (2014).

**Πίνακας 2.** Παράδειγμα πλήθους CCTV σε αστικές περιοχές Ευρώπης.[4]

| Institution | Total N = 100% | CCTV Systems | | Dummy systems | |
|---|---|---|---|---|---|
| (Metro) station | 7 | 7 cases | 100.0% | 0 cases | 0.0% |
| National government building | 1 | 1 | 100.0% | 0 | 0.0% |
| Bank | 70 | 58 | 82.9% | 0 | 0.0% |
| Post office | 5 | 4 | 80.0% | 0 | 0.0% |
| Hotel | 10 | 6 | 60.0% | 0 | 0.0% |
| Shopping mall | 8 | 4 | 50.0% | 0 | 0.0% |
| Public toilet | 2 | 1 | 50.0% | 0 | 0.0% |
| Museum | 2 | 1 | 50.0% | 0 | 0.0% |
| Chain store / Large retailer | 317 | 127 | 40.1% | 16 | 5.0% |
| Prescribing pharmacy | 11 | 4 | 36.4% | 0 | 0.0% |
| Restaurant | 88 | 24 | 27.3% | 0 | 0.0% |
| Pub / Bar / Café | 100 | 24 | 24.0% | 2 | 2.0% |
| Other local authorities | 5 | 1 | 20.0% | 0 | 0.0% |
| Small shop / Corner store / Grocery | 581 | 102 | 17.6% | 31 | 5.3% |
| Cinema / Theatre | 9 | 1 | 11.1% | 0 | 0.0% |
| Public School | 1 | 0 | 0.0% | 0 | 0.0% |
| Police station | 1 | 0 | 0.0% | 0 | 0.0% |
| College / University | 2 | 0 | 0.0% | 0 | 0.0% |
| Religious centre | 6 | 0 | 0.0% | 1 | 16.7% |
| Others | 123 | 24 | 24.0% | 1 | 0.8% |
| Total | 1349 | 389 | 28.8% | 51 | 3.8% |

## Τρόπος λειτουργίας καμερών 2.2.α

Την τελευταία δεκαετία έχουν πραγματοποιηθεί θεμελιώδεις αλλαγές, οι οποίες μεταμόρφωσαν τις δυνατότητες των συστημάτων βίντεο-επιτήρησης, στον τρόπο με τον οποίο συλλέγονται, αναλύονται, μοιράζονται αλλά και αποθηκεύονται τα ψηφιακά δεδομένα. Οι κάμερες ασφαλείας διαδραματίζουν ήδη καθοριστικό ρόλο στις «Έξυπνες Πόλεις», καθώς και στο αναπτυσσόμενο βιομηχανικό διαδίκτυο. Μέσω της χρήσης τεχνολογιών Βαθιάς Μάθησης (Deep learning) και της τεχνητής νοημοσύνης (Α.Ι.) οι κάμερες είναι σε θέση να συλλέγουν με μεγαλύτερη ακρίβεια δεδομένα και να κάνουν προβλέψεις με βάση το εκάστοτε ενσωματωμένο αναλυτικό λογισμικό που έχουν αναπτύξει οι κατασκευαστές. Μέσω αυτών, οι βιντεοκάμερες κατέχουν πλέον τεχνολογίες αναγνώρισης προσώπου. Η αναγνώριση προσώπου μπορεί να μειώσει δραστικά την ανωνυμία στην παρακολούθηση βίντεο με αλγοριθμική ανάλυση εικόνων σε μια βάση δεδομένων (Doberstein, Charbonneau, Morin and Despatie, 2021). Η δυνατότητα αναγνώρισης και πρόσβασης σε ευαίσθητη πληροφορία των πολιτών μέσω την συλλογή δεδομένων έχει οδηγήσει στην δημιουργία συζητήσεων

[4] Πίνακας από: Hempel and Töpfer, (2004).

για τα ζητήματα απορρήτου σε δικαστικές διαδικασίες (Doberstein, Charbonneau, Morin and Despatie, 2021).

Η χρήση και ενεργοποίηση αναλυτικών στοιχείων πραγματικού χρόνου στις βίντεο-ροές από δημόσιους χώρους μπορεί να είναι πολύτιμη, μόνο εάν τα ζητήματα ιδιωτικότητας μπορούν να αντιμετωπιστούν έχοντας ικανοποιητικά αποτελέσματα. Για παράδειγμα μια σήμανση «Amber Alert» για ένα χαμένο παιδί μπορεί να ενεργοποιήσει την αναγνώριση προσώπου σε πραγματικό χρόνο παράλληλα σε πολλές ροές βίντεο από κοινόχρηστους χώρους, έτσι βοηθώντας στον γρήγορο εντοπισμό του παιδιού. Επιπλέον, μπορούν να επωφεληθούν οι επιχειρήσεις, παραδείγματος χάρη ο έγκαιρος εντοπισμός παγωμένων πεζοδρομίων ωφελεί άμεσα τις ασφαλιστικές εταιρίες, οι οποίες αναλαμβάνουν τον κίνδυνο. Ακόμη, καθιστάτε γρηγορότερη η ανίχνευση εγκληματικής δραστηριότητας. Η πιθανή αξία της τεχνολογίας δημόσιας επιτήρησης αποδείχθηκε τον Απρίλιο του 2013, όταν οι ερευνητές αναγνώρισαν τους δύο ύποπτους για την βομβιστική επίθεση στον Μαραθώνιο της Βοστώνη με την ανάλυση βίντεο που κατέγραψαν οι κάμερες της πόλης (IFSEC Global, 2021). Οι βομβιστές της Βοστώνης συνελήφθησαν γρήγορα χάρη στις κάμερες παρακολούθησης, έχοντας ως αποτέλεσμα την εξασφάλιση της συνεχούς υποστήριξης των καμερών μέσω εγκατάστασης και ανάπτυξης καινούργιων τεχνολογιών για την βελτίωσή τους.

## Στατιστικά καμερών κλειστού κυκλώματος 2.2.β

Σύμφωνα με νέα ανάλυση της «Comparitech», οι πόλεις στην Κίνα βρίσκονται υπό την σκληρότερη CCTV επιτήρηση στον κόσμο (Bischoff, 2022). Οι ερευνητές της εταιρίας συγκέντρωσαν ένα πλήθος από πόρους δεδομένων και αναφορές, συμπεριλαμβανομένων κυβερνητικών αναφορών, ιστοσελίδων της αστυνομίας, και ειδησεογραφικών άρθρων, για να εκτιμήσουν τον αριθμό των CCTV καμερών που χρησιμοποιούνται σε 150 μεγάλες πόλεις σε όλο τον κόσμο εστιάζοντας κυρίως σε δημόσιες κάμερες που χρησιμοποιούνται από κρατικούς φορείς, όπως η επιβολή του νόμου (Bischoff, 2022).


**Σχήμα 3.** Οι περισσότερο εποπτευόμενες πόλεις στον κόσμο, κάμερες ανά 1000 άτομα. [5]

[5] Σχήμα από: Bischoff, (2022).

Με βάση τον δημόσιων καμερών ανά 1.000 άτομα, αυτές είναι οι 25 πιο επιτηρούμενες πόλεις στον κόσμο (Bischoff, 2022):

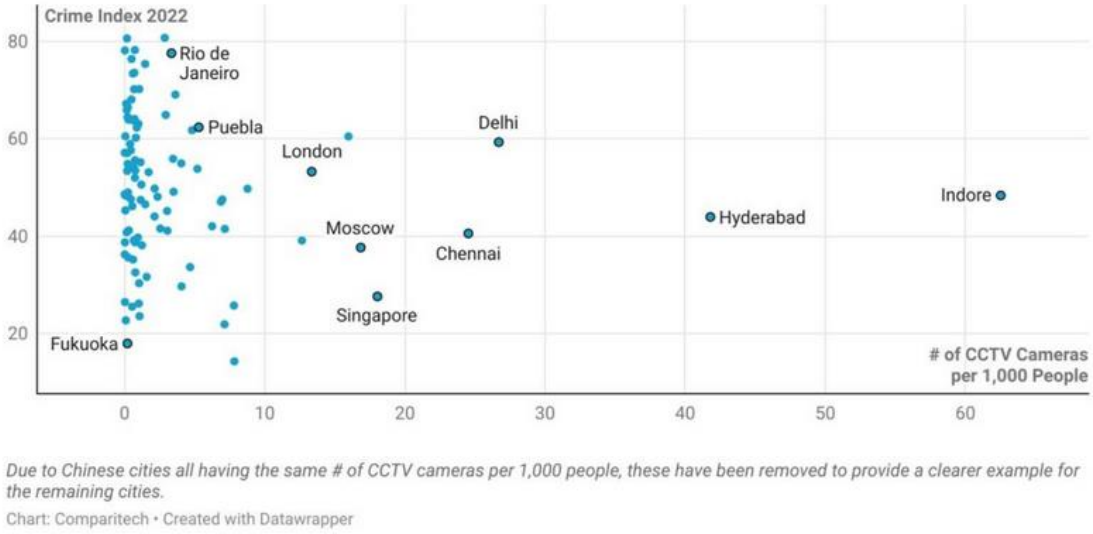
1. Taiwan, Κίνα – 467.255 κάμερες για 3.975.985 άτομα = 117,02 κάμερες ανά 1.000 άτομα.
2. Wuxi, Κίνα – 300.000 κάμερες για 3.315.113 άτομα = 90,49 κάμερες ανά 1.000 άτομα.
3. Indore, Ινδία – 200.600 κάμερες για 3.208.722 άτομα = 62,52 κάμερες ανά 1.000 άτομα.
4. Changsha, Κίνα – 262.000 κάμερες για 4.694.722 άτομα = 55,81 κάμερες ανά 1.000 άτομα.
5. Beijing, Κίνα – 1.150.000 κάμερες για 20.896.820 άτομα = 55,03 κάμερες ανά 1.000 άτομα.
6. Hangzhou, Κίνα – 400.000 κάμερες για 7.845.501 άτομα = 50,98 κάμερες ανά 1.000 άτομα.
7. Qingdao, Κίνα – 262.000 κάμερες για 5.742.486 άτομα = 45,62 κάμερες ανά 1.000 άτομα.
8. Kunming, Κίνα – 200.200 κάμερες για 4.550.831 άτομα = 43,95 κάμερες ανά 1.000 άτομα.
9. Hyderabad, Ινδία – 440.299 κάμερες για 10.534.418 άτομα = 41,8 κάμερες ανά 1.000 άτομα.
10. Xiamen, Κίνα – 150.000 κάμερες για 3.790.792 άτομα = 39,57 κάμερες ανά 1.000 άτομα.
11. Harbin, Κίνα – 250.000 κάμερες για 6.526.439 άτομα = 38,13 κάμερες ανά 1.000 άτομα.
12. Suzhou, Κίνα – 270.000 κάμερες για 7.427.096 άτομα = 36,35 κάμερες ανά 1.000 άτομα.
13. Shanghai, Κίνα – 1.000.000 κάμερες για 27.795.702 άτομα = 35,98 κάμερες ανά 1.000 άτομα.
14. Ürümqi, Κίνα – 160.000 κάμερες για 4.543.684 άτομα = 35,21 κάμερες ανά 1.000 άτομα.
15. Chengdu, Κίνα – 310.000 κάμερες για 9.305.116 άτομα = 33,32 κάμερες ανά 1.000 άτομα.
16. Shenzhen, Κίνα – 400.000 κάμερες για 12.591.696 άτομα = 31,77 κάμερες ανά 1.000 άτομα.
17. Jinan, Κίνα – 160.000 κάμερες για 5.513.597 άτομα = 31,77 κάμερες ανά 1.000 άτομα.
18. Shenyang, Κίνα – 200.000 κάμερες για 7.373.655 άτομα = 27,12 κάμερες ανά 1.000 άτομα.
19. Delhi, Ινδία – 436.600 κάμερες για 16.349.831 άτομα = 26,7 κάμερες ανά 1.000 άτομα.
20. Chennai, Ινδία – 282.126 κάμερες για 11,503,293 άτομα = 24,53 κάμερες ανά 1.000 άτομα.
21. Singapore, Σιγκαπούρη – 108.981 κάμερες για 6.039.577 άτομα = 18.04 κάμερες ανά 1.000 άτομα.
22. Moscow, Ρωσία – 213.000 κάμερες για 12.640.818 άτομα = 16,84 κάμερες ανά 1.000 άτομα.
23. Baghdad, Ιράκ – 120.000 κάμερες για 7.511.920 άτομα = 15,97 κάμερες ανά 1.000 άτομα.
24. London, Αγγλία (Ηνωμένο Βασίλειο) – 127.373 κάμερες για 9.540.576 άτομα = 13,35 κάμερες ανά 1.000 άτομα.
25. St. Petersburgh, Ρωσία – 70.000 κάμερες για 5.535.556 άτομα = 12,65κάμερες ανά 1.000 άτομα.

Οι κάμερες παρακολούθησης εξυπηρετούν πολλούς σκοπούς, από την πρόληψη του εγκλήματος και την παρακολούθηση κυκλοφορίας ως την παρατήρηση βιομηχανικών λειτουργιών σε περιβάλλοντα ακατάλληλα για τον άνθρωπο (Bischoff, 2022). Η ψηφιακή εποχή έχει ενισχύσει την επικράτηση των συστημάτων επιτήρησης. Οι κάμερες γίνονται καλύτερες και φθηνότερες, οι ζωντανές ροές βίντεο επιτρέπουν πρόσβαση άμεσα εξ αποστάσεως και δίνουν την δυνατότητα να αποθηκεύονται στο διαδίκτυο και να μεταδοθούν.

## Κάμερες και Εγκληματικότητα 2.2.γ

Έχοντας λοιπόν ως πρωταρχικό επιχείρημα υπέρ της CCTV παρακολούθησης τη βελτιωμένη επιβολή του νόμου και την πρόληψη του εγκλήματος, αναμένεται μείωσή της εγκληματικότητας. Όμως οι αξιολογήσεις αυτών των προσπαθειών ήταν μικτές. Μια ομάδα ερευνητών αποτελούμενη από τους Jerry H. Ratcliffe, Travis Taniguchi και Ralph B. Taylor πραγματοποίησαν ανάλυση πάνω στα συστήματα καμερών CCTV και την επίπτωση που έχουν στην εγκληματικότητα στην πόλη Φιλαδέλφεια, Η.Π.Α (Ratcliffe, Taniguchi and Taylor, 2009). Η ομάδα χρησιμοποίησε Ιεραρχική

Γραμμική Μοντελοποίηση (HLM), ένα τύπο στατιστικής ανάλυσης που αναγνωρίζει φωλιασμένες δομές δεδομένων καθώς και το Σταθμισμένο Πηλίκο Μετατόπισης (WDQ) (Ratcliffe, Taniguchi and Taylor, 2009). Το WDQ χρησιμοποιείται για να προσδιοριστούν αν οι διαφορές μεταξύ του στόχου και των buffer περιοχών είναι αποτέλεσμα μετατόπισης από την περιοχή στόχο ή διάχυση των οφελών από την χρήση επιτήρησης CCTV στην περιοχή στόχο (Ratcliffe, Taniguchi and Taylor, 2009). Ο προσδιορισμός ενός WDQ απαιτεί αρχικά τον ορισμό τριών περιοχών όπου έχει εγκατασταθεί σύστημα με σκοπό την μείωση της εγκληματικότητας, τον ορισμό μιας buffer περιοχής όπου έχει εκτιμηθεί ότι υπάρχει μεγαλύτερη πιθανότητα εγκληματικής δράσης και μίας περιοχής ελέγχου που λειτουργεί ως έλεγχος τάσεων εγκληματικότητας γενικότερα (Ratcliffe, Taniguchi and Taylor, 2009). Με την ανάλυση των δύο μεθόδων η ομάδα κατέληξε στο συμπέρασμα πως η εφαρμογή των συστημάτων παρακολούθησης είχε ένα αρχικό αποτρεπτικό αποτέλεσμα εντός δύο μηνών μετά την εφαρμογή, με μείωση της εγκληματικότητας κατά 13% συνολικά σε όλες τις περιοχές που έγινε η ανάλυση (Ratcliffe, Taniguchi and Taylor, 2009). Όμως, αυτό το αποτέλεσμα καταστολής του εγκλήματος μειώνεται, καθώς οι πολίτες προσαρμόζονται στην τοποθέτηση της κάμερας, με τις μισές περιοχές στις οποίες έγινε η έρευνα να μην έχει παρατηρηθεί διαφορά μακροπρόθεσμα (Ratcliffe, Taniguchi and Taylor, 2009).




