

ΙΟΝΙΟ ΠΑΝΕΠΙΣΤΗΜΙΟ

Τμήμα Πληροφορικής



Πτυχιακή Εργασία

Ανάλυση Κρυπτογραφίας και Θεμάτων Ιδιωτικότητας

ΣΕ

Εφαρμογές Έξυπνου Πάρκινγκ

Μουτσιούνας Παναγιώτης

Επιβλέπων : Νταντογιάν Χριστόφορος

Κέρκυρα, 2022

Επιβλέπων

Νταντογιάν Χριστόφορος, Επίκουρος Καθηγητής,

Ιόνιο Πανεπιστήμιο

Τριμελής Επιτροπή

Νταντογιάν Χριστόφορος, Επίκουρος Καθηγητής,

Ιόνιο Πανεπιστήμιο

Τσώχου Αγγελική, Επίκουρη Καθηγήτρια,

Ιόνιο Πανεπιστήμιο

Μάγκος Εμμανουήλ, Αναπληρωτής Καθηγητής,

Ιόνιο Πανεπιστήμιο

Περιεχόμενα

1. Πρόλογος
2. Εισαγωγή
3. Αρχιτεκτονικές Έξυπνων Πάρκινγκ
4. Προβλήματα - Επιθέσεις
5. Στόχοι προστασίας
6. Προσεγγίσεις προστασίας σε εφαρμογές
7. Σύγκριση μεθόδων
8. Επίλογος
9. Βιβλιογραφία

Κεφάλαιο 1 : Πρόλογος

Η πτυχιακή εργασία αυτή είναι αφιερωμένη στον καθηγητή και επιβλέποντα μου κ. **Νταντογιάν Χριστόφορο**, ο οποίος με υπομονή και καθοδήγηση με βοήθησε στο τελευταίο μου αυτό κομμάτι των σπουδών. Μου κέντρισε αρχικά το ενδιαφέρον για τα μαθήματα αλλά και τις προσεγγίσεις του σε διάφορα θέματα, στον τομέα της Ασφάλειας όπου και ειδικεύεται, αλλά και όχι μόνο. Με βοήθησε με την επιλογή και την διεκπεραίωση της εργασίας και έκανε υπομονή στις διάφορες αναποδιές που μου συνέβησαν στην πορεία. Γι' αυτό, τον ευχαριστώ θερμά και ελπίζω ολόψυχα να πετυχαίνει τους στόχους του με τα λιγότερα δυνατά εμπόδια.

Ο θεσμός της πτυχιακής εργασίας είναι ένα ξεχωριστό κομμάτι στην καριέρα του κάθε φοιτητή. Εκπονείται με κόπο, μεράκι και μαθαίνει στον φοιτητή για την συνεργασία, την έρευνα και την αναζήτηση σε επαγγελματικό πλέον επίπεδο. Αυτός είναι και ο λόγος όμως που η πτυχιακές εργασίες αποτελούν καθοριστικό παράγοντα για την μελλοντική επαγγελματική αποκατάσταση του φοιτητή. Στα πλαίσια της εκπόνησης της πτυχιακής, μαθαίνουμε για τεχνολογίες που χρησιμοποιούνται ανά τον κόσμο για την καινοτομία, την αυτοματοποίηση και την καλλιέργεια των διαφόρων κλάδων της πληροφορικής. Προσωπικά, τους τελευταίους μήνες, έμαθα πολλές νέες τεχνολογίες , τρόπους και προσεγγίσεις με τις οποίες, καθηγητές και ερευνητές απ' όλο τον κόσμο δίνουν λύση στα καθημερινά μας, άλυτα προβλήματα. Στο θέμα μου, **“Ανάλυση Κρυπτογραφίας και Θεμάτων Ιδιωτικότητας σε Εφαρμογές Έξυπνου Πάρκινγκ”**, ήρθα αντιμέτωπος με πολλές νέες τεχνολογίες με τις οποίες προσπαθούμε να βοηθήσουμε έναν άνθρωπο όπως εμείς, να γλυτώσει χρόνο και πιθανώς και χρήμα, για μια καθημερινή και κοινή προς όλους ανάγκη, το πάρκινγκ. Επιπρόσθετα, η διαδικασία αυτή γίνεται με ασφάλεια , αφού τα στοιχεία του κρυπτογραφούνται για την διασφάλιση αρετών όπως η ιδιωτικότητα και η ανωνυμότητα του. Σε τελικές γραμμές, ο κόσμος της πληροφορικής μπορεί να χαρακτηριστεί ως ένα σύμπαν από μόνο του, αφού μονίμως επεκτείνεται, με την πληθώρα των πλανητών - κλάδων του, που κάθε μέρα πολλαπλασιάζονται, επιβεβαιώνοντας την ανθρώπινη manía για εξέλιξη και συνεχής πρόοδο.

Κεφάλαιο 2 : Εισαγωγή

Η πτυχιακή εργασία αυτή αποτελεί μια **βιβλιογραφική εργασία**. Αυτό σημαίνει πως η εργασία αποτελεί οδηγό για κάποιον που επιθυμεί να αποκτήσει μια σφαιρική ματιά σε διάφορες προσεγγίσεις ανθρώπων, οι οποίοι προσπάθησαν να δώσουν λύση σε ένα συγκεκριμένο πρόβλημα, ή άλλα πανομοιότυπα προβλήματα.

Στον ανθρώπινο κόσμο, μείζον πρόβλημα αποτελεί στις μέρες μας το πρόβλημα του πάρκινγκ. Από πόλη σε πόλη, αλλά ειδικότερα στις μεγαλουπόλεις τόσο στην Ελλάδα όσο και παγκοσμίως, ο κόσμος βρίσκεται καθημερινά αντιμέτωπος με το πρόβλημα του πάρκινγκ. Για να εκπληρώσει καθημερινές ανάγκες, να μεταβεί από το σπίτι του στην δουλειά του και το αντίστροφο, για να μεταβεί στο σούπερ-μάρκετ ή οπουδήποτε θα χρειαστεί να παρκάρει το όχημά του, έρχεται στην κατάσταση όπου θα πρέπει να αναζητήσει μια ελεύθερη θέση, όσο κοντινότερα γίνεται στον προορισμό του. Η αδυναμία εύρεσης θέσεως πάρκινγκ μπορεί να αποβεί δαπανηρή στον οδηγό, τόσο σε χρόνο όσο και σε καύσιμο, δηλαδή χρήμα. Για του λόγου το αληθές, στην Ελλάδα και ειδικότερα σε μεγαλουπόλεις όπως η Αθήνα και η Θεσσαλονίκη, ο κόσμος έρχεται αντιμέτωπος καθημερινά με αυτό το χρόνιο πρόβλημα, ειδικότερα στην σημερινή εποχή όπου επικρατεί πληθώρα οχημάτων με μέσο όρο κατοχής για την Ελλάδα **606** οχήματα ανά **1000** άτομα.

Ερευνητές σε όλον τον κόσμο και κυρίως στην **Κίνα**, στην οποία το πρόβλημα αυτό είναι πιο αισθητό σε σύγκριση με την Ελλάδα, προσπάθησαν να δώσουν λύσεις. Σε κάποιες από τις λύσεις που θα δούμε στα επόμενα κεφάλαια, απαιτείται ο εκσυγχρονισμός της πόλης ενώ σε άλλες το μόνο που έχει να κάνει ο πολίτης είναι να κατεβάσει μια εφαρμογή στο κινητό του, η οποία θα τον βοηθήσει να βρει μια θέση πάρκινγκ, άλλοτε με μίσθωση και άλλοτε χωρίς.

Οι εφαρμογές αυτές, όμως, αν και λειτουργικές σε μια έξυπνη ή και σε μια συνηθισμένη πόλη, μπορεί να φέρουν κάποια θέματα όσον αφορά την παραβίαση στοιχείων ασφαλείας του χρήστη όπως η ιδιωτικότητα, η ανωνυμότητα των στοιχείων του αλλά και η εμπιστευτικότητα τους από την εταιρία που ορίζεται υπεύθυνη για την εφαρμογή εύρεσης πάρκινγκ, ή και άλλες τρίτες εφαρμογές που ορίζουν την διαδικασία πληρωμής.

Στην πτυχιακή αυτή, θα δούμε αναλυτικά **την αρχιτεκτονική τέτοιων εφαρμογών**, τα **προβλήματα** και τις πιθανές **επιθέσεις** που μπορεί να δεχτεί ένας χρήστης κατά τη χρήση τέτοιων εφαρμογών, τους **στόχους προστασίας** που θα πρέπει να εστιάζουν οι εφαρμογές και οι δημιουργοί τους. Επίσης θα δούμε **αναλυτικές προσεγγίσεις** από ερευνητές και επιστήμονες στην προσπάθειά τους να δώσουν λύση στα θεμελιώδη προβλήματα όπως αυτά που ειπώθηκε

ότι θα αναλυθούν. Τέλος, θα κάνουμε μια **σύγκριση** των μεθόδων που θα δούμε ότι θα χρησιμοποιηθούν. Η σύγκριση θα είναι από άποψη **ασφαλείας** αλλά θα αφορά το τεχνικό κομμάτι, το κομμάτι δηλαδή της **κρυπτογραφίας**, αφού, όπως θα δούμε, οι μέθοδοι που θα συναντήσουμε μπορεί να χρησιμοποιούν κάποια **fog nodes**, τα οποία μπορούν να παρομοιωθούν με μικρούς υπολογιστές, με σύνδεση στο διαδίκτυο, με περιορισμένα τεχνικά χαρακτηριστικά (μνήμη, ταχύτητα κ.λπ.) τα οποία συνδέονται πιθανώς σε κάποιον σέρβερ με σκοπό την ενημέρωση για την διαθεσιμότητα ή μη θέσεων στάθμευσης.