**Σχήμα 4.** Συσχέτιση καμερών και δείκτη εγκληματικότητας.[6]

# Ιδιωτικότητα και Νομικό Πλαίσιο 2.3

## Κάμερες παρακολούθησης και Ιδιωτικότητα 2.3.α

Τα συστήματα καμερών όπως αναφέρθηκε αρχικά εγκαταστάθηκαν με κύριο σκοπό την καταπολέμηση και μείωση της εγκληματικότητας, αλλά αποτελέσματα αναλύσεων όπως της ομάδας Jerry H. Ratcliffe, Travis Taniguchi και Ralph B. Taylor αποδεικνύουν πως δεν αποτελεί ιδανική λύση (Ratcliffe, Taniguchi and Taylor, 2009). Όμως, η ραγδαία ανάπτυξη και συνεχή εγκατάσταση συστημάτων CCTV έχει ως αποτέλεσμα την αυξανόμενη ανησυχία των πολιτών. Ενώ η πλειοψηφία των πολιτών που έλαβαν μέρος σε έρευνες σε όλη την Ευρώπη αρχικά είναι υποστηρικτικοί όταν τους ζητάτε η στάση τους προς τα συστήματα παρακολούθησης, όταν τους ζητάτε ξανά με περισσότερες

[6] Σχήμα από: Bischoff, (2022).

πληροφορίες και λεπτομέρειες, χαράζουν μια ξεκάθαρη γραμμή και αντιτίθενται στα συστήματα επιτήρησης στους ιδιωτικούς χώρους κυρίως (Hempel and Töpfer, 2004) καθώς υπάρχει ανησυχία καταπάτησης της ιδιωτικότητάς τους αλλά και των προσωπικών τους δεδομένων (Goold, 2002). Ειδικότερα στις Η.Π.Α, σε πολλές περιπτώσεις οι κάμερες έχουν εγκατασταθεί χωρίς δημόσια συναίνεση ή δημόσια συζήτηση και έχουν ελάχιστη είτε τυπική είτε άτυπη νομική ρύθμιση (Goold, 2002). Αν υπάρχει υποστήριξη της τοπικής κυβέρνησης η αστυνομία και άλλες αρχές επιβολής του νόμου είναι ελεύθερες να παρακολουθούν δημόσιους χώρους όπως παραδείγματος χάρη δρόμους, πάρκα και εμπορικά κέντρα με ελάχιστο σεβασμό στην ιδιωτικότητα των πολιτών (Goold, 2002). Συνεπώς, οι πολίτες βρίσκονται συχνά σε θέση παρεμβατικής επιτήρησης μέσω καμερών κλειστού κυκλώματος. Ο κάθε πολίτης έχει ανάγκη από ιδιωτικότητα, έστω και ελάχιστη, ώστε να μπορεί να διατηρήσει την αίσθηση αξιοπρέπειας και αυτονομίας στην καθημερινότητά του. Γνωρίζοντας ότι παρακολουθείτε ο πολίτης από σύστημα επιτήρησης δεν αποτελεί το ίδιο με το να γνωρίζει την ταυτότητα του ατόμου που τον παρακολουθεί. Κρίνεται αδύνατο να γνωρίζει από ποιόν παρακολουθείτε από την άλλη πλευρά της κονσόλας και τι επιδίωξη μπορεί να έχει αυτό το πρόσωπο (Goold, 2002). Συνεπώς, τα δικαιώματα απορρήτου κατά την καταγραφή μέσω CCTV αξίζουν προστασία καθώς κρίνονται βασικός πυλώνας της αυτονομίας και της ελευθερίας διατήρησης διαφορετικών κοινωνικών σχέσεων.

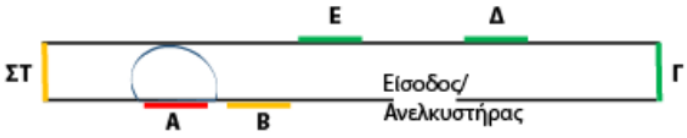
## Νομικό Πλαίσιο 2.3.β

Η επιτήρηση του δημόσιου χώρου αποτελεί πλέον αναπόφευκτο γεγονός με την ραγδαία και συνεχή ανάπτυξη της τεχνολογίας, επομένως αποτελεί επιτακτική ανάγκη η αναθεώρηση των νομικών αλλά και ηθικών πτυχών που περιλαμβάνει η εγκατάσταση συστήματος παρακολούθησης με σκοπό την προστασία της ιδιωτικής ζωής. Επομένως οφείλονται να τεθούν όρια για την χρήση των CCTV ώστε να διασφαλιστούν τα δικαιώματα απορρήτου και η ανωνυμία στους δημόσιους χώρους. Πολλές χώρες έχουν ήδη αρχίσει να λαμβάνουν βήματα για την καταπολέμηση της καταπάτησης της ιδιωτικότητας μέσω των συστημάτων επιτήρησης, όμως οι ρυθμίσεις αυτές διαφέρουν σημαντικά ανάμεσα στις χώρες τις Ευρώπης. Σε μερικές χώρες υπάρχουν αυστηροί κανονισμοί όσο αφορά τα ιδιωτικά συστήματα CCTV, σε άλλες κυρίως τα δημόσια συστήματα ρυθμίζονται νομικά (Hempel and Töpfer, 2004). Γενικότερα τα CCTV στην Ευρώπη ρυθμίζονται κυρίως στο πλαίσιο του απορρήτου και την προστασία δεδομένων, συγκεκριμένα μέσω του άρθρου 8 της Ευρωπαϊκής Σύμβασης Ανθρωπίνων Δικαιωμάτων, η Ευρωπαϊκή Σύμβαση για την Αυτοματοποιημένη Επεξεργασία Δεδομένων Προσωπικού Χαρακτήρα του Συμβουλίου της Ευρώπης και την Οδηγία Προστασίας Δεδομένων (95/46/ΕΚ) της Ευρωπαϊκής Ένωσης (Hempel and Töpfer, 2004).

Μία πρόταση του Andrew von Hirsch με στόχο αυτό, αποτελούσε η διακοπή τοποθέτησης κρυφών καμερών στους χώρους και η απαίτηση πως όπου υπάρχει τέτοιο σύστημα θα υπάρχει επίσης πινακίδα ή σήμα το οποίο θα ενημερώνει τους πολίτες πως βρίσκονται υπό επιτήρηση στην συγκεκριμένη περιοχή (Von Hirsch, Garland and Wakefield, 2004). Αυτό το σύστημα υιοθέτησε και η κυβέρνηση της Ελλάδας με τον Γενικό Κανονισμό Προστασίας Δεδομένων (ΕΕ) 2016/679 (ΓΚΠΔ) (Regulation (EU) 2016/679, 2016) όπου αναγράφονται οι κανονισμοί περί προστασίας προσωπικών δεδομένων (ΑΠΔ n.d. a). Για την λειτουργία συστήματος CCTV δεν χρειάζεται λήψη άδεια καθώς ο νόμος 2472/1997 καταργήθηκε και αντικαταστάθηκε από τον κανονισμό (ΕΕ) 2016/679 (Regulation (EU) 2016/679, 2016; ΑΠΔ n.d. b). Όμως επιβάλλεται η τήρηση όλων των προϋποθέσεων που απορρέουν από τον νόμο 2016/679, ειδικότερα κρίνεται αναγκαία η ενημέρωση των πολιτών κατά τον ερχομό τους στον χώρο με κατάλληλη πινακίδα καθώς και αναλυτική πληροφόρηση σε ιστοσελίδα ή έντυπο (ΑΠΔ n.d. b). Επίσης οφείλετε να υπάρχει τεκμηρίωση της νομιμότητας περί χρήσης των καμερών επιτήρησης (ΑΠΔ n.d. b). Τέλος, αποτελεί επιτακτική ανάγκη η δυνατότητα ικανοποίησης των δικαιωμάτων των πολιτών που καταγράφονται. Συγκεκριμένα (ΑΠΔ n.d. a):

- Θα υπάρχει δικαίωμα ενημέρωσης (άρθρα 13-14) και πρόσβασης (άρθρο 15) στα δεδομένα του εκάστοτε πολίτη με σαφή ενημέρωση κατά την συλλογή προσωπικής πληροφορίας.
- Επίσης ο πολίτης θα έχει δικαίωμα να διορθώσει μη ορθά ή και ελλιπή δεδομένα που τον αφορούν (άρθρο 16).
- Αν ο πολίτης επί επιτήρηση δεν επιθυμεί να αποθηκευτούν και να διατηρηθούν τα προσωπικά του δεδομένα, έχει την δυνατότητα να ζητήσει την διαγραφή αυτών των δεδομένων αρκεί να μην διατηρούνται για κάποιο συγκεκριμένο νόμιμο και δηλωμένο σκοπό (άρθρο 17).
- Ο πολίτης θα έχει δικαίωμα να περιορίσει την επεξεργασία των προσωπικών του δεδομένων αν συμπληρώνονται ορισμένες απαιτήσεις (άρθρο 18).
- Να υπάρχει δυνατότητα παράδοσης ή και μεταφοράς των δεδομένων που αφορούν τον πολίτη αν ζητηθεί (άρθρο 20).
- Ο πολίτης έχει το δικαίωμα να εναντιωθεί στην επεξεργασία των προσωπικών του στοιχείων αν συμπληρώνονται ορισμένες απαιτήσεις (άρθρο 21).

Αξίζει να σημειωθεί επίσης πως η εγκατάσταση καμερών που προορίζονται για δημόσιο χώρο, όπως είναι παραδείγματος χάρη, οδοί, πλατείες, άλση, παραλίες, λιμάνια καθώς και δημόσια δάση δεν επιτρέπεται από ιδιώτη με σκοπό την διατήρηση των προσωπικών δεδομένων των πολιτών (ΑΠΔ n.d. b). Στον ιδιωτικό τομέα επιτρέπεται η τοποθέτηση καμερών αφού πληρούνται οι παραπάνω απαιτήσεις στις εισόδους, εξόδους και στα ταμεία των πιθανών καταστημάτων και όχι σε χώρους συνεστίασης, αναψυχής ή σε άλλους χώρους στους οποίους ο πελάτης δεν έχει πρόσβαση (άρθρο 19 της οδηγίας 1/2011) (ΑΠΔ n.d. b). Σε περίπτωση που επιθυμείτε η εγκατάσταση συστήματος επιτήρησης σε σχολικό χώρο, απαιτείται να είναι ενημερωμένοι όλοι οι μαθητές καθώς και ο σύλλογος γονέων και διδακτικού προσωπικού οι οποίοι θα έχουν πρόσβαση στα δεδομένα βάσει του άρθρου 18 της οδηγίας 1/2011 και τα δεδομένα είναι απαραίτητο να διαγράφονται την επόμενη εργάσιμη ημέρα (ΑΠΔ n.d. b). Τέλος, όμοια με τον ιδιωτικό τομέα, κατά την εγκατάσταση καμερών σε σπίτι ή διαμέρισμα απαιτείται να μην γίνεται καταγραφή των δημόσιων χώρων ή των άλλων διαμερισμάτων και σε περίπτωση που άλλοι ένοικοι χρειάζονται να περάσουν μπροστά από την είσοδο που επιτηρείτε κρίνεται απαραίτητη η λήψη συναίνεσης καθώς και η ενημέρωσή τους προτού πραγματοποιηθεί η εγκατάσταση του συστήματος (ΑΠΔ n.d. c).




**Σχήμα 5.** Παράδειγμα πολυκατοικίας όπου ο ένοικος Α (κόκκινο) επιθυμεί να εγκαταστήσει σύστημα και θα χρειαστεί συναίνεση από τους ένοικους ΣΤ και Β (πορτοκαλί). [7]

[7] Σχήμα από: (ΑΠΔ n.d. b).

# ΚΕΦΑΛΑΙΟ 3 Προδιαγραφή Συστήματος

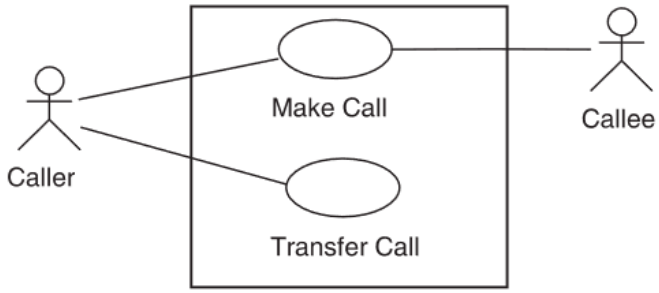
Είναι φανερό λοιπόν πως πρέπει να τεθούν όρια κατά την χρήση επιτήρησης CCTV με σκοπό την διασφάλιση προστασίας των προσωπικών δεδομένων και της ανωνυμίας στους δημόσιος χώρους. Κατά συνέπεια, στα πλαίσια της διπλωματικής εργασίας αποφασίστηκε να γίνει υλοποίηση ενός συστήματος ασφάλειας για τα δημόσια καθώς και ιδιωτικά ιδρύματα που χρησιμοποιούν κλειστά κυκλώματα τηλεόρασης για την επίτευξη της ασφάλειας σε διάφορους τομείς, είτε αυτά αποτελούν κοινωνική ασφάλεια για κάθε πολίτη είτε προστασία ιδιωτικής περιουσίας. Βασικό στόχο του συστήματος θα αποτελεί η διασφάλιση των προσωπικών δεδομένων των πολιτών παρέχοντας περιορισμένη πρόσβαση στην πληροφορία που καταγράφεται κάθε στιγμή με εξαίρεση ορισμένες περιπτώσεις χρήσης όπου θα πραγματοποιηθεί άρση των δικλείδων ασφάλειας.

Σκοπός του κεφαλαίου είναι η περιγραφή των περιπτώσεων χρήσης του λογισμικού, καθώς και η παρουσίαση των απαιτήσεων του συστήματος που υλοποιήθηκε. Θα γίνει αναφορά στις περιπτώσεις χρήσης σε ιστορικό περιεχόμενο, επεξήγηση του ρόλου τους σήμερα καθώς και παρουσίαση των περιπτώσεων χρήσης που καθιερώθηκαν για το σύστημα. Επίσης, θα καλυφθεί τι αποτελεί απαίτηση από ένα σύστημα, η προδιαγραφή αυτών για το σύστημα που αναπτύχθηκε και θα γίνει αναφορά στα προβλήματα που θα προκύπταν αν δεν γινόταν ανάλυση και ορισμός των απαιτήσεων.

## Περιπτώσεις χρήσης του συστήματος 3.1

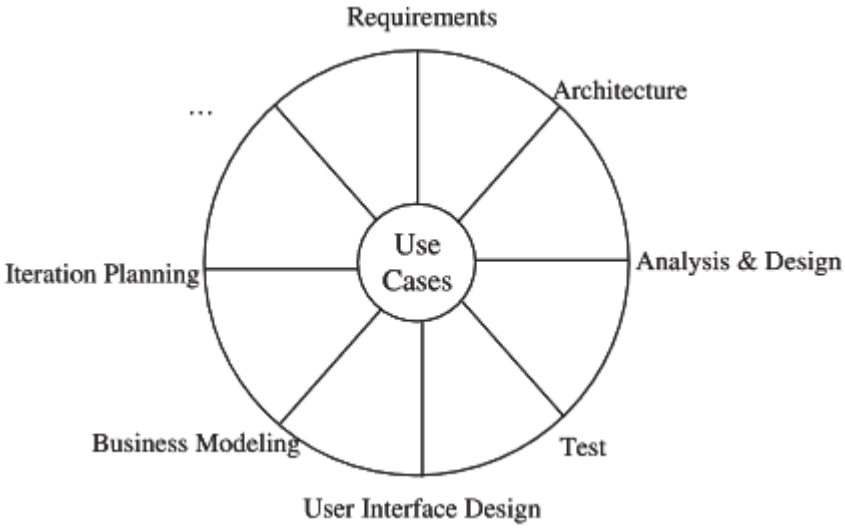
### Ορισμός περιπτώσεων χρήσης ιστορικά 3.1.α

Οι περιπτώσεις χρήσης παίζουν ρόλο σε πολλές διαφορετικές πτυχές της μηχανικής λογισμικού. Ειδικότερα, βασικό κομμάτι στην ανάλυση και ανάπτυξη ενός λογισμικού είναι η δυνατότητα μελέτης και δημιουργίας περιπτώσεων χρήσης. Τι αποτελεί όμως μια περίπτωση χρήσης; Το έτος 1987 σύμφωνα με το έγγραφο OOPSLA'87 «Μια περίπτωση χρήσης είναι ένα ειδικό είδος ακολουθίας συναλλαγών, οι οποίες εκτελούνται από έναν χρήστη και ένα σύστημα σε διάλογο» (Jacobson, 2004). Εκείνη την στιγμή το μοντέλο περίπτωσης περιλάμβανε επίσης οντότητες με παρόμοια λειτουργεία όπως τα αντικείμενα σε αντικειμενοστραφή προγραμματισμό. Έτσι κάθε οντότητα και περίπτωση χρήσης είχαν λειτουργίες και στοιχεία. Με την ολοκλήρωση του ορισμού των περιπτώσεων χρήσης τότε αυτές σχεδιάζονταν και δοκιμάζονταν. Κάθε περίπτωση ελέγχονταν ξεχωριστά έτσι ώστε να επιβεβαιωθεί πως το σύστημα ικανοποιεί τις απαιτήσεις του πελάτη (Jacobson, 2004). Με το πέρας της δημιουργίας και επαλήθευσης των περιπτώσεων χρήσης δημιουργούνταν διαγράμματα αλληλουχίας  τα οποία έδειχναν τις αλληλεπιδράσεις μεταξύ των οντοτήτων.




**Σχήμα 6.** Παράδειγμα περιπτώσεων χρήσης ενός συστήματος εναλλαγής. [8]

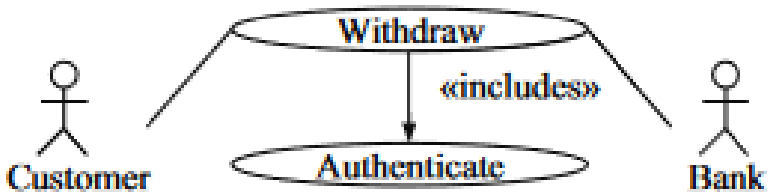
Συνεπώς, είναι φανερό λοιπόν πως και από το έτος 1987 οι ερευνητές είχαν αντιληφθεί την κρισιμότητα ύπαρξης περιπτώσεων χρήσης κατά την ανάπτυξη ενός έργου.




**Σχήμα 7.** Παράδειγμα διαγράμματος τροχού τη διαδικασίας που περιλάμβανε τις περιπτώσεις χρήσης το 1992. [9]

Σε κάθε βήμα γινόταν ανάλυση, σχεδιασμός, υλοποίηση και δοκιμή του συστήματος με τις περιπτώσεις χρήσης. Ο τελικός ορισμός των περιπτώσεων χρήσης έδινε στο παρελθόν, αλλά ακόμα και σήμερα, στον ερευνητή την δυνατότητα να δημιουργήσει ορθές διεπαφές χρήστη και εγχειρίδια χρήσης, έτσι ώστε να επιτευχθεί η ομαλή λειτουργία του συστήματος. Στην σύγχρονη εποχή οι περιπτώσεις χρήσης έχουν γίνει μέρος της Ενοποιημένης Γλώσσας Μοντελοποίησης (UML) (Jacobson, 2004).

[8] Σχήμα από: Jacobson, (2004).
[9] Σχήμα από: Jacobson, (2004).



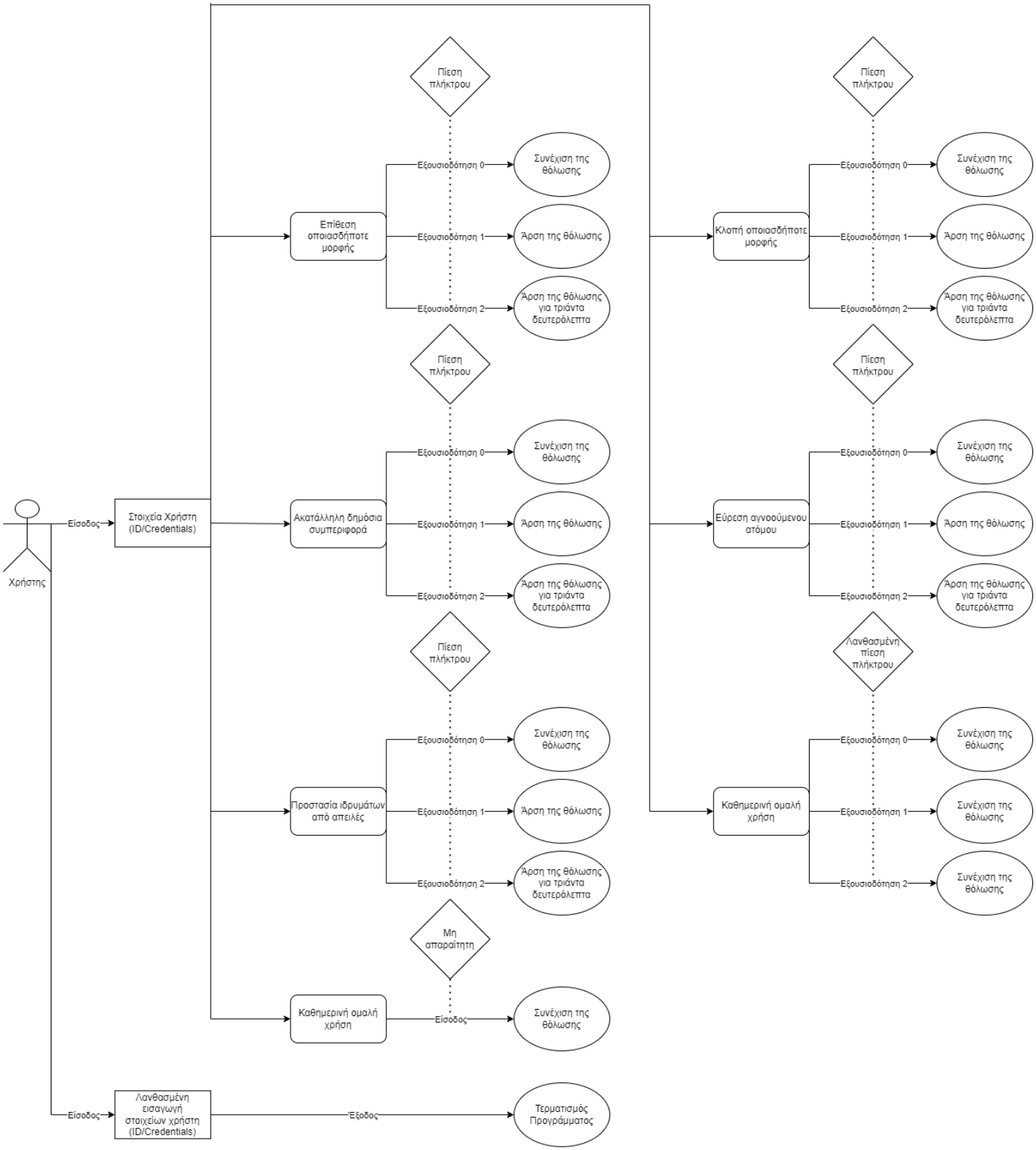

**Σχήμα 8.** Παράδειγμα ενός UML διαγράμματος μιας περίπτωσης χρήσης μεταξύ πελάτη και τράπεζας.[10]

## Διάκριση περιπτώσεων χρήσης του συστήματος. 3.1.β

Αρχικά, πριν ξεκινήσει η ανάλυση των περιπτώσεων χρήσης ήταν απαραίτητος ο ορισμός των πιθανών χειριστών που θα έχει το σύστημα οποιαδήποτε στιγμή. Στην περίπτωση που το σύστημα εγκατασταθεί στον ιδιωτικό τομέα, το κοινό προσωπικό δεν θα έχει πρόσβαση στα δεδομένα που θα παρέχει το λογισμικό. Ο εκάστοτε εργοδότης οφείλει να είναι υπεύθυνος για την ορθή ενημέρωση και εκπαίδευση εξιδεικευμένου προσωπικού. Αυτό θα έχει ως αποτέλεσμα την ελαχιστοποίηση περιπτώσεων κατάχρησης αλλά και την επίτευξη ομαλής λειτουργίας του συστήματος σε καθημερινή βάση. Όμοια στον δημόσιο τομέα δεν θα έχει όλο το προσωπικό πρόσβαση, αλλά μόνο εξιδεικευμένο προσωπικό που έχει ανατεθεί αφού πρωτύτερα υπάρξει η κατάλληλη εκπαίδευση και ενημέρωση. Παραδείγματος χάρη, υποθέτοντας πως το σύστημα έχει εγκατασταθεί σε περιοχή του νόμου Φθιώτιδας που παρακολουθεί η αστυνομία, μόνο οι ανώτεροι αξιωματούχοι, αφού γίνει η κατάλληλη εκπαίδευση για να επιτευχθεί η ομαλή χρήση καθώς και η πιστοποίηση ευθύνης, θα έχουν πρόσβαση και την δύναμη να κάνουν άρση των δικλείδων ασφάλειας επ' αόριστων και να εμφανίσουν τα πρόσωπα των πολιτών που καταγράφηκαν μέσω του συστήματος καμερών κλειστού κυκλώματος. Ακόμη, σε ειδική περίπτωση κατά την διάρκεια αστυνομικής έρευνας, για παράδειγμα κατά την ανάγκη εύρεσης αγνοούμενου ατόμου, θα έχει δυνατότητα και ο επικεφαλής αστυνόμος να κάνει άρση των δικλείδων ασφάλειας προσωρινά. Επομένως, για την επίτευξη αυτού του στόχου δημιουργήθηκαν στο σύστημα διαφορετικά επίπεδα εξουσιοδότησης. Αρχικά, εξουσιοδότηση βαθμού 0 (clearance 0) θα έχει το προσωπικό που δεν χρειάζεται πρόσβαση στα προσωπικά δεδομένα αλλά είναι υπεύθυνο για την παρακολούθηση μέσω του συστήματος ώστε να επιτευχθεί η ομαλή εξέλιξη της καθημερινότητας. Εξουσιοδότηση βαθμού 1 (clearance 1) θα έχει το προσωπικό που λόγω των περιπτώσεων, όπως αναφέρθηκε παραπάνω με τον επικεφαλής αστυνόμο κατά την διάρκεια μιας έρευνας, χρειάζεται προσωρινή πρόσβαση στα δεδομένα. Σε αυτή την περίπτωση, με το πάτημα του καθιερωμένου πλήκτρου ο χρήστης θα κάνει άρση της θόλωσης για 30 δευτερόλεπτα, ύστερα η θόλωση θα συνεχίσει αυτόματα. Τέλος, εξουσιοδότηση βαθμού 2 (clearance 2) θα έχει το προσωπικό το οποίο θα έχει πρόσβαση στα δεδομένα οποιαδήποτε στιγμή, όπως είναι για παράδειγμα οι ανώτεροι αξιωματούχοι που αναφέρθηκαν παραπάνω, όπου με το πάτημα του καθιερωμένου πλήκτρου θα πραγματοποιείται άρση της θόλωσης μέχρι ο χρήστης να κλείσει το σύστημα ή μέχρι να επαναφέρει την θόλωση χειροκίνητα.

Αφού έγινε ο ορισμός των πιθανών χειριστών ακολούθησε η μελέτη και ανάπτυξη των περιπτώσεων χρήσης που κρίθηκε απαραίτητο να συμπεριλαμβάνονται στο σύστημα που αναπτύχθηκε και επισημοποιήθηκαν με βάση το UML πρότυπο σε μορφή διαγράμματος ροής περιπτώσεων χρήσης.

[10] Σχήμα από: Faitelson and Tyszberowicz, (2017).




**Σχήμα 9.** Διάγραμμα ροής περιπτώσεων χρήσης για το RT_FaceBlur σύστημα που αναπτύχθηκε στα πλαίσια της διπλωματικής εργασίας.

Βάσει του διαγράμματος, βασικές περιπτώσεις χρήσης αποτελούν:

- Με λανθασμένη εισαγωγή των στοιχείων, ο χρήστης δεν θα έχει πρόσβαση στο πρόγραμμα και αυτό θα τερματίζει.
- Μετά την είσοδο του εκάστοτε χρήστη, το σύστημα θα είναι σε θέση να αναγνωρίζει την εξουσιοδότησή του και ανάλογα με αυτήν το σύστημα θα έχει διαφορετική λειτουργία.
- Ανάλογα με την περίσταση, ο χρήστης μπορεί να βρεθεί σε θέση όπου απαιτείται η άρση των δικλείδων ασφάλειας για την προστασία των πολιτών. Παραδείγματος χάρη, όταν σε κάποιο από τα δημόσια καθώς και τα ιδιωτικά ιδρύματα οι πολίτες βρεθούν αντιμέτωποι με κακόβουλα άτομα ή ακόμα και όταν αυτά τα άτομα επιδιώκουν να προκαλέσουν ζημιές ή και να κλέψουν ιδιωτική και δημόσια περιουσία.
- Κατά την διάρκεια ομαλής καθημερινής χρήσης η άρση της θόλωσης δεν θα είναι απαραίτητη.
- Οι τρείς λειτουργίες βάσεις εξουσιοδότησης είναι:

    - Εξουσιοδότηση 0: Δεν γίνεται άρση της θόλωσης.
    - Εξουσιοδότηση 1: Με την πίεση του σωστού πλήκτρου θα γίνει άρση της θόλωσης για 30 δευτερόλεπτα.
    - Εξουσιοδότηση 2: Με την πίεση του σωστού πλήκτρου θα γίνει άρση της θόλωσης μέχρι ο χειριστής να την επαναφέρει χειροκίνητα ή να τερματίσει το σύστημα.