Κεφάλαιο 3 : Αρχιτεκτονικές Έξυπνων Πάρκινγκ

Μετά από αναζήτηση στο διαδίκτυο και ανάλυση ερευνών δημοσιευμένες σε ιστοσελίδες επιστημονικού περιεχομένου (φερ' ευτείν IEEE), παρατήρησα πως οι περισσότερες προσεγγίσεις ακολουθούσαν κάποια συγκεκριμένη αρχιτεκτονική. Η αρχιτεκτονική αυτή μπορεί να αναλυθεί σε ένα γενικευμένο επίπεδο, πράγμα που θα δούμε σε αυτό το κεφάλαιο. Επίσης, είναι σημαντικό να σημειώσουμε πως, αν και πολλές από τις μελέτες που θα δούμε στο 6ο κεφάλαιο ακολουθούν την αρχιτεκτονική που θα αναλύσουμε, πολλοί ερευνητές έδωσαν μια εντελώς διαφορετική προσέγγιση στο θέμα. Αυτό μας προϋδεάζει για τις ραγδαίες τεχνολογικές καινοτομίες που επαιτώ να έρθουν στο σύντομο μέλλον, στην καθημερινή μας ζωή. Το Internet of Things είναι πλέον γεγονός πως θα το συναντάμε παντού, καθώς θα αυτοματοποιήσει πολλές από τις καθημερινές δυσκολίες που οι άνθρωποι των σημερινών fast-paced ρυθμών ζωής καλούνται να αντιμετωπίσουν.

Στο γενικευμένο αρχιτεκτονικό μοντέλο, συναντούμε τις εξής τεχνολογίες. Αρχικά, τα μοντέλα αυτά θα λαμβάνουν χώρα στις λεγόμενες **έξυπνες πόλεις (smart cities)**. Ως έξυπνη πόλη χαρακτηρίζεται μια πόλη όπου την διακατέχουν αρχές και τεχνολογίες Internet of Things. Μια έξυπνη πόλη, στο σενάριο που σχεδιάζουμε θα πρέπει να διαθέτει τις εξής τεχνολογίες :

- **Fog nodes ή Road-side Units(RSUs)**, δηλαδή μικρές συσκευές με περιορισμένα τεχνικά χαρακτηριστικά και σύνδεση (ή και μη) στο διαδίκτυο. Οι συσκευές αυτές θα επικοινωνούν με έναν **Cloud Server** και θα συνδέονται με **On-Board Units (OBUs)** . Στις **Εφαρμογές Έξυπνων Πάρκινγκ**, τα **RSUs** λαμβάνουν συνεχώς στην μνήμη τους την διαθεσιμότητα ορισμένων θέσεων στάθμευσης, τόσες όσες αναλογούν στο καθένα.
- **Cloud Server**, ένας σέρβερ ο οποίος θα είναι ζωντανός συνεχώς και θα διαχειρίζεται τις πληροφορίες που θα λαμβάνει από τα **RSUs**. Ο σέρβερ θα επεξεργάζεται τα δεδομένα και θα στέλνει στον χρήστη πληροφορίες σχετικά με την διαθεσιμότητα θέσεων στάθμευσης, μέσω μιας εφαρμογής που είτε ο χρήστης θα διαθέτει στο έξυπνο τηλέφωνο του, ή θα διατίθεται κατευθείαν στο έξυπνο όχημά του.
- **On-board Units(OBUs)**, τα οποία συντελούν μικρο-συσκευές τις οποίες ο χρήστης τοποθετεί στο αυτοκίνητό του. Οι συσκευές αυτές μπορούν να έρχονται μαζί με το αυτοκίνητο εργοστασιακά. Σκοπός των συσκευών αυτών είναι να ενημερώνουν κοντινά **RSUs** για την ακριβή τοποθεσία του χρήστη που αναζητεί θέση στάθμευσης. Ομοίως, εάν ένα αυτοκίνητο είναι παρκαρισμένο, το **OBU** θα εκπέμπει το δικό του μοναδικό ID στο κοντινότερο **RSU** το οποίο με τη σειρά του θα ενημερώνει τον **Cloud Server** και κατ' επέκτασιν τον χρήστη για τις κατειλημμένες θέσεις στάθμευσης.

- **Smart phone application**, εφαρμογή που θα παρέχει ο πάροχος της υπηρεσίας. Ο χρήστης θα καταχωρεί το ID του OBU του και θα συνδέεται στο σύστημα.

Τα παραπάνω εργαλεία θα βοηθήσουν στο να γίνει η προσπάθεια των Έξυπνων Πάρκινγκ ευφικτή. Όμως, είναι εξίσου σημαντικό να αναφέρουμε κάποιους παράγοντες στον τομέα της Ασφαλείας, που έχουν βασιστεί κάποιες από τις μελέτες της εργασίας. Εξάλλου, η παραπάνω αρχιτεκτονική δεν θα μπορούσε να γίνει εφικτή χωρίς ένα ισχυρό σχέδιο ασφαλείας το οποίο θα προστατεύει αξίες όπως η ανωνυμότητα του χρήστη, η ιδιωτικότητά του, η ακεραιότητα των στοιχείων του. Στο επόμενο κεφάλαιο που θα δούμε κάποιες από τις επιθέσεις που μπορούν να δεχτούν πανομοιότυπα χτισμένα συστήματα, είναι σημαντικό να θυμηθούμε πως, κατά την δημιουργία παρόμοιων εφαρμογών, θα πρέπει προτεραιότητά μας, εκτός από την ευχρηστία, να είναι και η προστασία των δεδομένων των χρηστών. Εάν παραβιαστεί η ασφάλεια και η ακεραιότητα, ας πούμε, του Cloud Server, τότε δεδομένα όπως οι αριθμοί κάρτας των χρηστών, η τοποθεσία του οχήματός ή του έξυπνου κινητού τηλεφώνου τους, τα προσωπικά τους στοιχεία και πολλά άλλα, μπορούν να βρεθούν διαθέσιμα στο διαδίκτυο και προσβάσιμα προς άλλους κακόβουλους χρήστες.

Όσον αφορά, τώρα, τα χαρακτηριστικά ασφαλείας, είναι σημαντικό να αναφέρουμε τα εξής :

- **Trusted Authority(TA)**, είναι μια οντότητα η οποία είναι υπεύθυνη για την δημιουργία ενός ασφαλές καναλιού επικοινωνίας ανάμεσα στις οντότητες που αναφέραμε παραπάνω. Είναι υπεύθυνη για:
 - την **έκδοση κλειδιών**, δημόσιων και ιδιωτικών,
 - την **δημιουργία ενός ασφαλές καναλιού επικοινωνίας**
 - την **υπογραφή** ορισμένων **πιστοποιητικών γνησιότητας (certificates)**
- **Embedded Cryptography**, δηλαδή την τροποποίηση αλγορίθμων κρυπτογράφησης έτσι ώστε να είναι συμβατοί με τα συστήματα περιορισμένων χαρακτηριστικών (π.χ. μνήμης και ταχύτητας), που αναφέραμε παραπάνω. Ενδεικτικά, πολλές μελέτες χρησιμοποιούν τεχνικές **Elliptic Curve Cryptography**, μέσα από τις οποίες τροποποιούν αλγόριθμους **ταχύτητας** συγκρίσιμης με τον γνωστό σε όλους αλγόριθμο **RSA** , με **μικρότερο μήκος κλειδιού** ,ώστε να είναι συμβατοί με τα περιορισμένα συστήματα που χρησιμοποιούνται. Πιο συγκεκριμένα, με **Elliptic Curve**, πετυχαίνουμε κρυπτογράφηση επιπέδου RSA, με μήκος κλειδιού **224bits**, ισοδύναμα ισχυρό με ένα αντίστοιχο κλειδί **2048bits**, για τον RSA.
- **ID**, είναι το κωδικοποιημένο όνομα των οντοτήτων. Για παράδειγμα, σε ένα πλήθος N από **OBUs**, θα υπάρχουν N διαφορετικά **ID_i (0<i≤N)** που θα κατονομάζουν το καθένα διαφορετικό OBU.
- **PK(Public Key)**, το δημόσιο κλειδί των οντοτήτων που χρησιμοποιούν ασύμμετρη κρυπτογράφηση.

- **SK(Secret Key)**, το ιδιωτικό κλειδί των οντοτήτων που χρησιμοποιούν ασύμμετρη κρυπτογράφηση.
- **CERT(Certificate)**, ένα πιστοποιητικό που εκδίδεται και υπογράφεται, από την Trusted Authority.