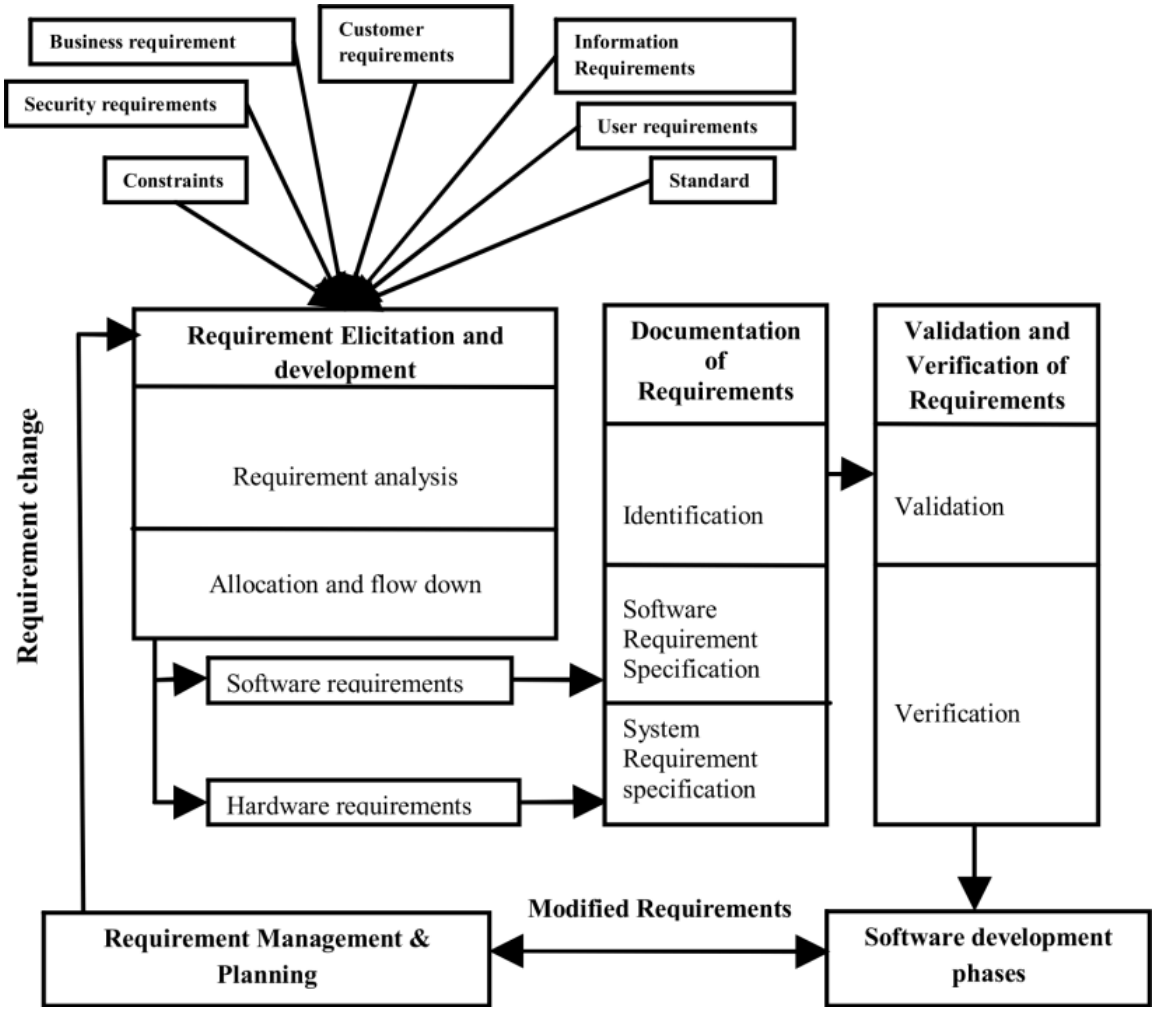
- Αν ο χρήστης πιέσει λανθασμένο πλήκτρο για την άρση της θόλωσης τότε το πρόγραμμα θα συνεχίζει να λειτουργεί κανονικά.

# Απαιτήσεις συστήματος 3.2

## Ορισμός απαιτήσεων 3.2.α

Απαιτήσεις ενός συστήματος είναι χαρακτηριστικά τα οποία ανακαλύπτονται πριν, αλλά και κατά την διάρκεια ανάπτυξης ενός προϊόντος. Είναι μία κατάσταση ή ικανότητα την οποία επιβάλλεται να πληροί ή να διαθέτει ένα σύστημα ή ένα στοιχείο του συστήματος ώστε να ικανοποιηθούν οι προδιαγραφές που έχουν τεθεί (Pandey, Suman and Ramani, 2010). Σε όλα τα συστήματα πραγματικού χρόνου διακρίνουμε δύο παράγοντες μεταξύ των οποίων γίνεται αμοιβαία αλληλεπίδραση για την συγκέντρωση απαιτήσεων, τους ανθρώπους και τις μηχανές (Ropohl, 1999). Οι απαιτήσεις ταξινομούνται συνήθως ως λειτουργικές και μη λειτουργικές (Kurtanovic and Maalej, 2017).

Ο ορισμός των απαιτήσεων ενός λογισμικού αποτελεί επιτακτική ανάγκη κατά την διάρκεια της ανάπτυξής του, ώστε με το πέρας της υλοποίησης του να είναι σε θέση να ανταποκρίνεται στις απαιτήσεις του πιθανού πελάτη. Άλλωστε, είναι ευρέως αποδεκτό πως αν η ομάδα ή ο εκάστοτε ερευνητής αδυνατεί να κατανοήσει πλήρως τις απαιτήσεις του προβλήματος που επιθυμεί να επιλύσει τότε η αποτυχία ανάπτυξης του λογισμικού είναι αναπόφευκτη (Ralph, 2012). Οφείλει ο ερευνητής λοιπόν να έχει τις απαραίτητες γνώσεις και κριτική σκέψη ώστε να είναι σε θέση να διακρίνει αυτές τις απαιτήσεις. Επίσης είναι απαραίτητη η εξοικείωσή του με την ουσία του προβλήματος, το οποίο είναι απαραίτητο να πραγματοποιηθεί στα πρώτα στάδια κατά την ανάπτυξη του έργου.




**Σχήμα 10.** Διάγραμμα συλλογής απαιτήσεων και επεξεργασίας μέσω κατηγοριοποίησης και πιστοποίησης. Υλοποίηση με βάση των απαιτήσεων και αλλαγή αυτών κατά περίπτωση.[11]

## Μέθοδοι διάκρισης απαιτήσεων 3.2.β

Για την διάκριση των απαιτήσεων μπορούν να χρησιμοποιηθούν διάφορες τακτικές. Η συλλογή αυτών μπορεί να γίνει με την χρήση ερωτηματολογίων και συνεντεύξεων για την καθιέρωση μιας πρώτης βασικής έννοιας η οποία θα λειτουργήσει ως βάση κατά την διάρκεια της μελέτης. Επίσης, αποτελεί επιτακτική ανάγκη η επιδίωξη συζητήσεων με ειδικούς πάνω στο θέμα ανάπτυξης, έτσι ώστε η ομάδα να εμβαθύνει την κατανόησή της και να είναι σε θέση να ανταποκριθεί στις απαιτήσεις που μπορεί να προκύψουν σε μελλοντικά επαναληπτικά βήματα κατά την διάρκεια του έργου. Επιπρόσθετα, η χρήση μηχανικής απαιτήσεων είναι μια συστηματική προσέγγιση μέσω της οποίας συλλέχθηκαν απαιτήσεις από διαφορετικές πηγές και εφαρμόστηκαν κατά την διαδικασία ανάπτυξης λογισμικού. Σε αυτό το βήμα μπορούν να εντοπιστούν πιθανές συγκρούσεις μεταξύ απαιτήσεων, δηλαδή μπορεί να υπάρχουν δύο ή περισσότερες απαιτήσεις των οποίων η ικανοποίηση δεν μπορεί να γίνει ταυτόχρονα οπότε επιβάλλεται η επίλυση συγκρούσεων σε συνεργασία με τον πελάτη. Αφού ολοκληρωθεί ο ορισμός των απαιτήσεων που απαιτούνται από το λογισμικό αποτελεί ανάγκη να γίνει επαλήθευση αυτών.

[11] Σχήμα από: Pandey, Suman and Ramani, (2010).


**Σχήμα 11.** Γενική μορφή διαδικασίας προσδιορισμού των απαιτήσεων από το λογισμικό με μηχανική απαιτήσεων. [12]

## Ορισμός απαιτήσεων του συστήματος 3.2.γ

Συνεπώς, ορίστηκαν απαιτήσεις που κρίθηκαν απαραίτητες για την ανάπτυξη του συστήματος και η προδιαγραφή αυτών στα πλαίσια της διπλωματικής εργασίας.

- Αρχικά είναι αναγκαίο το τελικό πρόγραμμα να είναι λειτουργικό και σε άλλα συστήματα όπως είναι τα λειτουργικά συστήματα Linux και MacOS του Linus Torvalds και Apple Inc. αντίστοιχα πέρα από τα Windows της εταιρίας Microsoft. Επίσης οφείλετε να υπάρχει απαίτηση της επίδοσης του συστήματος ώστε να είναι ανταγωνιστικό ως προς τον χρόνο λειτουργίας που χρειάζεται, καθώς και με τους πόρους που χρησιμοποιεί όπως η μνήμη και οι μονάδες επεξεργασίας. Για την ικανοποίηση αυτών των προδιαγραφών επιλέχθηκε η γλώσσα προγραμματισμού Python για την ανάπτυξη του συστήματος. Η γλώσσα Python είναι αντικειμενοστραφής και διαπλατφορμική (Summerfield, 2009), ιδανική για ανάπτυξη εφαρμογών με καλή διαχείριση μνήμης καθιστώντας την γρήγορη και αποδοτική.
- Επιπρόσθετα κύριος στόχος του προγράμματος αποτελεί να είναι σε θέση να πραγματοποιεί επεξεργασία στιγμιότυπων που περιλαμβάνουν πρόσωπα σε βίντεο πραγματικής ροής ώστε το αποτέλεσμα να είναι η ροή με θολωμένα πρόσωπα.
- Επιβάλλεται ο ορισμός απαιτήσεων χρήσης για την ευκολία διαχείρισης του συστήματος από τον χρήστη. Απαίτηση χρήσης καθορίζουν τα χαρακτηριστικά της χρήσης του συστήματος καθώς και η διεπαφή χρήσης που θα περιλαμβάνει το πρόγραμμα με την χρήση κατάλληλων βιβλιοθηκών.
- Για την επίτευξη αξιοπιστίας του προγράμματος και την ελαχιστοποίηση των πιθανών διαρροών ο κάθε χρήστης θα έχει προσωπικό κωδικό που θα πληροί ορισμένες προϋποθέσεις (ο κωδικός θα είναι ίσος ή μεγαλύτερος από 8 χαρακτήρες και θα περιλαμβάνει υποχρεωτικά έναν ή παραπάνω ειδικούς χαρακτήρες). Ακόμη, οι κωδικοί κατά την σύνδεση δεν θα εμφανίζονται στην οθόνη του συστήματος.
- Επίσης το πρόγραμμα θα είναι σε θέση να κλειδώνει χωρίς να γίνει πρόσβαση στην πληροφορία σε περίπτωση που ο εκάστοτε χρήστης κάνει επαναλαμβανόμενες λανθασμένες προσπάθειες σύνδεσης.

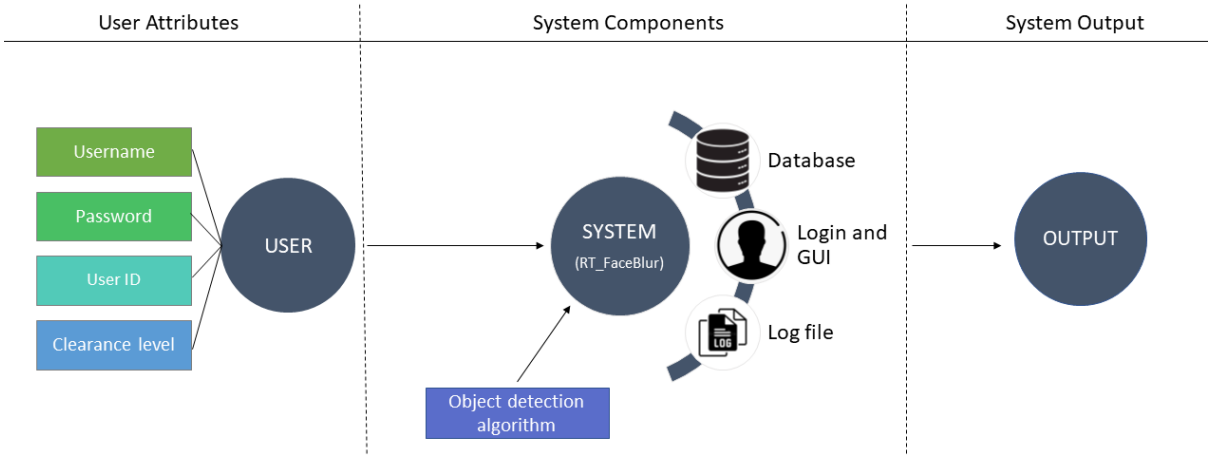
[12] Σχήμα από: Veskoukis, (2015).

- Τέλος δεν μπορεί να παραληφθεί πως οφείλετε να υπάρχει απαίτηση ευθύνης από τους εκάστοτε χειριστές κατά την χρήση του προγράμματος ώστε να μην υπάρξει κατάχρηση. Το πρόβλημα στην σύγχρονη εποχή είναι πως με την επέκταση της προσβασιμότητας σε συστήματα παρακολούθησης αναπόφευκτα θα υπάρξει κατάχρηση. Παραδείγματος χάρη, το 1997 ένας αξιωματούχος της αστυνομίας στην Ουάσιγκτον, Η.Π.Α συνελήφθη καθώς χρησιμοποιούσε βάσεις δεδομένων της αστυνομίας για να συλλέξει πληροφορίες αναζητώντας τον αριθμό των πινακίδων αυτοκινήτων που ήταν σταθμευμένα σε λέσχες ομοφυλόφιλων μέσω των καμερών που διέθετε η αστυνομία και ύστερα εκβίασε παντρεμένα άτομα που σύχναζαν εκεί (ACLU, 2002). Επιπλέον έρευνες έδειξαν πως οι γυναίκες είναι πιο συχνά θύματα παρακολούθησης για λόγους ηδονοθηρίας (Honovich, 2015). Είναι φανερό λοιπόν πως η ολοκληρωτική αποφυγή κατάχρησης του συστήματος είναι αδύνατη, όμως μπορούν να ληφθούν μέτρα για την επίτευξη της απαίτησης ευθύνης. Οι υπηρεσίες οφείλουν να καταγράφουν πληροφορίες σχετικά με την χρήση του συστήματος σε αρχείο (Molnar and Warren, 2020). Αρχικά, επιβάλετε ο χρήστης να συνδεθεί στο σύστημα με τα διαπιστευτήριά του προτού του δοθεί η δυνατότητα να κάνει άρση των δικλείδων ασφάλειας έτσι ώστε το σύστημα να μπορεί να αναγνωρίζει κάθε στιγμή ποιος χρήστης είναι συνδεδεμένος. Άρα, το αρχείο αυτό θα περιλαμβάνει τον κωδικό «ID» του συνδεδεμένου χρήστη, την ημερομηνία και ώρα όποτε χρήστης συνδέθηκε αλλά και αποσυνδέθηκε από το σύστημα, την ημερομηνία και ώρα όποτε χρησιμοποίησε το πρόγραμμα για να κάνει άρση της θόλωσης στο βίντεο ζωντανής ροής, καθώς και ένα στιγμιότυπο της ροής βίντεο όποτε έγινε η άρση της θόλωσης. Με την πληροφορία αυτή γίνεται δυνατή η καταπολέμηση του φαινομένου κατάχρησης του συστήματος καθώς γνωρίζουμε κάθε στιγμή τον υπεύθυνο, το οποίο επίσης θα αποτρέψει πιθανές μελλοντικές καταχρήσεις.