Κάπου εδώ είναι σημαντικό να σημειωθεί πως οι παραπάνω έννοιες θα εξηγηθούν στις ερευνητικές εργασίες στη συνέχεια. Όμως, η κάθε έρευνα μπορεί να τις χρησιμοποιεί με διαφορετικό τρόπο και για να εκφράσει ένα διαφορετικό αποτέλεσμα. Σκοπός του παρόντος κεφαλαίου είναι να αναφερθούν έννοιες που χρησιμοποιούνται **γενικευμένα** και που θα δώσουν στον αναγνώστη της πτυχιακής εργασίας μια εικόνα για την αρχιτεκτονική και τις έννοιες ασφαλείας που **συνήθως** χρησιμοποιούνται σε μια πανομοιότυπη έρευνα.

Αναλύοντας την αρχιτεκτονική και έχοντας αναφέρει βασικές και θεμελιώδης έννοιες που χρησιμοποιούνται για την ασφάλεια των εφαρμογών έξυπνου πάρκινγκ, είναι πλέον η στιγμή να αναφέρουμε τις **απειλές** που μπορεί να αντιμετωπίσει ένα σύστημα. Στον κόσμο του Internet of Things, οι ανάγκες του μέσου ανθρώπου θα μπορούν να καλυφτούν με έναν αυτοματοποιημένο, έξυπνο και κατά βάση εύκολο για τον ίδιο τρόπο. Δεν θα πρέπει όμως να ξεχνάμε πως, όσο υπάρχουν συσκευές που κατέχουν διαδικτυακή σύνδεση, τόσο θα υπάρχουν προσπάθειες για **υποκλοπές στοιχείων** και την **διέρρευση** τους, με κέρδος το χρήμα και όχι μόνο.

Κεφάλαιο 4 : Προβλήματα - Επιθέσεις

Από την αρχή του διαδικτύου, οι άνθρωποι σχετική με τα αντικείμενα της ασφάλειας και της ανάγνωσης και κατανόησης κώδικα, προσπαθούσαν να ανακαλύψουν πιθανές ευπάθειες στα συστήματα. Οι ευπάθειες αυτές μπορούσαν να είναι στον **κώδικα**, από χαμηλό ή και υψηλό επίπεδο, αλλά και στον **χρήστη** με επιθέσεις τύπου **phishing**. Στις μέρες μας, οι ευπάθειες αυτές χρησιμοποιούνται για να καλύψουν τα κενά ασφαλείας ενός συστήματος ή μιας εφαρμογής, με μεθόδους **Penetration Testing** και **Ethical Hacking**. Παρ' όλ' αυτά, υπάρχουν άνθρωποι ή ομάδες ανθρώπων που δεν δημοσιεύουν τις ευπάθειες σε συστήματα που οι ίδιοι ανακαλύπτουν και επιλέγουν να προβούν σε διάρρηξη των πληροφοριών στο διαδίκτυο με κακόβουλο τρόπο.

Στις εφαρμογές Έξυπνων Πάρκινγκ, το περιεχόμενο που μπορεί να διαρρεύσει στο διαδίκτυο μπορεί να είναι προσωπικά δεδομένα του χρήστη, όπως :

- Το ονοματεπώνυμό του,
- Ο αριθμός του τηλεφώνου του,
- Τα στοιχεία της κάρτας τραπεζής του,
- Η τοποθεσία του,
- Η τοποθεσία του έξυπνου τηλεφώνου του,
- Η τοποθεσία του αυτοκινήτου του

και η λίστα συνεχίζεται στο βάθος που φτάνει η φαντασία του θήτη, ή **χάκερ**.

Κατανοούμε πλέον πως είναι σημαντικό να αναφέρουμε μερικές από τις επιθέσεις που μπορεί να δεχτεί ο χρήστης, από άποψη ασφαλείας. Οι επιθέσεις αυτές αναφέρονται ενδεικτικά στις έρευνες που θα δούμε στο 6ο κεφάλαιο. Σκοπός του παρόντος κεφαλαίου είναι η ανάλυσή τους ώστε να αποκτήσει ο αναγνώστης της πτυχιακής μια καλύτερη εικόνα για το πως λειτουργούν.

4.1 Man-in-the-Middle Attack

Στην κρυπτογραφία και την ασφάλεια των υπολογιστών, μια επίθεση man-in-the-middle είναι μια κυβερνοεπίθεση όπου ο επιτιθέμενος εισέχεται κρυφά και πιθανώς αλλάζει τις επικοινωνίες μεταξύ δύο κόμβων που επικοινωνούν μεταξύ τους. Ένα παράδειγμα επίθεσης MITM είναι η ενεργή υποκλοπή, στην οποία ο επιτιθέμενος κάνει ανεξάρτητες συνδέσεις με τα θύματα και μεταδίδει μηνύματα μεταξύ τους για να τους κάνει να πιστέψουν ότι μιλούν απευθείας μεταξύ τους, μέσω μιας ιδιωτικής σύνδεσης. Στην πραγματικότητα ολόκληρη η συνομιλία ελέγχεται από τον εισβολέα. Ο επιτιθέμενος είναι σε θέση να υποκλέψει όλα τα σχετικά μηνύματα που ανταλλάσσονται μεταξύ των δύο θυμάτων και να εισάγει νέα στην θέση τους.

4.2 Secret Disclosure Attack

Στην επίθεση αυτή, ο επιτιθέμενος προσπαθεί να εισβάλλει σε ένα δίκτυο. Εάν η εισβολή πετύχει, σκοπός του είναι να υποκλέψει προσωπικές πληροφορίες που αφορούν φυσικά πρόσωπα, εταιρίες κ.α.. Στη συνέχεια διαρρέει τα δεδομένα αυτά ανώνυμα στον κυβερνοχώρο. Ως χαρακτηριστικό παράδειγμα αξίζει να σημειωθεί το **data leakage** της εταιρίας **Meta (πρώην Facebook)** η οποία τον Απρίλιο του 2019 δέχτηκε μια παρόμοια επίθεση με αποτέλεσμα τα στοιχεία 533 εκατομμυρίων λογαριασμών να διαρρεύσουν σε ένα hacker forum.

4.3 Impersonation Attack

Στην επίθεση αυτή, μια κακόβουλη οντότητα που θα καταφέρει να εισβάλει σε ένα κανάλι επικοινωνίας δυο κόμβων, θα χρησιμοποιήσει μια τεχνική με σκοπό να μιμηθεί την οντότητα-αποστολέας. Για παράδειγμα, στην διαδικτυακή σύνδεση, ο client που θα επικοινωνεί με τον server κάποιας ιστοσελίδας, μπορεί να στείλει ένα πακέτο κακόβουλο, κάνοντας τον server να πειστεί πως ο client είναι ασφαλής και να το εκτελέσει. Τότε το κακόβουλο λογισμικό θα εκτελεστεί στο σύστημα του server, διαδικασία που μπορεί να καταλήξει σε παραβίαση της ασφάλειας του συστήματος του server, ακόμη και την πλήρη κατοχή του (root access) από την κακόβουλη οντότητα. Η διαδικασία αυτή ονομάζεται και **reverse shell attack** και μπορεί να συνδυαστεί με την εν λόγω επίθεση.

4.4 Background Knowledge Attack

Στην επίθεση αυτή, η κακόβουλη οντότητα πραγματοποιεί μια άλλη επίθεση “συστημένα”. Αυτό συμβαίνει επειδή μπορεί να γνωρίζει ήδη κάποια πληροφορία για τον στόχο της επίθεσης. Για παράδειγμα, εάν ο master server μιας εφαρμογής έξυπνου πάρκινγκ λειτουργεί σε Linux λειτουργικό σύστημα και η κακόβουλη οντότητα το μάθει, θα δημιουργήσει μια επίθεση στοχευμένη να δουλέψει σε linux συστήματα.

4.5 Sniffing Attack

Η επίθεση sniffing attack αντιστοιχεί σε κλοπή ή υποκλοπή δεδομένων με τη λήψη της κίνησης του δικτύου χρησιμοποιώντας ένα packet sniffer (μια εφαρμογή που στοχεύει στη λήψη πακέτων δικτύου). Όταν τα δεδομένα μεταδίδονται μέσω των δικτύων, εάν δεν είναι κρυπτογραφημένα, μπορούν να διαβαστούν χρησιμοποιώντας ένα sniffer. Χρησιμοποιώντας μια εφαρμογή sniffer, ένας εισβολέας μπορεί να αναλύσει το δίκτυο και να αποκτήσει πληροφορίες για να προκαλέσει τελικά τη διακοπή λειτουργίας ή την καταστροφή του δικτύου ή και να διαβάσει τις επικοινωνίες που συμβαίνουν σε όλο το δίκτυο.

4.6 Double Reservation Attack

Όπως θα δούμε παρακάτω, οι εφαρμογές έξυπνου πάρκινγκ μπορεί να προσβληθούν από την double reservation attack. Η επίθεση αυτή δεν απαιτεί στην πλειοψηφία των περιπτώσεων κάποια κακόβουλη ενέργεια ως προς τον πυρήνα του συστήματος του έξυπνου πάρκινγκ, ή και του κώδικα που χρησιμοποιείται. Αξιοποιώντας κάποια εμφανή ευπάθεια στο σύστημα, ένας χρήστης μπορεί να δεσμεύσει πολλές θέσεις πάρκινγκ, για μια συγκεκριμένη οντότητα, για ένα μοναδικό δηλαδή φυσικό πρόσωπο. Η επίθεση αυτή, εμφανέστερα στο κεφάλαιο 6, μπορεί να αποτραπεί με την χρήση μοναδικών διευθύνσεων σε blockchain βασισμένα συστήματα. Οι διευθύνσεις αυτές αντιστοιχούν προς μια συγκεκριμένη οντότητα και χρησιμοποιούνται για την ανταλλαγή πληροφοριών όπως τα parking queries, ή και χρήματος για την πληρωμή κάποιας μισθωμένης θέσης.