Η ελλιπή ανάλυση για την διάκριση των απαιτήσεων από το λογισμικό θα οδηγούσε στην μη ορθή ανάπτυξη του λογισμικού και στην δημιουργία προβλημάτων. Αρχικά αν το σύστημα δεν είχε την δυνατότητα να λειτουργήσει σε οποιοδήποτε λειτουργικό σύστημα, αυτό θα καθιστούσε την συντήρησή του αλλά και την ικανότητα προσαρμογής του αρκετά δύσκολη. Επίσης θα περιοριστεί αρκετά η διαθεσιμότητα του συστήματος καθώς και η ικανότητα να είναι ανταγωνιστικό στον χώρο εργασίας. Διαφορετικές εταιρίες ή και διαφορετικοί τομείς κάτω από την ίδια εταιρία μπορεί να χρησιμοποιούν διαφορετικά λειτουργικά συστήματα το οποίο καθιστά την εγκατάσταση, διατήρηση και επικοινωνία του συστήματος με άλλα συστήματα δύσκολη, έτσι οδηγώντας τον πιθανό πελάτη να προτιμήσει άλλο προϊόν. Ακόμη, χωρίς την δυνατότητα θόλωσης των προσώπων τα άτομα που καταγράφονται στο κλειστό κύκλωμα τηλεόρασης θα είναι περισσότερο επιρρεπή να πέσουν θύματα καταπάτησης της ιδιωτικότητάς τους. Επιπρόσθετα, χωρίς διεπαφή χρήσης το σύστημα θα είναι δύσκολο στην διαχείρισή του, έτσι απαιτώντας από τον πελάτη παραπάνω χρήματα για την εκπαίδευση του προσωπικού ως προς την χρήση του συστήματος. Ύστερα, σε περίπτωση που το σύστημα δεν είναι σε θέση να ικανοποιήσει την ανάγκη αξιοπιστίας με την ορθή διαχείριση των κωδικών, αυξάνονται οι πιθανές διαρροές και με αυτές η πιθανότητα κατάχρησης του συστήματος. Συμπληρωματικά, το πρόγραμμα πρέπει επίσης να είναι σε θέση να κλειδώνει μετά από επαναλαμβανόμενες λανθασμένες προσπάθειες, αλλιώς καθιστάτε περισσότερο ευάλωτο σε πιθανές επιθέσεις από κακόβουλα τρίτα πρόσωπα που μπορεί να επιθυμούν να εισβάλουν στο σύστημα. Τέλος, υποθέτοντας πως το σύστημα που αναπτύχθηκε δεν κατείχε αρχείο καταγραφής δεδομένων, κατά συνέπεια το παρελθόν θα επαναληφθεί και θα υπάρξει κατάχρηση όπως είχε έχει καταγραφεί στην Βρετανία όπου πολλοί χειριστές των καμερών λειτουργούσαν βάσει δικών τους προκαταλήψεων εστιάζοντας κυρίως σε έγχρωμους ανθρώπους (ACLU, 2002). Συνεπώς δεν θα υπάρχει γρήγορος και αποτελεσματικός τρόπος για την εύρεση του δράστη.

# ΚΕΦΑΛΑΙΟ 4 Ανάπτυξη Συστήματος

Με το πέρας της ανάλυσης και οριστικοποίησης των περιπτώσεων χρήσης καθώς και των απαιτήσεων του συστήματος, γίνεται πλέον δυνατός ο σχεδιασμός του λογισμικού καθώς και η ανάπτυξη μιας γενικής αρχιτεκτονικής, πάνω στην οποία θα βασιστεί η υλοποίηση του συστήματος με όνομα RT_FaceBlur. Η αρχιτεκτονική είναι ως εξής:




**Σχήμα 12.** Γενική αρχιτεκτονική του συστήματος RT_FaceBlur.

Ορίστηκε πως ο χρήστης θα έχει ορισμένα χαρακτηριστικά για την ομαλή λειτουργία του συστήματος καθώς και την ικανοποίηση των απαιτήσεων:

- «Username», αποτελεί το όνομα του χρήστη με το οποίο θα πραγματοποιηθεί σύνδεση.
- «Password», αποτελεί τον κωδικό του χρήστη με τον οποίο θα πραγματοποιηθεί σύνδεση.
- «User ID», είναι ένας αριθμός μοναδικός για τον κάθε χρήστη με τον οποίο θα αναγνωρίζει το σύστημα ποιος είναι συνδεδεμένος κάθε στιγμή.
- «Clearance level», αποτελεί το επίπεδο εξουσιοδότησης του κάθε χρήστη και αφού το σύστημα το αναγνωρίσει, ανάλογα με αυτό θα έχει διαφορετική λειτουργία.

Για το σύστημα RT_FaceBlur αποφασίστηκε να χρησιμοποιηθεί αλγόριθμος αναγνώρισης αντικειμένων, αλλά και να δημιουργηθούν μονάδες με διαφορετικές λειτουργίες:

- «Database», αποτελεί μονάδα η οποία δημιουργεί μια βάση δεδομένων που θα περιέχει τα στοιχεία του κάθε χρήστη, με την εκκίνηση του προγράμματος.
- «Login and GUI», αποτελεί μονάδα η οποία θα επιτρέπει στον χρήστη να πραγματοποιήσει σύνδεση με χρήση κατάλληλου γραφικού περιβάλλοντος διεπαφής. Επίσης θα πραγματοποιεί όλους τους απαραίτητους ελέγχους για την ταυτοποίηση του χρήστη.
- Τέλος, «Log file» αποτελεί μονάδα η οποία καταγράφει όλες τις πληροφορίες για τις ενέργειες που πραγματοποιήθηκαν κατά την διάρκεια λειτουργίας του συστήματος και τις αποθηκεύει σε αρχείο για περαιτέρω ανάλυση όποτε χρειάζεται.

Στην συνέχεια του κεφαλαίου θα γίνει αναλυτική αναφορά στις τεχνολογίες που χρησιμοποιήθηκαν κατά την ανάπτυξη του συστήματος καθώς και τα πιθανά σενάρια λειτουργίας.

# Εργαλεία υλοποίησης 4.1

## Python 4.1.α

Η γλώσσα προγραμματισμού Python δημιουργήθηκε το 1991 από τον ολλανδό προγραμματιστή Guido van Rossum, ο οποίος αποφάσισε να την δημιουργήσει σε μοντέλο ανοιχτού κώδικα. Αυτό σημαίνει πως ο καθένας μπορεί ελευθέρα να προσθέσει στον κώδικα όπως θέλει. Κατά συνέπεια, η γλώσσα στην σημερινή εποχή είναι από τις πιο διαδεδομένες, καθώς και από τις πιο εύκολες στην χρήση. Ο κώδικας στην γλώσσα προγραμματισμού Python είναι ξεκάθαρος στην ανάγνωση και την εγγραφή αλλά και συνοπτικός. Ως αποτέλεσμα, είναι δυνατή η ανάπτυξη κώδικα με πολύ λιγότερες γραμμές συγκριτικά με άλλες προγραμματιστικές γλώσσες όπως είναι η Java ή C. Επιπρόσθετα, η γλώσσα Python είναι διαπλατφορμική, το οποίο σημαίνει πως το ίδιο πρόγραμμα Python μπορεί να εκτελεστεί σε Windows καθώς και σε συστήματα παρόμοια με το Unix, όπως είναι το Linux, το BSD και το Mac OS X, με απλή αντιγραφή του επιθυμητού αρχείου στο μηχάνημα που επιθυμεί ο χρήστης χωρίς περεταίρω προετοιμασία ή επεξεργασία (Summerfield, 2009). Λόγω της φύσης της γλώσσας καθώς και τις διασημότητας της, χρησιμοποιείται για αναρίθμητους στόχους, από καθημερινή χρήση για οργάνωση αρχείων μέχρι και ανάπτυξη τεχνητής νοημοσύνης. Αυτό είναι αποτέλεσμα των χαρακτηριστικών που αποτελούν αυτήν την γλώσσα, των οποίων κύρια είναι (Simplilearn, 2022):

- Εύκολη στην κωδικοποίηση και ανάγνωση.
- Δωρεάν και ανοιχτού κώδικα.
- Εκτενή τυπική βιβλιοθήκη.
- Διερμηνευμένη.
- Φορητή και Διαπλατφορμική.
- Αντικειμενοστραφής.
- Εκφραστική.
- Υποστηρίζει Διεπαφή Χρήστη.
- Δυναμική.
- Υψηλού επιπέδου γλώσσα προγραμματισμού.
- Παροχή προηγμένων δυνατοτήτων προγραμματισμού.

## OpenCV 4.2.β

OpenCV (Open Source Computer Vision Library) είναι μια βιβλιοθήκη ανοιχτού κώδικα της γλώσσας Python, η οποία περιλαμβάνει εκατοντάδες αλγορίθμους υπολογιστικής όρασης. Επίσης, διαχειρίζεται την μνήμη αυτόματα και κάνει αυτόματη κατανομή των δεδομένων εξόδου. Τέλος, έχει δομοστοιχειωτή δομή, δηλαδή περιλαμβάνει πολλές κοινόχρηστες ή στατικές βιβλιοθήκες οι οποίες αποτελούν (OpenCV, 2022):

- Βασική λειτουργία (core): Μία συμπαγής μονάδα η οποία καθορίζει τις βασικές δομές των δεδομένων, όπως του πυκνού πολυδιάστατου πίνακα Mat.
- Επεξεργασία εικόνας (imgproc): Μία μονάδα επεξεργασίας εικόνας η οποία περιλαμβάνει γραμμικό, καθώς και μη γραμμικό φιλτράρισμα εικόνας, γεωμετρικούς μετασχηματισμούς εικόνας, μετατροπή χρωματικού χώρου, ιστογράμματα και άλλα.
- Ανάλυση βίντεο (video): Αποτελεί μια μονάδα ανάλυσης στην οποία περιλαμβάνεται η εκτίμηση κίνησης, αφαίρεση του υπόβαθρου, καθώς και αλγόριθμοι παρακολούθησης αντικειμένων.

- Βαθμονόμηση κάμερας και τρισδιάστατη ανακατασκευή (calib3d): Περιέχει αλγόριθμους γεωμετρίας πολλαπλής προβολής, βαθμονόμηση μονής αλλά και στερεοφωνικής κάμερας, αλγόριθμους στερεοφωνικής αντιστοιχίας και στοιχεία τρισδιάστατης ανακατασκευής.
- Πλαίσιο δισδιάστατων χαρακτηριστικών (features2d): Δίνει πρόσβαση σε ανιχνευτές και σε περιγραφείς .
- Ανίχνευση αντικειμένων (objdetect): Δυνατότητα ανίχνευσης αντικειμένων και παρουσιών προκαθορισμένων κλάσεων.
- Υψηλού επιπέδου GUI (highgui): Εύχρηστη διεπαφή χρήστη.
- Βίντεο I/O (videoio): Εύχρηστη διεπαφή για λήψη βίντεο καθώς και κωδικοποιητές βίντεο.

Αξίζει επίσης να αναφερθεί πως για την αναγνώριση των προσώπων κατά την διάρκεια καταγραφής των δεδομένων χρησιμοποιήθηκε το αρχείο `Haarcascade_frontalface_alt.xml` (Avelino, 2011). Το συγκεκριμένο αρχείο της OpenCV βιβλιοθήκης περιέχει σειριακό ανιχνευτή προσώπων Haar cascade βασισμένο πάνω στον αλγόριθμο Viola-Jones. Αποτελεί μια κωδικοποιημένη λίστα δέντρων αποφάσεων της οποίας κάθε κορυφή δοκιμάζει ένα χαρακτηριστικό Haar και κάθε λίστα ενημερώνει αν έχει πραγματοποιηθεί ανίχνευση προσώπου ή όχι. Συγκεκριμένα αυτό το αρχείο είναι μόνο για ανίχνευση μετωπικών προσώπων ενώ υπάρχουν εναλλακτικά για αναγνώριση όλου του σώματος καθώς και για συγκεκριμένα μέρη του σώματος.

## Keyboard 4.3.γ

Η Keyboard είναι μια μικρή βιβλιοθήκη της γλώσσας Python με την οποία γίνεται δυνατή η καταγραφή πλήκτρων πρόσβασης, η προσομοίωση πατημάτων πλήκτρων και άλλα. Μερικά από τα πιο βασικά της χαρακτηριστικά αποτελούν (PyPI, 2020):

- Παγκόσμιος γάντζος εκδήλωσης σε όλα τα πληκτρολόγια (καταγράφει πλήκτρα ανεξάρτητα από την εστίαση στο πρόγραμμα).
- «Ακούει» και στέλνει όποτε γίνονται συμβάντα με το πληκτρολόγιο.
- Λειτουργεί σε λειτουργικά συστήματα Windows και Linux, με πειραματική υποστήριξη σε OS X.
- Περιέχει μόνο γλώσσα Python, δεν υπάρχουν μονάδες της γλώσσας C για να μεταγλωττιστούν.
- Μηδενικές εξαρτήσεις.
- Python 2 και 3.
- Σύνθετη υποστήριξη πλήκτρων πρόσβασης.
- Περιλαμβάνει API υψηλού επιπέδου.
- Καταγράφει πλήκτρα όπως είναι στην πραγματική διάταξη με πλήρη υποστήριξη διεθνοποίησης.
- Τα συμβάντα καταγράφονται αυτόματα σε ξεχωριστό νήμα χωρίς να εμποδίζουν το κύριο πρόγραμμα.
- Δοκιμασμένο και τεκμηριωμένο.
- Δεν σπάει τα τονισμένα νεκρά πλήκτρα.
- Υποστήριξη ποντικού διαθέσιμη μέσω της βιβλιοθήκης Mouse.

## Time 4.4.δ

Η time αποτελεί βιβλιοθήκη της γλώσσας προγραμματισμού Python, η οποία παρέχει στον χρήστη διάφορες λειτουργίες που σχετίζονται με τον χρόνο. Οι περισσότερες συναρτήσεις της καλούν συναρτήσεις της βιβλιοθήκης C με το ίδιο όνομα (Python, 2022a).

## Daytime 4.5.ε

Η datetime είναι βιβλιοθήκη της γλώσσας προγραμματισμού Python, η οποία δίνει στον χρήστη την δυνατότητα να χειριστεί ημερομηνίες καθώς και ώρες. Ενώ υποστηρίζει την αριθμητική ημερομηνία και ώρα, η υλοποίηση εστιάζεται στην αποτελεσματική εξαγωγή χαρακτηριστικών για τον χειρισμό και την μορφοποίηση εξόδου. Τα αντικείμενα αυτά χαρακτηρίζονται ως «ενημερωμένα» ή «αφελής», ανάλογα με το αν περιλαμβάνουν ή όχι πληροφορίες της ζώνης ώρας (Python, 2022b).

## Sys 4.6.στ

System-specific parameters and functions ή Sys είναι μια βιβλιοθήκη της γλώσσας προγραμματισμού Python η οποία παρέχει πρόσβαση σε ορισμένες μεταβλητές που χρησιμοποιούνται ή διατηρούνται από τον διερμηνέα καθώς και σε συναρτήσεις που αλληλοεπιδρούν έντονα με αυτόν (sys — System-specific parameters and functions — Python 3.10.7 documentation, 2022).