4.7 Phishing Attack

Το ηλεκτρονικό ψάρεμα (phishing) είναι ένας τύπος επίθεσης όπου ένας εισβολέας στέλνει ένα δόλωμα (π.χ. πλαστογραφημένο, ψεύτικο μήνυμα ή άλλως παραπλανητικό μήνυμα) που έχει σχεδιαστεί για να εξαπατήσει ένα άτομο να αποκαλύψει ευαίσθητες πληροφορίες στον εισβολέα ή να αναπτύξει κακόβουλο λογισμικό στην υποδομή του θύματος. Οι επιθέσεις ηλεκτρονικού ψαρέματος έχουν γίνει όλο και πιο εξελιγμένες. Συχνά παρατηρείται η δημιουργία πανομοιότυπων σελίδων στο διαδίκτυο όπως το Facebook, οι οποίες επιτρέπουν στον εισβολέα να παρατηρεί τις ενέργειες του θύματος ενώ το θύμα πλοηγείται στον ιστότοπο. Από το 2020, το ηλεκτρονικό ψάρεμα είναι μακράν η πιο κοινή επίθεση που εκτελείται από εγκληματίες στον κυβερνοχώρο, στην οποία επίθεση το Κέντρο Καταγγελιών Διαδικτυακού Εγκλήματος του FBI καταγράφει πάνω από διπλάσιο αριθμό περιστατικών ηλεκτρονικού ψαρέματος από οποιοδήποτε άλλο είδος εγκλήματος στον υπολογιστή.

4.8 Replay Attack

Μια επίθεση τύπου replay attack είναι μια μορφή επίθεσης δικτύου στην οποία η έγκυρη μετάδοση δεδομένων επαναλαμβάνεται κακόβουλα ή με δόλιο τρόπο ή καθυστερεί. Αυτό πραγματοποιείται είτε από τον δημιουργό είτε από μια κακόβουλη οντότητα που υποκλέπτει τα δεδομένα και τα μεταδίδει εκ νέου. Αυτή είναι μια από τις εκδόσεις χαμηλότερης βαθμίδας μιας επίθεσης man-in-the-middle. Οι επιθέσεις replay attack είναι συνήθως παθητικής φύσης.

Κεφάλαιο 5 : Στόχοι προστασίας

Στο κεφάλαιο αυτό θα δούμε κάποιους από τους στόχους που καλούνται να επιτύχουν οι ερευνητές στο πρόβλημα προστασίας των εφαρμογών τους αλλά και των ξεχωριστών προσεγγίσεων τους στο θέμα μας. Κατά την δημιουργία εφαρμογών γενικότερα αλλά και ειδικότερα εφαρμογών που λειτουργούν με τη χρήση ορισμένων προσωπικών στοιχείων του χρήστη, η ασφάλεια θα πρέπει να είναι ικανοποιητική και ισχυρή. Τα δεδομένα θα πρέπει να κρυπτογραφούνται και να διαμοιράζονται ανάμεσα στους πόλους του πληροφοριακού συστήματος της εφαρμογής, από ασφαλή κανάλια επικοινωνίας. Εάν οι προϋποθέσεις αυτές είναι εκπληρωμένες, τότε μπορούμε να αναφέρουμε τους στόχους που θα πετύχουν σε κάθε περίπτωση, στην προσπάθεια τους να προστατέψουν τελείως τον χρήστη από οποιαδήποτε κακόβουλη προσβολή ή επίθεση μπορεί να δεχτεί στα προσωπικά του δεδομένα.

1. Κατά την διασφάλιση της **ιδιωτικότητας**, αναφερόμαστε σε τεχνικές που αποσκοπούν σε έναν στόχο και χρησιμοποιούν τα προσωπικά δεδομένα του χρήστη για την αυθεντικοποίηση του. Όμως η χρήση αυτή θα πρέπει να γίνει με απόλυτη ασφάλεια και μυστικότητα και να βεβαιωθεί με απόλυτη σιγουριά πως τα προσωπικά δεδομένα του χρήστη θα μείνουν απόρρητα για περαιτέρω χρήση. Οι εφαρμογές που χρησιμοποιούν τα προσωπικά στοιχεία των χρηστών τους θα πρέπει να δημιουργούν ένα ολοκληρωμένο μοντέλο ασφαλείας που θα βασίζεται προπαντός στην διασφάλιση της ιδιωτικότητας τους.
2. Κατά την διατήρηση της **ανωνυμότητας**, οι εφαρμογές που θα παρέχουν υπηρεσίες προς τους χρήστες, θα πρέπει να στοχεύουν στην δημιουργία ενός μοντέλου που δεν θα χρησιμοποιεί τα προσωπικά στοιχεία των χρηστών του. Επίσης, θα πρέπει να προστατέψουν τον χρήστη από επιθέσεις που θα εισβάλλουν στον προσωπικό του χώρο, όπως οι συσκευές του. Από εκεί, κακόβουλοι χρήστες που θα έχουν ανακαλύψει μια ευπάθεια στην υπηρεσία, θα μπορέσουν να υποκλέψουν τις προσωπικές πληροφορίες του χρήστη.
3. Κατά την **ακεραιότητα** των δεδομένων του χρήστη, θα πρέπει διασφαλίζεται το ακέραιο των στοιχείων του κατά την χρήση της εφαρμογής. Σε πολλές εφαρμογές και ειδικότερα έξυπνου πάρκινγκ, είναι πιθανόν κάποιος κακόβουλος χρήστης να αποκτήσει πρόσβαση στα προσωπικά δεδομένα του χρήστη με απώτερο σκοπό να τα αλλοιώσει. Θα πρέπει λοιπόν οι εφαρμογές να δημιουργούν μοντέλα ασφαλείας σεβόμενα της ακεραιότητας των δεδομένων των χρηστών τους.

4. Τέλος, εξίσου σημαντική είναι η διασφάλιση της **εμπιστευτικότητας** από πλευράς των δημιουργών της εφαρμογής. Θα πρέπει να παρέχουν μοντέλα λειτουργικά προς το κοινό που όμως δεν θα προδίδουν την εμπιστοσύνη των χρηστών. Σε πολλές εφαρμογές αλλά και συγκεκριμένα σε εφαρμογές έξυπνου πάρκινγκ, η χρήση των κρυπτογραφημένων προσωπικών δεδομένων των χρηστών ήταν απαραίτητη για την εξαγωγή αποτελεσμάτων διαφόρων ερευνών. Η κάθε εταιρία επομένως θα πρέπει να διατηρεί υπεύθυνα την ευθύνη των δυνάμεων της και να προστατεύει τα δεδομένα που φιλοξενεί, προασπίζοντας την εμπιστευτικότητα των χρηστών της.

Κεφάλαιο 6 : Προσεγγίσεις προστασίας σε εφαρμογές

Μέχρι στιγμής αναφερθήκαμε στις πιθανές επιθέσεις αλλά και στους στόχους που μπορούμε να πετύχουμε εάν ασφαλίσουμε σωστά και σφαιρικά τις εφαρμογές μας. Αναφέραμε επίσης γενικά, την αρχιτεκτονική μιας εφαρμογής έξυπνου πάρκινγκ. Τα δεδομένα που χρησιμοποιήσαμε για να συντάξουμε τα παραπάνω κεφάλαια, όμως, αποτελούν ένα γενικευμένο σύνολο των μελετών και ερευνών που θα παρουσιάσουμε εκτενέστερα στο κεφάλαιο αυτό. Θα δούμε **29** διαφορετικές προσεγγίσεις από ερευνητές ανά τον κόσμο, πράγμα που θα βοηθήσει τον αναγνώστη της πτυχιακής να κατανοήσει σε έκταση το θέμα που εξετάζουμε αλλά και να πάρει μια σφαιρική εικόνα για την λειτουργικότητα αυτών των εφαρμογών, τις προϋποθέσεις λειτουργίας τους και, τέλος, τον τρόπο για να πετύχει ένα ασφαλές και ικανοποιητικό, προς τον χρήστη αλλά και τον ίδιο, αποτέλεσμα. Τέλος, θα προσεγγίσουμε τις μεθόδους **κρυπτογράφησης** που χρησιμοποίησαν οι ερευνητές στις μελέτες τους και θα δούμε μια σύγκριση τους στο επόμενο κεφάλαιο. Αυτό δεν θα γίνει για όλες τις έρευνες, παρά μόνο για αυτές που το αναφέρουν.