## Tkinter 4.7.ζ

Το Tkinter (Tk Interface) είναι μία βιβλιοθήκη γραφικής διεπαφής χρήστη της γλώσσας Python. Είναι διαθέσιμη στις περισσότερες πλατφόρμες Unix, macOS καθώς και σε λειτουργικά συστήματα Windows. Το Tkinter υποστηρίζει μια σειρά από εκδόσεις Tcl και Tk, κατασκευασμένες με ή χωρίς υποστήριξη νήματος. Δεν αποτελεί μία μόνο βιβλιοθήκη αλλά αποτελείτε από μερικές ξεχωριστές βιβλιοθήκες, από τις οποίες η κάθε μία έχει διαφορετική λειτουργικότητα και την δικιά της επίσημη οδηγία. Συγκεκριμένα, αυτές είναι οι Tcl, Tk και Ttk. Tcl είναι γλώσσα προγραμματισμού με δυναμική ερμηνεία όπως η γλώσσα Python, αλλά κυρίως ενσωματώνεται σε εφαρμογές C ως μηχανή δημιουργίας σεναρίων ή ως γραφική διεπαφή για το Tk (Python, 2022c). Η Tk υλοποιείται στην C και χρησιμοποιείται στην διαχείριση των γραφικών στοιχείων GUI, με κάθε αντικείμενο Tk να έχει ενσωματωμένο το δικό του στιγμιότυπο του διερμηνέα Tcl (Python, 2022c). Τέλος, το Ttk (themed Tk) είναι τα νεότερα γραφικά στοιχεία Tk που αναπτύχθηκαν με πολύ καλύτερη εμφάνιση, η οποία διαφέρει ανά λογισμικό σε αντίθεση με την βιβλιοθήκη Tk (Python, 2022c).

## Logging 4.8.η

Η βιβλιοθήκη logging της γλώσσας προγραμματισμού Python, καθιστά δυνατή την αποθήκευση πληροφορίας όπως είναι για παράδειγμα ποιος χρήστης ή IP απέκτησε πρόσβαση στο σύστημα. Επίσης μπορεί να παρουσιάσει αναλυτικά τις πληροφορίες σε περίπτωση που παρουσιαστεί σφάλμα. Με την πληροφορία που διαθέτει καθιστάτε εύκολη η διόρθωση σφαλμάτων αλλά και η ανάλυση απόδοσης ενός συστήματος. Μέσω του logger ο χρήστης είναι σε θέση να καταγράψει την πληροφορία που επιθυμεί, έχοντας ως προεπιλογή πέντε επίπεδα που υποδεικνύουν την σοβαρότητα των συμβάντων από τα οποία, κάθε ένα έχει μια αντίστοιχη μέθοδο που μπορεί να χρησιμοποιηθεί για την καταγραφή. Τα επίπεδα σε αύξουσα σειρά είναι (Ajitsaria, 2022):

- Εντοπισμός σφαλμάτων ή DEBUG.
- Πληροφορία ή INFO.
- Προειδοποίηση ή WARNING.
- Σφάλμα ή ERROR.
- Κρίσιμο ή CRITICAL.

### Pandas 4.9.0

Pandas, είναι μια βιβλιοθήκη της γλώσσας Python η οποία ειδικεύεται στην ανάλυση δεδομένων. Δημιουργήθηκε από τον Wes McKinney το 2008 ως ένα ισχυρό και ευέλικτο εργαλείο ποσοτικής ανάλυσης το οποίο ύστερα εξελίχθηκε σε μια από τις πιο δημοφιλείς βιβλιοθήκες της γλώσσας Python (Mode, 2022). Η βιβλιοθήκη Pandas έχει θεμελιωθεί πάνω σε δύο βασικές βιβλιοθήκες τις Python, το Matplotlib για την οπτικοποίηση των δεδομένων και NumPy για τις μαθηματικές πράξεις (Mode, 2022). Λειτουργεί ως περιτύλιγμα, επιτρέποντας στον χρήστη να έχει πρόσβαση και να μπορεί να χρησιμοποιήσει πολλές από τις μεθόδους των άλλων βιβλιοθηκών με χρήση λιγότερου κώδικα (Mode, 2022). Η βιβλιοθήκη Pandas εισήγαγε στην γλώσσα δύο νέους τύπους αντικειμένων για την αποθήκευση δεδομένων οι οποίοι οδήγησαν στην διευκόλυνση αναλυτικών εργασιών και την εξάλειψη της ανάγκης εναλλαγής προγραμματιστικής γλώσσας. Αυτά τα αντικείμενα είναι οι σειρές οι οποίες έχουν παρόμοια δομή με της λίστες καθώς και τα DataFrames τα οποία έχουν δομή πίνακα (Mode, 2022). Τέλος, κύρια χαρακτηριστικά και λειτουργίες της βιβλιοθήκης αποτελούν (Pandas, 2022):

- Εργαλεία για ανάγνωση καθώς και εγγραφή δεδομένων μεταξύ δομών δεδομένων στην μνήμη αλλά και διαφορετικών μορφών αρχεία (CSV, text files, Microsoft Excel, SQL databases and HDF5.
- Έξυπνη στοίχιση δεδομένων και ολοκληρωμένος χειρισμός δεδομένων που λείπουν.
- Ευέλικτη αναμόρφωση και περιστροφή συνόλων δεδομένων.
- Έξυπνος τεμαχισμός βάσει ετικετών, δείκτη και υποσυνόλων μεγάλων συνόλων δεδομένων.
- Οι στήλες μπορούν να εισαχθούν και να διαγραφούν από δομές δεδομένων για μεταβλητότητα μεγέθους.
- Επιτρέπει λειτουργίες διαχωρισμού, εφαρμογής και συνδυασμού στα σύνολα δεδομένων.
- Υψηλή απόδοση ένωσης συνόλων δεδομένων.
- Ιεραρχικός δείκτης αξόνων παρέχει έναν διαισθητικό τρόπο εργασίας με δεδομένα υψηλών διαστάσεων σε μία δομή χαμηλότερης διάστασης.
- Εξαιρετικά βελτιστοποιημένο για απόδοση.

## Λειτουργία και σενάρια χρήσης 4.2

Βασίζοντας στην γενική αρχιτεκτονική που δημιουργήθηκε στα πλαίσια της εργασίας (Σχήμα 12), αναπτύχθηκε το σύστημα RT_FaceBlur. Όπως έχει αναφερθεί, κύριος στόχος του συστήματος αποτελεί η διασφάλιση της προστασίας των προσωπικών δεδομένων των πολιτών όποτε καταγράφονται αυτοί από συστήματα καμερών κλειστής παρακολούθησης. Για την πλήρη υλοποίηση του συστήματος χρησιμοποιήθηκαν τα εργαλεία που αναφέρθηκαν παραπάνω με πρότυπο το Σχήμα 12. Συγκεκριμένα, υλοποιήθηκαν τρείς μονάδες.

- Για την υλοποίηση της βάσης δεδομένων (Database), δημιουργήθηκε μονάδα με όνομα `DataBase_Generator`. Το συγκεκριμένο αρχείο θα καλείται από το κύριο πρόγραμμα με την εκκίνησή του και θα πραγματοποιήσει την δημιουργία της βάσης δεδομένων στην οποία είναι αποθηκευμένα τα χαρακτηριστικά του κάθε χρήστη, δηλαδή το όνομα και ο κωδικός που θα χρησιμοποιηθούν για την ταυτοποίησή του καθώς και ο αριθμός ID και το επίπεδο εξουσιοδότησής του. Γίνεται χρήση της βιβλιοθήκης Pandas της γλώσσας Python για την δημιουργία της βάσης ως τύπο δεδομένων DataFrame, το οποίο ύστερα επιστρέφεται στο κύριο πρόγραμμα.

- Για την υλοποίηση του συστήματος σύνδεσης καθώς και της διεπαφής που θα χρησιμοποιήσει ο χρήστης (Login and GUI), δημιουργήθηκε μονάδα με όνομα `Login_System`. Ειδικότερα, γίνεται χρήση των βιβλιοθηκών sys και tkinter της γλώσσας Python. Η μονάδα καλείται αφού δημιουργηθεί η βάση δεδομένων, την οποία θα δεχθεί ως όρισμα και μέσω της οποίας θα γίνουν οι απαραίτητες ταυτοποιήσεις. Μέσω της βιβλιοθήκης tkinter, η μονάδα ζητάει από τον χρήστη την εισαγωγή των απαραίτητων στοιχείων για την επίτευξη της ταυτοποίησης μέσω γραφικών διεπαφών, καθώς και εμφανίζει τα κατάλληλα μηνύματα σε κάθε περίπτωση, επιτυχίας ή αποτυχίας σύνδεσης.

```
#Tkinter window.
window = tk.Tk()
#Hide the root windows.
window.withdraw()
#Get the username through a GUI censored.
password = simpledialog.askstring(title="Login system", prompt="Password:\t\t\t\t", show='*')
```

**Σχήμα 13.** Απόσπασμα του κώδικα που δημιουργήθηκε για να ζητηθεί ο κωδικός πρόσβασης του χρήστη καθώς και η επικάλυψη αυτού.

Στην συνέχεια με την χρήση της βιβλιοθήκης sys, αν ο χρήστης αποτύχει να κάνει ορθή ταυτοποίηση τρείς φορές συνεχόμενα τότε το σύστημα θα τερματίσει. Τέλος, όταν πραγματοποιηθεί επιτυχής ταυτοποίηση, επιστρέφεται ο κωδικός ID του συνδεδεμένου χρήστη καθώς και το επίπεδο εξουσιοδότησής του στο κύριο πρόγραμμα.

- Για την υλοποίηση του συστήματος το οποίο θα παράγει αρχεία καταγραφής (Log file), δημιουργήθηκε μονάδα με όνομα `Logging_System`. Η λειτουργικότητα του συγκεκριμένου αρχείου κρίθηκε απαραίτητη για το σύστημα. Από τα πρώτα προβλήματα που συζητήθηκαν κατά την ανάπτυξη του συστήματος, κύριο ήταν η επίτευξη της ευθύνης. Αποτελούσε επιτακτική ανάγκη η πρόσβαση σε πληροφορίες ώστε σε περίπτωση κατάχρησης του συστήματος, να είναι δυνατή η δίωξη των υπεύθυνων. Η ύπαρξη όμως της συγκεκριμένης πληροφορίας μπορεί να λειτουργήσει και ως αποτρεπτικό. Συγκεκριμένα, το σύστημα καταγραφής είναι σε θέση να καταγράψει το ID του εκάστοτε συνδεδεμένου χρήστη, καθώς και την συγκεκριμένη ώρα και ημερομηνία που αυτός πραγματοποίησε σύνδεση, αποσύνδεση και έκανε άρση των μέτρων ασφάλειας. Για την υλοποίηση της παραπάνω λειτουργίας, το σύστημα με την κλήση του, αφού έχει ολοκληρωθεί η λειτουργία του κύριου προγράμματος, δέχεται τον αριθμό ID του συνδεδεμένου χρήστη, το επίπεδο εξουσιοδότησής του, καθώς και την ημερομηνία και ώρα όποτε αυτός πραγματοποίησε είσοδο, έξοδο, και άρση των συστημάτων ασφάλειας. Με την χρήση της βιβλιοθήκης logging της γλώσσας Python, καταγράφονται τα παραπάνω στοιχεία και τέλος τερματίζει το σύστημα.

```
INFO:root:
User ID:[13]
        * Accessed the system at: 2022-09-25 15:35:31.587952
        * Logged out of the system at: 2022-09-25 15:36:56.818528
        * Lifted security measures at: 2022-09-25 15:36:39.217356
INFO:root:
User ID:[14]
        * Accessed the system at: 2022-09-26 18:11:43.531859
        * Logged out of the system at: 2022-09-26 18:18:56.021717
INFO:root:
User ID:[11]
        * Accessed the system at: 2022-09-26 18:31:53.766596
        * Logged out of the system at: 2022-09-26 18:50:03.453467
        * Lifted security measures at: 2022-09-26 18:33:20.541633
                                       2022-09-26 18:46:04.205688
```

**Σχήμα 14.** Παράδειγμα αρχείου καταγραφής.

Με την ολοκλήρωση της ανάπτυξης των μονάδων του συστήματος ολοκληρώθηκε και το κύριο πρόγραμμα το οποίο πραγματοποιεί το κάλεσμα όλων αυτών και εκτελεί την κύρια λειτουργία θόλωσης. Έγινε χρήση των βιβλιοθηκών OpenCV (cv2), Keyboard, time και datetime. Το πρόγραμμα καλεί τις απαραίτητες συναρτήσεις που δημιουργήθηκαν και μέσω των συναρτήσεων της βιβλιοθήκης OpenCV σε συνδυασμό με τον αλγόριθμο `Haarcascade_frontalface_alt.xml`, πραγματοποιείται καταγραφή πραγματικής ροής βίντεο και ταυτόχρονα αναγνώριση, επεξεργασία, και θόλωση των προσώπων που καταγράφονται.

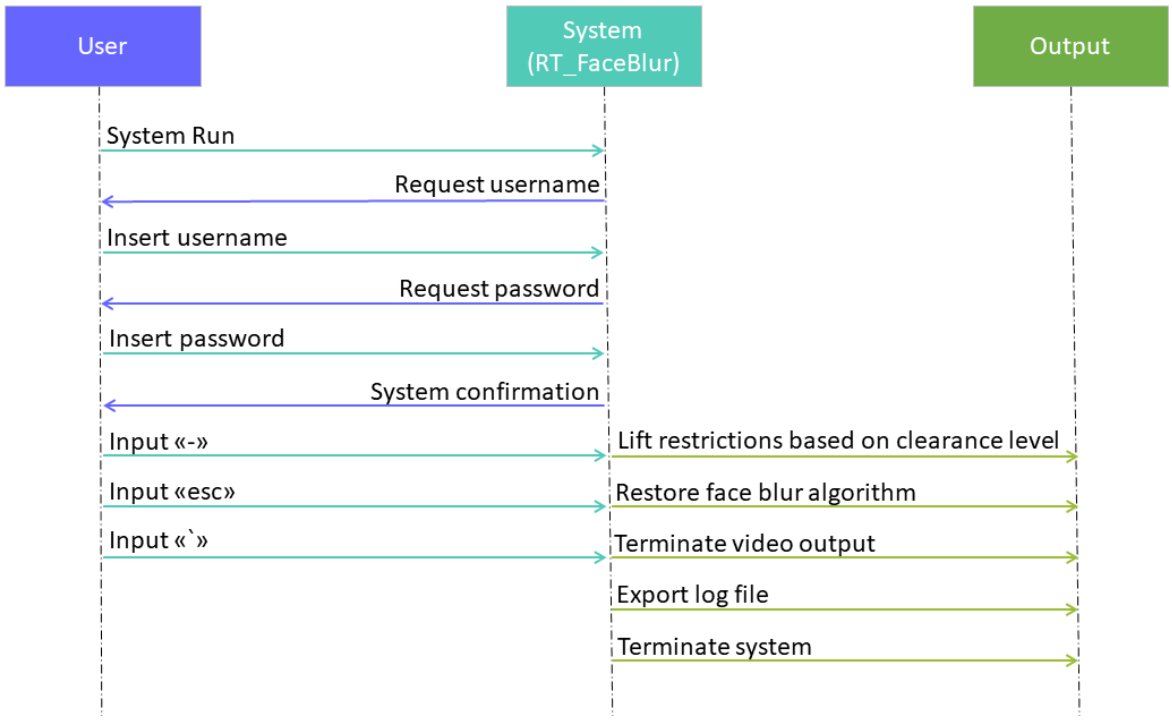
```python
face_cascade = cv2.CascadeClassifier("haarcascade_frontalface_alt.xml")

#Video capture from webcam.
capture = cv2.VideoCapture(0, cv2.CAP_DSHOW)

#Check if the camera opened successfully.
if (capture.isOpened() == False):
  print("Error, feed not found.")
```

**Σχήμα 15.** Απόσπασμα του κώδικα το οποίο κάνει εισαγωγή του αλγορίθμου, ξεκινάει την καταγραφή της ζωντανής ροής και εμφανίζει κατάλληλο μήνυμα σε περίπτωση αποτυχίας.