6.1 *Web-based framework for Smart Parking Applications* [1]

Η περιγραφόμενη διαδικασία της εργασίας αυτής, λαμβάνει χώρα μέσα σε δικές της εγκαταστάσεις, τα "Έξυπνα Πάρκινγκ" ή "Smart Carparks". Ο πελάτης, μέσω μιας εφαρμογής, κλειδώνει μια θέση στάθμευσης, τον χρόνο που υπολογίζει πως θα την χρειαστεί και τον χρόνο που υπολογίζει πως θα φτάσει στον χώρο του πάρκινγκ. Όταν φτάσει, μια κάμερα ανιχνεύει την πινακίδα του αυτοκινήτου για να επιβεβαιώσει την κράτηση. Ο πελάτης κατευθύνεται στο σημείο στάθμευσης. Αν επιθυμήσει να παρατείνει τον χρόνο στάθμευσης, πρέπει να πληρώσει ένα επιπλέον ποσό, προτού να εξέλθει από τον χώρο του πάρκινγκ. Όταν τελικά ο οδηγός εξέλθει του πάρκινγκ, η πινακίδα του αυτοκινήτου ανιχνεύεται ξανά για να αποδεσμεύσει τον χώρο στάθμευσης. Η διαδικασία ανίχνευσης της πινακίδας των οχημάτων, γίνεται με τη χρήση του OCR αλγόριθμου, τον οποίο οι ερευνητές τροποποίησαν, ώστε να μπορεί να χρησιμοποιηθεί σε .NET Framework μορφή.

6.2 A Secure and Privacy Preserved Parking Recommender System Using Elliptic Curve Cryptography and Local Differential Privacy [2]

Η έρευνα αυτή, παρουσιάζει μια πολλαπλών παραγόντων προσέγγιση που ενισχύει εφαρμογές Έξυπνου Πάρκινγκ και προστατεύει την ανωνυμότητα και την αυθεντικότητα των χρηστών της. Προστατεύει επίσης τα προσωπικά τους δεδομένα αλλά και την τρέχουσα τοποθεσία τους, σε περιπτώσεις υποβοήθησης των εφαρμογών από "τρίτες" εφαρμογές και άλλους εξωτερικούς παράγοντες. Αρχικά, ο χρήστης ζητά από μια Υπηρεσία Διαμοιρασμού και Έκδοσης Κλειδιών, για ένα ψεύτικο αναγνωριστικό. (Fake ID, FID). Η υπηρεσία το δημιουργεί χρησιμοποιώντας τον αλγόριθμο της ελλειπτικής καμπύλης (elliptic curve). Η αυθεντικοποίηση του χρήστη με την εφαρμογή εύρεσης Έξυπνου Πάρκινγκ, γίνεται με το ψεύτικο αναγνωριστικό του χρήστη, ώστε να διατηρηθεί η ανωνυμότητα του και η απόκρυψη των προσωπικών του στοιχείων. Στη συνέχεια, η τεχνική της Τοπικής Διαφορικότητας (Local Differential Privacy) , δια μέσω της κατανομής Laplace, χρησιμοποιείται για να δώσει "θόρυβο" στα δεδομένα του χρήστη, να τα αλλοιώσει δηλαδή, τοπικά. Τα αλλοιωμένα δεδομένα, στέλνονται στη συνέχεια στην "τρίτη" υπηρεσία, με τη χρήση μιας τελευταίας προσθήκης στην άμυνα του συστήματος, την υπηρεσία IOTA, ενός πρωτοκόλλου μεταφοράς που ξεφεύγει από τους περιορισμούς της τεχνολογίας blockchain, αποκεντροποιώντας τις συναλλαγές. Μετά από την ολοκλήρωση αυτής της διαδικασίας, ο χρήστης μπορεί να επικοινωνήσει με εφαρμογές εύρεσης Έξυπνου Πάρκινγκ, με ασφάλεια. Το μοντέλο προστατεύει από επίθεση Man in the Middle, επίθεση Secret Disclosure, επίθεση απομίμησης (Impersonation Attack) και επίθεση Background Knowledge. Εν κατακλείδι, η μέθοδος αυτή χρησιμοποιεί τον αλγόριθμο ελλειπτικής καμπύλης, επειδή είναι γρήγορος και χρησιμοποιεί μικρότερο μήκος κλειδιού από άλλους αλγορίθμους. Η Τοπική Διαφορικότητα επιτρέπει την πρόσβαση σε ακατέργαστα (raw) δεδομένα με ασφαλή τρόπο. Η υπηρεσία IOTA αποκεντρικοποιεί το σύστημα και το καθιστά πιο ασφαλές στο πεδίο των συναλλαγών.

6.3 A navigation and reservation based smart parking platform using genetic optimization for smart cities [3]

Η έρευνα αυτή παρουσιάζει ένα πλάνο υλοποιήσιμο σε ένα περιβάλλον “έξυπνης πόλης”. Προϋποθέτει πως ο οδηγός θα διαθέτει σύνδεση στο διαδίκτυο αλλά και μια εφαρμογή στο έξυπνο τηλέφωνό του. Κάτω από κάθε σημείο στάθμευσης θα υπάρχει μια συσκευή η οποία θα είναι εξίσου συνδεδεμένη στο διαδίκτυο. Με τη χρήση ενός μαγνήτη, η συσκευή θα είναι ικανή να ανιχνεύσει την παρουσία ή μη, οχήματος στον χώρο του πάρκινγκ. Η συσκευή, με τη χρήση του πρωτοκόλλου IEEE 802.15.4, θα μεταδίδει την πληροφορία σε έναν **cloud server**, ο οποίος στη συνέχεια θα ενημερώνει τον οδηγό για το πλήθος των ελεύθερων θέσεων στάθμευσης, κοντά του. Η πληροφορία θα μεταβιβάζεται από τον **cloud server**, στο έξυπνο τηλέφωνο του χρήστη, με τη χρήση του GPRS (Point to Point Protocol). Στη συνέχεια, ένας γενετικός αλγόριθμος που θα βασίζεται στις αρχές της φυσικής επιλογής, θα παρέχει τον κοντινότερο δρόμο για τον χρήστη, προς τις θέσης στάθμευσης που είναι πιο κοντά στον χώρο που επιθυμεί να μεταβεί, με βάση την στιγμιαία τοποθεσία του. Η έρευνα δεν διαθέτει επιπλέον πληροφορίες για τον τρόπο ή την κρυπτογράφηση που μπορεί να χρησιμοποιείται, πράγμα που μας αναγκάζει να βασιστούμε στην ασφάλεια και την αξιοπιστία των πρωτοκόλλων που γνωρίζουμε ότι χρησιμοποιούνται.

6.4 An Intelligent Secure and Privacy-Preserving Parking Scheme Using Vehicular Communications [4]

Η παρούσα μελέτη προτείνει μια μέθοδο στάθμευσης, η οποία θα κατευθύνει τους οδηγούς σε διαθέσιμες θέσεις στάθμευσης σε πραγματικό χρόνο. Βοηθάει στην αντιμετώπιση της κλοπής της θέσης στάθμευσης από κάποιον άλλο οδηγό, αλλά και σε μια ταχεία διαδικασία στάθμευσης με τη χρήση ad hoc vehicular networks. Τα οχήματα πρέπει να είναι εξοπλισμένα με μια ενσωματωμένη μονάδα (**OBU**), η οποία θα είναι πιστοποιημένη από ένα **Trusted Authority** και θα της αποδίδεται ένα μοναδικό **IDi** και ένα **ψεύδο-IDi (PIDi)**. Μια άλλη συσκευή που ονομάζεται Roadside Unit (**RSU**), “σαρώνει” την περιοχή για **OBUs**. Το **PIDi** διασφαλίζει την ανωνυμότητα και την αποκάλυψη πληροφοριών όπως το μέγεθος ή το κόστος κάθε εξοπλισμένου οχήματος. Το **TA** είναι αξιόπιστο, επειδή αποτελείται από ένα κύριο κλειδί, το οποίο, με τη χρήση της τεχνικής Bilinear Pairing, χρησιμοποιείται για την ανάθεση και διανομή κλειδιών σε κάθε εγγεγραμμένη **OSU** και **RSU**. Όταν ένα αυτοκίνητο σταθμεύει, δημιουργείται ένα ζεύγος εισιτηρίων και ένα μοναδικό κλειδί για το εισιτήριο της θέσης στάθμευσης,

χρησιμοποιώντας το PIDi του OSU του αυτοκινήτου, το μοναδικό κλειδί RSUi και την τρέχουσα χρονοσφραγίδα. Αυτό συμβάλλει στη βελτίωση της κλοπής αυτοκινήτων αλλά και στην προστασία των προσωπικών δεδομένων του οδηγού.

6.5 A privacy-preserving smart parking system using an IoT elliptic curve based security platform [5]

Σκοπός της παρούσας μελέτης είναι η εφεύρεση ενός καινοτόμου τρόπου ασφαλείας, εφαρμοσμένο σε μικροτσίπ, λειτουργικά συστήματα των έξυπνων τηλεφώνων και άλλα συστήματα με περιορισμένα τεχνικά χαρακτηριστικά, όπως μνήμη και ταχύτητα. Η μελέτη αναφέρεται σε συσκευές όπως το Arduino, που χρησιμοποιούν Contiki OS, iSense OS, Tiny OS κ.λπ. Οι ερευνητές επέλεξαν να εφαρμόσουν την τεχνική κρυπτογραφίας της **ελλειπτικής καμπύλης (Elliptic Curve Cryptography)**. Υλοποίησαν αυτή την ιδέα με τη χρήση της C++, χρησιμοποιώντας την **Standard Template Library** και τη **Computational Geometry Algorithms Library**. Αρχικά, ένας **Issuer** δημιουργεί ένα μοναδικό ιδιωτικό κλειδί, το οποίο θα χρησιμοποιηθεί από την εφαρμογή έξυπνου πάρκινγκ, στο έξυπνο τηλέφωνο του χρήστη. Στη συνέχεια, ο **Issuer** πιστοποιεί τον χρήστη χρησιμοποιώντας έναν εξωτερικό μηχανισμό, online ή offline, δημιουργώντας έτσι τα ψευδο-στοιχεία του (Pseudo IDi). Στη συνέχεια, ο χρήστης τα χρησιμοποιεί, υπογεγραμμένα από μια **Trusted Authority** και το ιδιωτικό κλειδί που ο **Issuer** έχει εκχωρήσει στην εφαρμογή, ολοκληρώνοντας την διαδικασία της ταυτοπροσωπίας. Προκειμένου ο κώδικας να μπορεί να επαναχρησιμοποιηθεί. Προκειμένου ο κώδικας να μπορεί να επαναχρησιμοποιηθεί, αλλά και το ενσωματωμένο ECC να μπορεί να λειτουργήσει χωρίς πρόβλημα σε κάθε γλώσσα προγραμματισμού, οι ερευνητές υλοποίησαν την εφαρμογή με τη βοήθεια της **Wiselib** βιβλιοθήκης. Για να μπορέσουν να τεστάρουν τις μεθόδους τους, χρησιμοποίησαν το **SmartSantander testbed** σε ένα σύστημα περιορισμένων τεχνικών χαρακτηριστικών. Για να διασφαλίσουν την εγκυρότητα των ελέγχων, χρησιμοποίησαν το **Zero Knowledge Protocol**, με πολλές και διαφορετικές εισόδους που αντιστοιχούσαν σε πραγματικές καταστάσεις. Όλα τα τεστ έδειξαν πως η διαδικασία της κρυπτογράφησης σε κάθε περίπτωση συνέβαινε σε χρονικό πλαίσιο κάτω του ενός λεπτού. Το αποτέλεσμα ήταν η χρήση της elliptic curve, με σκοπό την προστασία των προσωπικών δεδομένων του χρήστη, αλλά και την διασφάλιση της ακεραιότητας και της εμπιστευτικότητας. Αυτό είναι ιδιαίτερα χρήσιμο σε περιπτώσεις που η εφαρμογή καλείται να λειτουργήσει σε πολλές διαφορετικές περιορισμένων

χαρακτηριστικών συσκευές. Οι διαδικασίες που χρησιμοποιούν την Elliptic Curve, βασίστηκαν στον αλγόριθμο του Diffie Hellman. Χρησιμοποιήθηκε κατακερματισμός SHA-1, όπου χρειάστηκε. Εν κατακλείδι, το τελικό κλειδί είχε μήκος μόλις 160-bit αλλά αποτελεσματικότητα ίδια με ένα κλειδί 1024-bit σε ένα συμβατικό κρυπτοσύστημα.

6.6 ASAP: An Anonymous Smart-Parking and Payment Scheme in Vehicular Networks [6]

Η παρούσα μελέτη προτείνει μια εφαρμογή έξυπνου πάρκινγκ, η οποία συμβάλλει στην ανωνυμότητα του οδηγού, τόσο κατά τη χρήση της όσο και κατά τη διαδικασία πληρωμής, διαδικασία που μπορεί να πραγματοποιηθεί από μια τρίτη εφαρμογή. Οι ερευνητές ονομάζουν την εφαρμογή αυτή ASAP (Anonymous Smart Parking and Payment). Σκοπός της είναι να ενημερώνει τους οδηγούς για την ενοικίαση θέσεων στάθμευσης κοντά στην εργασία τους, σε οργανωμένους χώρους στάθμευσης ή στην άκρη του δρόμου. Δίνει επίσης στους προμηθευτές θέσεων πάρκινγκ την δυνατότητα να μισθώνουν τις θέσεις στάθμευσής τους. Στη συνέχεια, χρησιμοποιώντας την υπηρεσία WhoPay, δίνει τη δυνατότητα στους χρήστες να πληρώνουν ανώνυμα, χρησιμοποιώντας ένα μοναδικό κλειδί πληρωμής. Ένα **Trusted Authority** είναι υπεύθυνο για την ανάθεση του IDi του προμηθευτή, με τη χρήσης τεχνικής Bilinear Pairing. Αρχικά, ο οδηγός και οι προμηθευτές εγγράφονται στην **TA**. Όταν ο οδηγός θέλει να αναζητήσει μια θέση στάθμευσης, στέλνει το αίτημά του με τη μορφή ενός **query**, υπογεγραμμένο από το TA. Του αποδίδεται επίσης ένα ψευδο-αναγνωριστικό PIDj, από την TA, το οποίο χρησιμοποιείται από τον διακομιστή (**cloud server**) για cross validation. Το query είναι ένα hashmap, που περιέχει το request του οδηγού για στάθμευση. Στη συνέχεια, ο διακομιστής δημοσιεύει τα queries στους προμηθευτές. Εάν ο προμηθευτής επαληθεύσει τη διαθεσιμότητα της θέσης στάθμευσής του, στέλνει μια αναφορά στον cloud server. Η **TA**, χρησιμοποιώντας έναν μοναδικό αριθμό k, δημιουργεί ένα προσωρινό δημόσιο κλειδί που χρησιμοποιείται σε κάθε συναλλαγή. Για κάθε κλειδί που πρόκειται να παραχθεί, ο αλγόριθμος τυχαίας επιλογής (Random Selection) χρησιμοποιεί τον αριθμό k, ο οποίος επίσης εκδίδεται από την TA. Ο server αντιστοιχίζει το query του οδηγού με την έκθεση του προμηθευτή και στη συνέχεια ξεκινά η διαδικασία πληρωμής. Ο διακομιστής δημιουργεί ένα κουπόνι συγκεκριμένης αξίας και το στέλνει στον οδηγό, υπογεγραμμένο από την TA, χρησιμοποιώντας και πάλι ένα προσωρινό δημόσιο κλειδί, ξεχωριστό για κάθε κουπόνι. Όταν ο οδηγός θέλει να πληρώσει, αγοράζει ένα συγκεκριμένο ποσό κουπονιών, που αντιστοιχεί στο συνολικό κόστος της στάθμευσης. Στη

συνέχεια, στέλνει το hash των υπογεγραμμένων κουπονιών πίσω στον διακομιστή για να επαληθεύσει τη συναλλαγή και, μόλις δημιουργηθεί η σύνδεση, η πληρωμή πραγματοποιείται μέσω της εφαρμογής WhoPay. Στην παρούσα μελέτη, παρατηρούμε τη χρήση της τεχνικής Bilinear Pairing, η οποία εξασφαλίζει ένα ασφαλές κανάλι μεταξύ του προμηθευτή θέσης στάθμευσης και του οδηγού. Η ακεραιότητα, η ανωνυμία και η εμπιστευτικότητα τόσο του οδηγού όσο και του προμηθευτή διασφαλίζονται από την TA. Τέλος, ο διακομιστής εξασφαλίζει μια ασφαλή και ανώνυμη διαδικασία πληρωμής, χρησιμοποιώντας τον αλγόριθμο Random Selection, καθιστώντας έτσι δυνατή την ανώνυμη πληρωμή των τελών από μια τρίτη υπηρεσία, την WhoPay.

6.7 BSFP: Blockchain-Enabled Smart Parking With Fairness Reliability and Privacy Protection [7]

Η παρούσα μελέτη ασχολείται με ένα σύστημα έξυπνης στάθμευσης, το οποίο λειτουργεί με τη χρήση της τεχνολογίας blockchain και στοχεύει στην δίκαια κατανομή των θέσεων στάθμευσης και προστασίας της ιδιωτικής ζωής. Ονομάζεται BSFP: Blockchain-Enabled Smart Parking With Fairness, Reliability and Privacy Protection. Στόχος της είναι να δημιουργήσει μια ασφαλή σύνδεση μεταξύ ενός ιδιοκτήτη θέσης στάθμευσης, μιας RoadSide Unit (RSU) και ενός οδηγού ηλεκτρικού οχήματος, χρησιμοποιώντας τη σύνδεση του ηλεκτρικού οχήματος στο διαδίκτυο και τη δυνατότητα συναλλαγών blockchain. Ο αποκεντρωμένος χαρακτήρας του διασφαλίζει το απόρρητο των προσωπικών πληροφοριών, την ανωνυμία και την ακεραιότητα, καθώς και συνδράμει στην αποτροπή της αποκάλυψης της θέσης τόσο για τον οδηγό όσο και για τον ιδιοκτήτη του χώρου στάθμευσης. Μια έμπιστη αρχή (TA) παράγει ένα κοινόχρηστο κλειδί. Στη συνέχεια χρησιμοποιεί το κλειδί για να δημιουργήσει ένα κύριο δημόσιο κλειδί και ένα κύριο ιδιωτικό κλειδί. Χρησιμοποιεί το ιδιωτικό κλειδί για να δημιουργήσει και να υπογράψει μια ομάδα δημόσιων κλειδιών ανάλογα με τον αριθμό των εγγεγραμμένων οδηγών και μια ξεχωριστή ομάδα ανάλογα με τον αριθμό των εγγεγραμμένων ιδιοκτητών χώρων στάθμευσης. Για κάθε εγγεγραμμένο ιδιοκτήτη χώρου στάθμευσης, η TA κρυπτογραφεί κάθε ακριβή θέση του χώρου στάθμευσης και επίσης τον διαθέσιμο χρόνο του χώρου στάθμευσης. Οι προσωπικές πληροφορίες του οδηγού φιλτράρονται με την τεχνική **bloom filter** και δεν εκτίθενται ποτέ στον ιδιοκτήτη του χώρου στάθμευσης, στις μονάδες **RoadSide** ή στο blockchain. Όταν ο οδηγός Dj χρειάζεται μια θέση στάθμευσης, στέλνει ένα κρυπτογραφημένο αίτημα στο