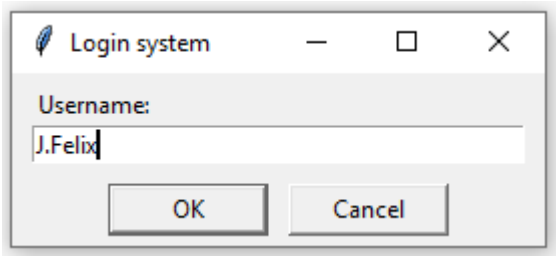
Ανάλογα με το επίπεδο εξουσιοδότησης του εκάστοτε χρήστη το πρόγραμμα θα έχει διαφορετική λειτουργία όποτε ο χρήστης επιθυμεί να κάνει άρση των μέτρων ασφαλείας πατώντας το πλήκτρο «-». Οπότε το σύστημα θα έχει συνολικά τέσσερα πιθανά σενάρια, ένα για κάθε επίπεδο εξουσιοδότησης και ένα για την αποτυχία σύνδεσης.




**Σχήμα 16.** Ακολουθιακό διάγραμμα αλληλεπίδρασης του συστήματος σε πρότυπο UML.

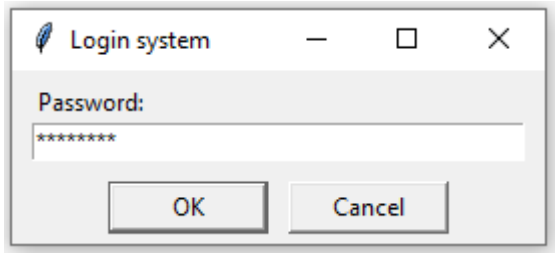
## Εξουσιοδότηση Βαθμού 0 4.2.α

Με την έναρξη του προγράμματος εμφανίζεται η παρακάτω διεπαφή και ζητάτε από τον χρήστη το όνομα σύνδεσής του.



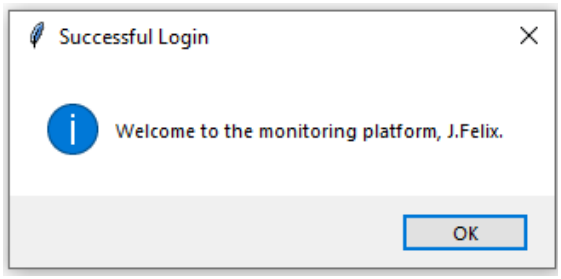

**Σχήμα 17.** Διεπαφή ονόματος χρήσης.

Αφού ο χρήστης κάνει εισαγωγή του ονόματος χρήσης, μια νέα διεπαφή ζητάει τον κωδικό.

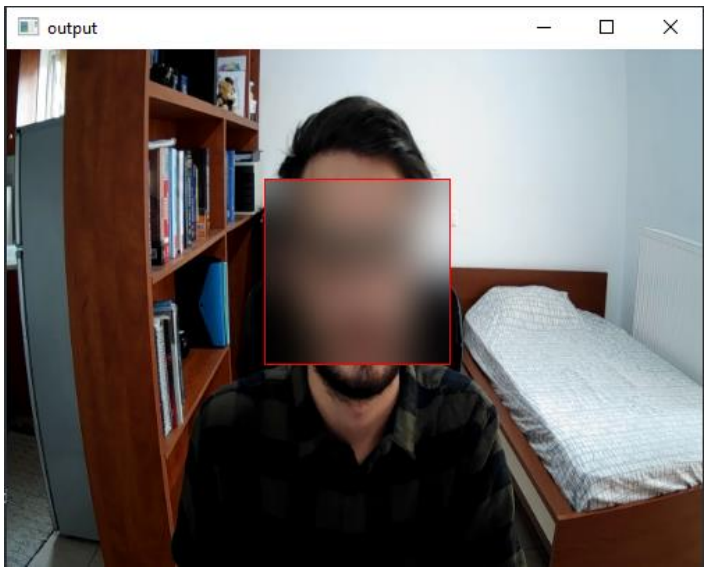



**Σχήμα 18.** Διεπαφή κωδικού πρόσβασης με απόκρυψη αυτού.

Στην συνέχεια, με την εισαγωγή ορθού κωδικού εμφανίζεται μήνυμα επιτυχής σύνδεσης, καθώς και η ροή βίντεο που καταγράφεται σε πραγματικό χρόνο αφού γίνει επεξεργασία αυτού και θόλωση των προσώπων, όπου αυτά αναγνωρίζονται.




**Σχήμα 19.** Διεπαφή επιτυχής σύνδεσης.




**Σχήμα 20.** Παράθυρο που παρέχει την επεξεργασμένη ροή βίντεο για ανάλυση.

Καθώς ο χρήστης στο συγκεκριμένο σενάριο έχει επίπεδο εξουσιοδότησης 0 (clearance 0), το πάτημα του πλήκτρου «-» δεν θα οδηγήσει στην άρση των δικλείδων ασφαλείας και η θόλωση θα παραμείνει. Τέλος με πάτημα του πλήκτρου «`» τερματίζει η λειτουργία και η επεξεργασία της ροής, και το σύστημα προσθέτει στο αρχείο καταγραφής τις κατάλληλες πληροφορίες.

## Εξουσιοδότηση Βαθμού 1 4.2.β

Τα αρχικά βήματα είναι παρόμοια σε αυτό το σενάριο. Ο χρήστης καλείται να εισάγει το όνομα χρήσης του (Σχήμα 17) και ύστερα τον κωδικό πρόσβασης (Σχήμα 18). Αφού γίνει ορθή ταυτοποίηση εμφανίζεται κατάλληλο μήνυμα (Σχήμα 18), καθώς και η ροή βίντεο που καταγράφεται σε πραγματικό χρόνο αφού γίνει επεξεργασία αυτού και θόλωση των προσώπων, όπου αυτά αναγνωρίζονται (Σχήμα 19). Στην συνέχεια, αν ο χρήστης με εξουσιοδότηση 1 (clearance 1) επιλέξει να πραγματοποιήσει άρση των μέτρων ασφάλειας πατώντας το πλήκτρο «-», το σύστημα θα κάνει αναστολή του κώδικα που τροποποιεί την εικόνα και πραγματοποιεί την θόλωση για 30 δευτερόλεπτα, εμφανίζοντας την ροή βίντεο χωρίς να έχει γίνει επεξεργασία.


**Σχήμα 21.** Εμφάνιση μη επεξεργασμένης ροής βίντεο.

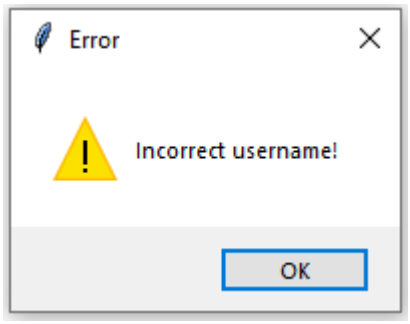
Επιπρόσθετα, ο χρήστης έχει την επιλογή να επαναφέρει την θόλωση στο βίντεο πατώντας το πλήκτρο «esc» οποιαδήποτε στιγμή, χωρίς να χρειάζεται να περιμένει 30 δευτερόλεπτα για την επαναφορά της. Τέλος, ξανά με πάτημα του πλήκτρου «`» σταματάει η λειτουργία και η επεξεργασία της ροής και προστίθενται στο αρχείο καταγραφής οι πληροφορίες του χρήστη.

## Εξουσιοδότηση Βαθμού 2 4.2.γ

Στο σενάριο που ο χρήστης έχει τον μέγιστο βαθμό εξουσιοδότησης (clearance 2), αρχικά γίνεται όμοια εισαγωγή του ονόματος χρήσης (Σχήμα 17) καθώς και εισαγωγή του κωδικού πρόσβασης (Σχήμα 18). Ύστερα, με την πραγματοποίηση ορθής σύνδεσης στο σύστημα εμφανίζεται μήνυμα επιτυχίας (Σχήμα 19) και το παράθυρο που θα εμφανίσει την επεξεργασμένη ροή βίντεο με θολωμένα τα πρόσωπα (Σχήμα 20). Στην περίπτωση που ο χρήστης επιθυμεί να εμφανίσει τα δεδομένα των ατόμων που καταγράφηκαν από τις κάμερες κλειστού κυκλώματος πατώντας το πλήκτρο «-», θα γίνει άρση της θόλωσης (Σχήμα 21) μέχρι ο ίδιος την επαναφέρει χειροκίνητα πατώντας το πλήκτρο «esc» ή μέχρι να τερματίσει την λειτουργία του συστήματος πατώντας «`», όπου θα γίνει καταγραφή των δεδομένων του στο κατάλληλο αρχείο.

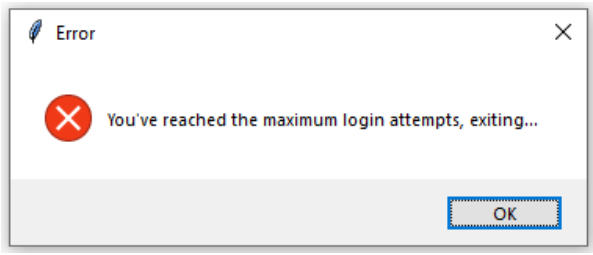
## Λανθασμένη εισαγωγή στοιχείων 4.2.δ

Ακόμη ένα πιθανό σενάριο αποτελεί η αδυναμία του χρήστη να εισάγει τα ορθά στοιχεία κατά την διάρκεια της ταυτοποίησης. Όταν ο χρήστης εισάγει λανθασμένο όνομα σύνδεσης, το σύστημα θα εμφανίσει διεπαφή μηνύματος λάθους και ύστερα θα ζητήσει ξανά το όνομα χρήσης (Σχήμα 17) μέχρι ο χρήστης να εισάγει το σωστό.




**Σχήμα 22.** Διεπαφή λανθασμένης εισαγωγής ονόματος χρήσης.

Αφού ο χρήστης εισάγει το σωστό όνομα σύνδεσης, αν στην συνέχεια εισάγει λανθασμένο κωδικό πρόσβασης, τότε το σύστημα θα εμφανίσει ξανά διεπαφή με μήνυμα λάθους και ύστερα θα ζητήσει ξανά τον κωδικό (Σχήμα 18) μέχρι ο χρήστης να εισάγει τον σωστό ή μέχρι να κάνει συνεχόμενα τρία λάθη. Τότε το σύστημα θα εμφανίσει μήνυμα στο οποίο ο χρήστης θα ενημερώνεται πως χρησιμοποίησε όλες τις δυνατές προσπάθειες και πως το πρόγραμμα θα τερματίσει την λειτουργία του.




**Σχήμα 23.** Διεπαφή συνεχόμενων λανθασμένων προσπαθειών και τερματισμού του συστήματος.

# ΚΕΦΑΛΑΙΟ 5 Συμπεράσματα

Στόχος της πτυχιακής εργασίας ήταν η άμβλυνση των προβλημάτων που προκύπτουν κατά την συλλογή προσωπικών δεδομένων και συγκεκριμένα κατά την καταγραφή των ατόμων από κάμερες παρακολούθησης. Αν δεν πραγματοποιούνται έλεγχοι και δεν υπάρχουν καθιερωμένα συστήματα για την καταπολέμηση αυτών, τότε οι περιπτώσεις καταπάτησης της ιδιωτικότητας των ατόμων θα αυξηθούν ανεξέλεγκτα. Με την χρήση διαβαθμισμένης πρόσβασης, χρησιμοποιώντας επίπεδα εξουσιοδότησης, καθώς και με την καταγραφή των πληροφοριών του εκάστοτε χρήστη για την διασφάλιση της ευθύνης μειώνονται έτσι σημαντικά οι πιθανότητες εμφάνισης κακομεταχείρισης του συστήματος και συνεπώς καταπάτησης της ιδιωτικότητας των πολιτών. Όμως, δεν γίνεται να αποφευχθεί ολοκληρωτικά η κατάχρηση των δεδομένων προσωπικής πληροφορίας. Το σύστημα σχεδιάστηκε έτσι ώστε σε περίπτωση που γίνει παραβίαση των δικαιωμάτων να υπάρχει δυνατότητα εύρεσης του υπεύθυνου ατόμου.

Σε μελλοντική εργασία, με την περεταίρω ανάπτυξη του συστήματος, θα γίνει επιδίωξη διασφάλισης της προστασίας των προσωπικών δεδομένων των πολιτών ακόμη περισσότερο. Αυτό θα επιτευχθεί με την ολοκλήρωση της μεθόδου ελέγχου πρόσβασης βάσει ιδιοτήτων, υλοποιώντας στο σύστημα και το Policy Decision Point, το οποίο αποτελεί οντότητα η οποία λαμβάνει αποφάσεις εξουσιοδότησης για τον εαυτό της καθώς και για τις υπόλοιπες οντότητες στο σύστημα παρέχοντας έτσι έναν ολοκληρωμένο έλεγχο πρόσβασης.

# ΒΙΒΛΙΟΓΡΑΦΙΑ


ACLU (American Civil Liberties Union), 2002. *What's Wrong With Public Video Surveillance?* [online] Available at: <https://www.aclu.org/other/whats-wrong-public-video-surveillance> [Accessed 17 July 2022].

Ajitsaria, A., 2022. *Logging in Python.* Real Python [online] Available at: <https://realpython.com/python-logging/> [Accessed 22 September 2022].

ΑΠΔ (Αρχή Προστασίας Δεδομένων), 2022. *ΑΠΟΦΑΣΗ 35/2022, Καταγγελία κατά Clearview AI*. [online] available at: < https://www.dpa.gr/sites/default/files/2022-07/35_2022%20anonym_0.pdf> [Accessed 23 September 2022].

ΑΠΔ (Αρχή Προστασίας Δεδομένων), n.d. a. *Συμμόρφωση με ΓΚΠΔ*. [online] Available at: <https://www.dpa.gr/el/foreis/odigos_gkpd> [Accessed 2 October 2022].

ΑΠΔ (Αρχή Προστασίας Δεδομένων), n.d. b. *Συστήματα βιντεοεπιτήρησης*: *Συχνές ερωτήσεις*. [online] Available at: <https://www.dpa.gr/el/enimerwtiko/thematikes_enotites/eisagwgi_videoepitirisi/faq_videoepitirisi> [Accessed 2 October 2022].

ΑΠΔ (Αρχή Προστασίας Δεδομένων), n.d. c. 2022. *Συστήματα βιντεοεπιτήρησης σε οικίες και πολυκατοικίες*. [online] Available at: <https://www.dpa.gr/el/enimerwtiko/thematikes_enotites/eisagwgi_videoepitirisi/oikies_videoepitirisi> [Accessed 2 October 2022].

Avelino, T., 2011. *python-opencv-detect/haarcascade_frontalface_alt.xml at master · avelino/python-opencv-detect*. [online] GitHub. Available at: <https://github.com/avelino/python-opencv-detect/blob/master/haarcascade_frontalface_alt.xml> [Accessed 23 September 2022].

Bischoff, P., 2022. *Surveillance Camera Statistics: Which City has the Most CCTV Cameras?.* [online] Comparitech. Available at: <https://www.comparitech.com/vpn-privacy/the-worlds-most-surveilled-cities/> [Accessed 4 August 2022].

Capitani di Vimercati, S., Samarati, P. and Sandhu, R., 2014. *Chapter 47*: *Access Control*, Computing Handbook, 3rd ed., CRC Press.

Cavallaro, A., 2007. Privacy in Video Surveillance [In the Spotlight]. *IEEE Signal Processing Magazine*, [online] 24(2), pp.166-168. Available at: <https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=4117949> [Accessed 5 August 2022].

Cavoukian, A., 2010. *Privacy By Design: The 7 Foundational Principles, Implementation and Mapping of Fair Information Practices*, [online] Available at: https://privacysecurityacademy.com/wp-content/uploads/2020/08/PbD-Principles-and-Mapping.pdf.

Cavoukian, A., Chibba, M., Williamson, G. and Ferguson, A., 2015. The Importance of ABAC: Attribute-Based Access Control to Big Data: Privacy and Context. *Ryerson University*, [online] Available at: <https://www.torontomu.ca/content/dam/pbdce/papers/The-Importance-of-ABAC-to-Big-Data-05-2015.pdf> [Accessed 17 October 2022].

Chatterjee, S. and Sreenivasulu N.S., 2019. *Personal data sharing and legal issues of human rights in the era of Artificial Intelligence*, *International Journal of Electronic Government Research*, 15(3), pp. 21–36, [online] Available at: https://doi.org/10.4018/ijegr.2019070102.

Doberstein, C., Charbonneau, É., Morin, G. and Despatie, S., 2021. Measuring the Acceptability of Facial Recognition-Enabled Work Surveillance Cameras in the Public and Private Sector. *Public Performance & Management Review*, [online] 45(1), pp.198-227. Available at: <https://www.tandfonline.com/doi/abs/10.1080/0731129X.2002.9992113?journalCode=rcre20> [Accessed 4 August 2022].

Evening Standard, 2012. *We're watching you: 'Britons caught on CCTV 70 times a day'*. [online] Available at: <https://www.standard.co.uk/hp/front/we-re-watching-you-britons-caught-on-cctv-70-times-a-day-6573202.html> [Accessed 1 August 2022].

Faitelson, D. and Tyszberowicz, S., 2017. UML Diagram Refinement (Focusing on Class-and Use Case Diagrams). *2017 IEEE/ACM 39th International Conference on Software Engineering (ICSE)*, [online] p.742. Available at: <https://ieeexplore.ieee.org/abstract/document/7985709/citations#citations> [Accessed 19 July 2022].

Goold, B., 2002. Privacy rights and public spaces: CCTV and the problem of the “unobservable observer”. *Criminal Justice Ethics*, [online] 21(1), pp.21-27. Available at: <https://www.tandfonline.com/doi/abs/10.1080/0731129X.2002.9992113?journalCode=rcre20> [Accessed 28 July 2022].

Hempel, L. and Töpfer, E., 2004. *Working Paper No.15 CCTV in Europe: Final Report*. Urbaneye, [online] 15, p.18-29. Available at: <http://www.urbaneye.net/results/ue_wp15.pdf> [Accessed 4 August 2022].

Honovich, J., 2015. *Frightening Surveillance Misuse - Spying on Women*. [online] IPVM. Available at: <https://ipvm.com/reports/guard-using-cctv-to-spy> [Accessed 17 July 2022].

IFSEC Global, 2021. *Role of CCTV Cameras: Public, Privacy and Protection*. [online] Available at: https://www.ifsecglobal.com/video-surveillance/role-cctv-cameras-public-privacy-protection/ [Accessed 16 October 2022].

Jacobson, I., 2004. Use cases – Yesterday, today, and tomorrow. *Software & Systems Modeling*, [online] 3(3), pp.210-220. Available at: <https://link.springer.com/article/10.1007/s10270-004-0060-3> [Accessed 18 July 2022].

Kurtanovic, Z. and Maalej, W., 2017. Automatically Classifying Functional and Non-functional Requirements Using Supervised Machine Learning. *2017 IEEE 25th International Requirements Engineering Conference (RE)*, [online] pp.490-495. Available at: <https://ieeexplore.ieee.org/abstract/document/8049171> [Accessed 17 July 2022].

Mode, 2022. *Pandas – Python Library*. [online] Available at: <https://mode.com/python-tutorial/libraries/pandas/> [Accessed 22 September 2022].

Molnar, A. and Warren, I., 2020. Governing Liberty Through Accountability: Surveillance Reporting as Technologies of Governmentality. *Critical Criminology*, [online] 28(1), pp.13-26. Available at: <https://link.springer.com/article/10.1007/s10612-020-09490-9> [Accessed 17 July 2022].

OpenCV, 2022. *Open Source Computer Vision: Introduction*. [online] Available at: <https://docs.opencv.org/4.x/d1/dfb/intro.html> [Accessed 23 September 2022].

Pandas, 2022. *Python Data Analysis Library: About pandas.* [online] Available at: <https://pandas.pydata.org/about/> [Accessed 22 September 2022].

Pandey, D., Suman, U. and Ramani, A., 2010. An Effective Requirement Engineering Process Model for Software Development and Requirements Management. *2010 International Conference on Advances in Recent Technologies in Communication and Computing*, [online] pp.287-291. Available at: <https://ieeexplore.ieee.org/document/5656776> [Accessed 17 July 2022].

Papagiannakopoulou, E., Koukovini, M., Lioudakis, G., Dellas, N., Kaklamani, D. and Venieris, L., 2014. Leveraging Semantic Web Technologies for Access Control. *Emerging Trends in ICT Security*, [online] p.493. Available at: <https://www.sciencedirect.com/science/article/pii/B978012411474600030X> [Accessed 17 October 2022].

PyPI, 2020. *Keyboard 0.13.5*. [online] Available at: <https://pypi.org/project/keyboard/> [Accessed 22 September 2022].

Python, 2022a. *Time – Time access and conversions — Python 3.10.7 documentation*. [online] Available at: <https://docs.python.org/3/library/time.html> [Accessed 22 September 2022].

Python, 2022b. *Datetime — Basic date and time types — Python 3.10.7 documentation*. [online] Available at: <https://docs.python.org/3/library/datetime.html> [Accessed 22 September 2022].

Python, 2022c. *tkinter — Python interface to Tcl/Tk — Python 3.10.7 documentation*. [online] Available at: <https://docs.python.org/3/library/tkinter.html> [Accessed 22 September 2022].

Ralph, P., 2012. The illusion of requirements in software development. *Requirements Engineering*, [online] 18(3), pp.293-296. Available at: <https://link.springer.com/article/10.1007/s00766-012-0161-4#citeas> [Accessed 18 July 2022].

Ratcliffe, J., Taniguchi, T. and Taylor, R., 2009. The Crime Reduction Effects of Public CCTV Cameras: A Multi-Method Spatial Approach. *Justice Quarterly*, [online] 26(4), pp.746-770. Available at: <https://www.tandfonline.com/doi/full/10.1080/07418820902873852?needAccess=true> [Accessed 5 August 2022].

Regulation (EU) 2016/679 of the European parliament and of the council, (2016), Official Journal of the European Union L 119/1. [online]. Available at: https://eur-lex.europa.eu/eli/reg/2016/679/oj [Accessed 18 October 2022].

Ropohl, G., 1999. Philosophy of Socio-Technical Systems. *Society for Philosophy and Technology Quarterly Electronic Journal*, 4(3), pp.59-71.

Samarati, P. and Capitani di Vimercati, S., 2001. Access Control: Policies, Models, and Mechanisms. *Foundations of Security Analysis and Design*, [online] 2171, pp.141,151. Available at: <https://link.springer.com/chapter/10.1007/3-540-45608-2_3> [Accessed 16 October 2022].

Simplilearn, 2022. *14 Most Important Python Features and How to Use them*. [online] Available at: <https://www.simplilearn.com/python-features-article> [Accessed 22 September 2022].

Summerfield, M., 2009. *Programming in Python 3: a complete introduction to the Python language*. 2nd ed. Addison-Wesley, pp.1-5.

Veskoukis, V., 2015. *Στοιχεία Τεχνολογίας Λογισμικού*. 1st ed. Kallipos, Open Academic Editions, pp.106-108.

Von Hirsch, A., Garland, D. and Wakefield, A., 2004. *Ethical and Social Perspectives on Situational Crime Prevention*. 1st ed. Hart Publishing Ltd., pp.59-76.

## ΠΑΡΑΡΤΗΜΑ

# Κώδικας 1. RT_FaceBlur.py

```
"""MAIN PROGRAM - Real-time face blurring algorithm"""

import cv2
import keyboard
import time
import datetime
from DataBase_Generator import generateData
from Login_System import login
from Logging_System import logData

#Function to resize an image.
def resize(image, new_width = 500):
    height, width,_ = image.shape
    ratio = height/width
    new_height = int(ratio*new_width)

    return cv2.resize(image,(new_width, new_height))

#Generate the user dataFrame.
user_data = generateData()
#Run the login system and save the ID and clearance of the connected user.
user_ID, clearance = login(user_data)

#Get current (login) time for the log file.
loginTime = datetime.datetime.now()
#Declare timestamp as an empty list.
timestamp = []

face_cascade = cv2.CascadeClassifier("haarcascade_frontalface_alt.xml")

#Video capture from webcam.
capture = cv2.VideoCapture(0, cv2.CAP_DSHOW)

#Check if the camera opened successfully.
if (capture.isOpened() == False):
  print("Error, feed not found.")

#Loop to examine frame by frame.
while True:

    #Read all the frames.
    _,frame = capture.read()

    #Resize the frame
    frame = resize(frame)

    #Face detections using cascade function detectMultiScale.
    detections = face_cascade.detectMultiScale(frame, scaleFactor = 1.1,
minNeighbors = 6)

    #Loop for each face in our capture.
    for face in detections:
        #Unpacking each face to the variables x, y, width, height.
        x, y, width, height = face

        #Blurring using GaussianBlur from OpenCV.
        source = frame[y:y+height, x:x+width]
        frame[y:y+height, x:x+width] = cv2.GaussianBlur(source, (91,91), 0)

        #Draw a boundry box around the face.
        cv2.rectangle(frame,(x,y),(x+width,y+height),(0,0,255), 1)

        #Display the result.
```

```
        cv2.imshow("output", frame)

        if cv2.waitKey(1) == 27:
            break

    #Lift the bluring algorithm at the press of the button depending on clearance.
    if keyboard.is_pressed("-") and clearance == "clearance 1":

        #Timer start.
        start = time.time()

        #Get current (blur lift timestamp) time for the log file.
        timestamp.append(datetime.datetime.now())

        while True:

            _,frame = capture.read()

            frame = resize(frame)

            detections = face_cascade.detectMultiScale(frame, scaleFactor = 1.1,
minNeighbors = 6)

            cv2.imshow("output", frame)

            if cv2.waitKey(1) == 27:
                break

            #if 30 seconds have passed break from the loop and blur the feed.
            if time.time() - start >= 30:
                break

            if keyboard.is_pressed("`"):
                break

    #Lift the bluring algorithm at the press of the button depending on clearance.
    if keyboard.is_pressed("-") and clearance == "clearance 2":

        #Get current (blur lift timestamp) time for the log file.
        timestamp.append(datetime.datetime.now())

        while True:

            _,frame = capture.read()

            frame = resize(frame)

            detections = face_cascade.detectMultiScale(frame, scaleFactor = 1.1,
minNeighbors = 6)

            cv2.imshow("output", frame)

            if cv2.waitKey(1) == 27:
                break

            if keyboard.is_pressed("`"):
                break

    #Close the window if "`" is pressed.
    if keyboard.is_pressed("`"):
        break


#Get current (logout) time for the log file.
logoutTime = datetime.datetime.now()
#Add information to the logfile.
logData(user_ID, loginTime, logoutTime, timestamp, clearance)
```

```
#Releasing the feed.
capture.release()
cv2.destroyAllWindows()
```

## Κώδικας 2. Login_System.py

```
"""LOGIN SYSTEM"""

import sys
import tkinter as tk
from tkinter import simpledialog
from tkinter import messagebox

def login(user_data):

    #User ID and clearance.
    logged_in = 0
    clearance = 0

    #Flags.
    correct_username = 0
    correct_password = 0
    pw_check = 0
    error = 0

    while correct_username == 0:

        #Tkinter window.
        window = tk.Tk()
        #Hide the root windows.
        window.withdraw()
        #Get the username through a GUI.
        username = simpledialog.askstring(title="Login system",
prompt="Username:\t\t\t\t")

        for ID, name, pword, clrnc in user_data.itertuples(index=False):
            #Check the username and password.
            if username == name:
                correct_username = 1
                while pw_check == 0:

                    #Tkinter window.
                    window = tk.Tk()
                    #Hide the root windows.
                    window.withdraw()
                    #Get the username through a GUI censored.
                    password = simpledialog.askstring(title="Login system",
prompt="Password:\t\t\t\t", show='*')

                    if password == pword:
                        correct_password = 1
                        pw_check = 1
                    #If the password is incorrect print the appropriate message and
exit after 3 attempts.
                    else:
                        messagebox.showwarning("Error", "Incorrect password!")
                        error += 1
                        if error == 3:
                            messagebox.showerror("Error", "You've reached the
maximum login attempts, exiting...")
                            sys.exit()

            #If password and username are correct change flags and save ID.
            if correct_username and correct_password == 1:
                logged_in = ID
                clearance = clrnc
            #Reset password flag.
```

```
            correct_password = 0

        if correct_username == 0:
            messagebox.showwarning("Error", "Incorrect username!")

    if not logged_in == 0:

        messagebox.showinfo("Successful Login", "Welcome to the monitoring
platform, "+username+".")

    #return the ID of the logged in user
    return logged_in, clearance
```

## Κώδικας 3. Logging_System.py

```
"""LOGGING SYSTEM"""

import logging

def logData(ID, loginTime, logoutTime, timestamp, clearance):

    ID = str(ID)
    loginTime = str(loginTime)
    logoutTime = str(logoutTime)

    #Change filename to desired path with the log file name.
    if clearance == "clearance 0":
        logging.basicConfig(filename="DataLog.log", level=logging.INFO)
        logging.info("\nUser ID:["+ID+"] \n\t* Accessed the system at:
"+loginTime+"\n\t* Logged out of the system at: "+logoutTime)

    else:
        logging.basicConfig(filename="DataLog.log", level=logging.INFO)
        logging.info("\nUser ID:["+ID+"] \n\t* Accessed the system at:
"+loginTime+"\n\t* Logged out of the system at: "+logoutTime+"\n\t* Lifted security
measures at: {}".format('\n\t                                    '.join(map(str,
timestamp))))

    logging.shutdown()
```

## Κώδικας 4. DataBase_Generator.py

```
"""Data Base Generator"""

import pandas as pd

def generateData():

    #Create a dataFrame and return it.
    header = ['id', 'username', 'password', 'clearance']
    data = [[10, 'K.Thomas', 'felina@19', 'clearance 0'],
            [11, 'M.Nicholaos', '2118159!', 'clearance 2'],
            [12, 'M.Oscar', '1617#2198', 'clearance 1'],
            [13, 'S.Michael', '!vidi1234', 'clearance 1'],
            [14, 'J.Felix', 'Koump7#4321', 'clearance 0']]

    pd_userData = pd.DataFrame(data, columns=header)

    return pd_userData
```