blockchain μέσω μιας RSU. Εκεί, η αίτηση υπογράφεται από το δημόσιο κλειδί της ομάδας RSU, χρησιμοποιώντας την **υπογραφή BBS**. Το αίτημα αποτελείται από την τρέχουσα διεύθυνση και τη χρονοσφραγίδα, οι οποίες κρυπτογραφούνται και στη συνέχεια αποστέλλονται από την RSU στο δίκτυο blockchain. Ο ομότιμος του δικτύου blockchain λαμβάνει το αίτημα, χρησιμοποιεί το δημόσιο κλειδί του RSU για να επαληθεύσει την ομαδική υπογραφή. Εάν η επαλήθευση είναι επιτυχής, εκδίδεται το έξυπνο συμβόλαιο. Στη συνέχεια πραγματοποιείται αντιστοίχιση βάσει χρόνου για την αντιστοίχιση του αιτήματος του οδηγού με τη διαθεσιμότητα του ιδιοκτήτη του χώρου στάθμευσης, χρησιμοποιώντας την κρυπτογραφημένη χρονοσφραγίδα του οδηγού. Εάν ο ιδιοκτήτης του χώρου στάθμευσης δεχτεί, ανταλλάσσονται πληροφορίες μεταξύ του οδηγού και του ίδιου και στη συνέχεια πρέπει να επικοινωνήσουν φυσικά μεταξύ τους (μέσω μηνυμάτων ή τηλεφωνημάτων) για να επαληθεύσουν τα τέλη στάθμευσης και να προχωρήσουν στη στάθμευση. Εν κατακλείδι, παρακολουθήσαμε τη χρήση της ομαδικής υπογραφής BBS και την αποτελεσματική χρήση της για την υπογραφή πολλαπλών οντοτήτων (RSU, κλειδιά και συναλλαγές των οδηγών και των ιδιοκτητών χώρων στάθμευσης). Είδαμε τη χρήση των bloom filters για την προσθήκη θορύβου στις προσωπικές πληροφορίες των χρηστών της εφαρμογής. Συναντήσαμε επίσης τη χρήση της τεχνολογίας blockchain, ως τρόπο μετάδοσης δεδομένων με τη μορφή συναλλαγών.

6.8 CBACS: A Privacy-Preserving and Efficient Cache-Based Access Control Scheme for Software Defined Vehicular Networks [8]

Σε αυτή τη μελέτη, βλέπουμε μια πολύ ενδιαφέρουσα προσέγγιση του τρόπου με τον οποίο μπορούν να ανταλλάσσονται αποθηκευμένες πληροφορίες με τη χρήση δικτύων οχημάτων. Αυτό το σύστημα προτείνει αμοιβαίες και ασφαλείς επικοινωνίες μεταξύ των οχημάτων και **fog nodes**, οι οποίες είναι συσκευές που μεταδίδουν συνεχώς τη λίστα αποθηκευμένων πληροφοριών τους (δείκτης, σύντομη περιγραφή και μήκος), στην περιοχή εύρους ζώνης τους. Παρακολουθούμε επίσης το πρωτόκολλο TESLA που χρησιμοποιείται για ασφαλή έλεγχο ταυτότητας, το ProVerif για εύκολη επαλήθευση της απάντησης-πρόκλησης και το Pedersen Commitment. Ένας πάροχος υπηρεσιών είναι υπεύθυνος για τη δημιουργία των ιδιωτικών και δημόσιων κλειδιών, των ψευδωνύμων PID και την εγγραφή νέων κόμβων και οχημάτων ομίχλης στο σύστημα. Χρησιμοποιώντας την ελλειπτική καμπύλη, ο πάροχος υπηρεσιών (SP) παράγει ένα ιδιωτικό κλειδί και μια ομάδα δημόσιων κλειδιών, ανάλογα με τον αριθμό των **fog nodes** που πρόκειται να χρησιμοποιηθούν. Χρησιμοποιεί το Pedersen

Commitment, για να αποκρύψει τα δυναμικά μεταβαλλόμενα διαπιστευτήρια πρόσβασης, κατά τη διάρκεια της μετάδοσής τους στα οχήματα. Στη συνέχεια χρησιμοποιεί το πρωτόκολλο TLS για να εγγράψει τα fog nodes στο σύστημα. Ακολουθώντας την ίδια διαδικασία, τα οχήματα εγγράφονται στο σύστημα χρησιμοποιώντας ένα ψευδώνυμο περιορισμένου χρόνου και ένα ιδιωτικό κλειδί που εκχωρείται από τον SP και θα χρησιμοποιηθεί για την υπογραφή των προκλήσεων που αποστέλλονται στα fog nodes. Το πρωτόκολλο TESLA χρησιμοποιείται για να αποτρέψει την τροποποίηση της λίστας προσωρινής αποθήκευσης περιεχομένου των fog node. Η ανταλλαγή πληροφοριών έχει ως εξής. Όταν ένα όχημα λαμβάνει τη λίστα κρυφής μνήμης ενός fog node, την επαληθεύει πρώτα χρησιμοποιώντας το ProVerif. Στη συνέχεια, αποστέλλεται μια πρόκληση στο fog node προκειμένου να διασφαλιστεί η φρεσκάδα των πληροφοριών του fog node. Εάν η πρόκληση ικανοποιηθεί, ο κατάλογος κρυφής μνήμης πιστοποιείται και χρησιμοποιείται από το όχημα κατά το δοκούν. Προκειμένου να ενημερωθούν οι πληροφορίες cache, ένας ελεγκτής SDN υπολογίζει τη μνήμη του fog node. Στη συνέχεια, καθ' όλη τη διάρκεια των αιτημάτων από ένα κοντινό όχημα, δημιουργείται ένας βρόχος και η νέα λίστα προσωρινής αποθήκευσης γεμάτη με δεδομένα μεταδίδεται συνεχώς στο fog node. Ο ελεγκτής SDN αντικαθιστά τις πληροφορίες του fog node. Εν κατακλείδι, παρατηρήσαμε για άλλη μια φορά τη χρήση της τεχνικής ελλειπτικής καμπύλης, λόγω της ταχύτητάς της στη δημιουργία ομαδικών κλειδιών για έναν αριθμό δεκτών. Είδαμε το πρωτόκολλο TESLA που εξασφάλιζε την ακεραιότητα των πληροφοριών των fog nodes, οι οποίες μεταδίδονταν συνεχώς στον έξω κόσμο και στις οποίες θα μπορούσε να έχει πρόσβαση ο καθένας. Το σύστημα του παρόντος εγγράφου διασφαλίζει την ανωνυμία των πληροφοριών του οχήματος, η διαρροή των οποίων θα μπορούσε να οδηγήσει σε ευαίσθητες πληροφορίες του οδηγού. Προστατεύει επίσης τις δημόσιες παραμέτρους του συστήματος και την τροποποίηση των διαπιστευτηρίων πρόσβασης, χρησιμοποιώντας τη δέσμευση Pedersen.

6.9 Identity Privacy Protection in Smart Parking Navigation [9]

Η παρούσα μελέτη προτείνει ένα ασφαλές σύστημα πλοήγησης σε ένα έξυπνο πάρκινγκ, χρησιμοποιώντας Vehicular Ad hoc networks. Ο οδηγός πρέπει να αποκτήσει μια ενσωματωμένη μονάδα (**OBU**). Για να πραγματοποιηθεί η εγγραφή του, πρέπει να προσκομίσει την άδεια οδήγησής του, ψηφιακά. Αυτό το σύστημα, που ονομάζεται P-SPAN, απαιτεί επίσης τη χρήση μιας αξιόπιστης αρχής (Trusted Authority - TA) και μονάδων στην άκρη του δρόμου (RSU), οι οποίες συνδέονται με έναν διακομιστή νέφους μέσω ασφαλούς σύνδεσης στο διαδίκτυο. Όταν ο οδηγός συνδέεται στην υπηρεσία, υποβάλλει την ψηφιακή του άδεια οδήγησης στην TA, χρησιμοποιώντας την OBU του, η οποία είναι συνδεδεμένη με την πλησιέστερη RSU,

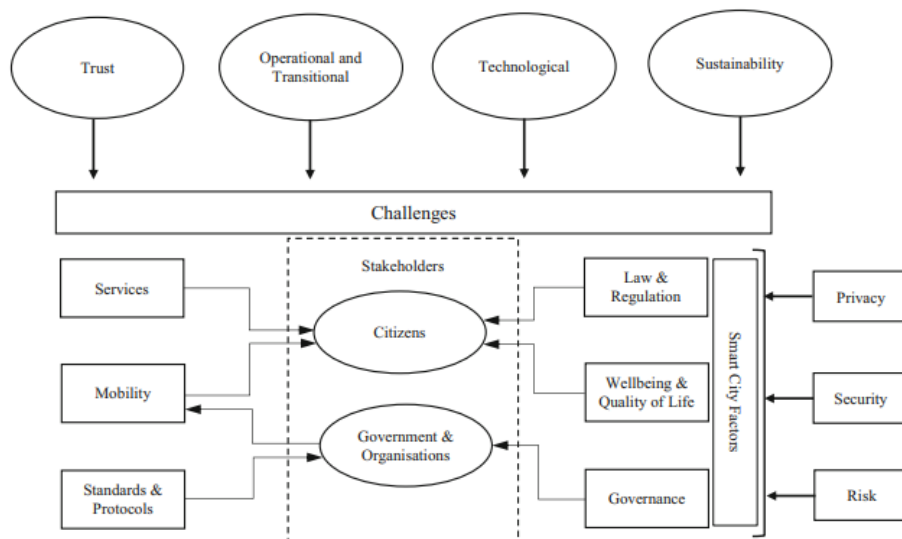
συνδέοντάς την αντίστοιχα με την TA. Εκτελείται το πρωτόκολλο απόδειξης γνώσης μηδενικής γνώσης, χρησιμοποιώντας την υπογραφή PS. Η TA ορίζει μια παράμετρο ασφαλείας P_i ή 160 ή 256 bit, χρησιμοποιώντας την κρυπτογραφία ελλειπτικής καμπύλης. Ένας μεγάλος πρώτος αριθμός αποτελούμενος από P bits, χρησιμοποιείται για τη δημιουργία μιας γεννήτριας κλειδιών. Για την κρυπτογράφηση και την αποκρυπτογράφηση των παραμέτρων της γεννήτριας χρησιμοποιείται ο αλγόριθμος AES. Ο TA υπολογίζει και επαληθεύει την απόδειξη και χρησιμοποιεί τη γεννήτρια g για να δημιουργήσει δύο νέες τιμές (ID, A_1) και (ID, W, W') . Το A_1 είναι η υπογραφή του TA. Διανέμει την πρώτη τιμή σε ένα μυστικό και ένα δημόσιο μέρος και στη συνέχεια τη μεταβιβάζει στον οδηγό, μέσω του ίδιου ασφαλούς καναλιού που αναφέρθηκε προηγουμένως. Τη δεύτερη τιμή, την αποθηκεύει στην ασφαλή βάση δεδομένων του σύννεφου. Τα δύο μέρη αποτελούνται από τη γνώση μηδενικής απόδειξης, οπότε ο TA δεν γνωρίζει τίποτα για την ταυτότητα του οδηγού, διατηρώντας έτσι την ανωνυμία. Όταν ο οδηγός IDi χρησιμοποιεί την υπηρεσία πλοήγησης στάθμευσης, η OBU προωθεί ένα ερώτημα στάθμευσης στην πλησιέστερη RSU. Το ερώτημα αποτελείται από μια χρονοσφραγίδα, ένα αποδεκτό εύρος τιμών, έναν αναμενόμενο χρόνο άφιξης, έναν χρόνο λήξης. Πριν η OBU προωθήσει το ερώτημα, το κρυπτογραφεί πρώτα χρησιμοποιώντας τον αλγόριθμο κρυπτογράφησης AES. Το νέφος παράγει ένα αποτέλεσμα πλοήγησης RS για κάθε ερώτημα που αποστέλλεται και το αποστέλλει στην RSU που βρίσκεται πλησιέστερα στην OBU-πηγή. Περιλαμβάνονται η γεωγραφική θέση του χώρου στάθμευσης, το κόστος, οι συνιστώμενες θέσεις στάθμευσης και τα εύρη τιμών. Επίσης, όσον αφορά τα RSU, σε κάθε RSU αποδίδεται ένας μοναδικός αριθμός RID που το συνδέει με τη θέση του. Χρησιμοποιώντας έναν τυχαίο πραγματικό αριθμό ως μυστικό κλειδί, η γεννήτρια του TA χρησιμοποιείται για τη δημιουργία ενός δημόσιου κλειδιού. Κάθε RSU ορίζει δύο φίλτρα Bloom, τα οποία χρησιμοποιούνται κάθε φορά που ένας οδηγός στέλνει το ερώτημα στάθμευσης μέσω της OBU. Αυτά τα φίλτρα Bloom χρησιμοποιούνται για τον εντοπισμό της θέσης του οδηγού. Η τοποθεσία κάθε RSU είναι επίσης κρυπτογραφημένη και κρυμμένη από τον διακομιστή νέφους. Συνοψίζοντας, αυτό το σύστημα κρυπτογραφεί τις προσωπικές πληροφορίες του οδηγού και εξασφαλίζει την ανωνυμία του. Είναι ασφαλές επειδή ζητείται η ψηφιακή άδεια οδήγησης πριν από τη χρήση. Αποκρύπτει τη θέση του οδηγού χρησιμοποιώντας τα φίλτρα bloom, διατηρώντας την πλήρη ακεραιότητα και εμπιστευτικότητα των δεδομένων του. Η κρυπτογραφία ελλειπτικής καμπύλης ενισχύει τους αλγόριθμους κρυπτογράφησης που αναφέρθηκαν, όπως είναι ο AES, χρησιμοποιώντας ένα κλειδί μικρότερου μεγέθους 160 ή 256 bit. Αυτό το μειωμένο μέγεθος είναι σημαντικό, επειδή οι RSU και οι OBU έχουν περιορισμένες προδιαγραφές υλικού. Είναι επίσης ενεργειακά και οικονομικά αποδοτικό για τον διακομιστή νέφους που φιλοξενεί, για τους ίδιους λόγους.

6.10 IoTRec: The IoT Recommender for Smart Parking System [10]

Η παρούσα εργασία παρουσιάζει μια Internet of Things προσέγγιση, στην προσπάθεια να δημιουργηθεί μια ασφαλής εφαρμογή έξυπνου πάρκινγκ. Κατά την υλοποίησή της, στόχος των ερευνητών ήταν η εφαρμογή να καλύπτει τον χρήστη, σύμφωνα με το General Data Protection Regulation. Λειτουργεί με τη βοήθεια της τεχνολογίας **IoTRec** (IoT recommender), η οποία βασίζεται σε δεδομένα αισθητήρων πάρκινγκ αλλά και από αισθητήρες που βρίσκονται σε φανάρια στο πλάι του δρόμου. Οι αισθητήρες μπορεί να βρίσκονται στο πλάι του δρόμου, κάτω από την θέση πάρκινγκ ή μέσα σε ιδιωτικά πάρκινγκ. Παρέχει επίσης ένα εργαλείο που παρουσιάστηκε στο συνέδριο H2020 EU-KR WISE-IoT project, το **Trust Monitoring**. Με την βοήθεια του σημασιολογικού ιστού, χρησιμοποιήθηκαν τα **FIWARE** μοντέλα, για την αναπαράσταση των οντολογιών και των οντοτήτων όπως ο χώρος του πάρκινγκ, το αυτοκίνητο κ.α. Τα δεδομένα του πάρκινγκ είναι δομημένα σε μορφή JSON για την γρήγορη καταγραφή των ιδιοτήτων των οντοτήτων που καλύπτει η εφαρμογή. Ο χρήστης Η εφαρμογή, σε έναν cloud server, χρησιμοποιεί τα δεδομένα των parking sensors αλλά και την τοποθεσία του χρήστη, για να υπολογίσει την κοντινότερη διαδρομή. Επίσης, με την τεχνολογία του Trust Monitoring, χρησιμοποιούνται trust scores, ώστε ο οδηγός να οδηγηθεί στην κοντινότερη αλλά και πιο έμπιστη θέση πάρκινγκ. Δεδομένα από τον σημασιολογικό ιστό (Internet of Things), συλλέγονται για να υπολογιστεί η κίνηση και κατά συνέπεια, η βέλτιστη διαδρομή για τον χρήστη προς την θέση πάρκινγκ. Επίσης, για τις θέσεις που δεν διαθέτουν κάποιον αισθητήρα, συλλέγονται δεδομένα από τους γειτονικούς αισθητήρες με σκοπό να παρουσιάσουν περιοχές στις οποίες είναι πιθανό ο οδηγός να μπορέσει με ευκολία να παρκάρει. Μόλις ο IoTRec εντοπίσει το καλύτερο δυνατό σημείο, η τεχνολογία BRouter routing engine υπολογίζει την βέλτιστη διαδρομή. Από άποψη ασφαλείας, δυστυχώς η έρευνα δεν διαθέτει στοιχεία που θα μας βοηθήσουν να αναγνωρίσουμε την προστασία ή μη των προσωπικών δεδομένων του χρήστη. Παρ' ολ' αυτά, γνωρίζουμε πως εφαρμογές που βασίζονται σε συλλογή δεδομένων από τον σημασιολογικό ιστό, είναι κατασκευασμένες με τέτοιο τρόπο ώστε να επικοινωνούν βέλτιστα με γλώσσες μηχανής. Αυτό μας προϊδεάζει να καταλάβουμε πως τα δεδομένα του χρήστη κρυπτογραφούνται σε κάποια μορφή, ορισμένη ώστε να μπορέσει να την διαβάσει το σύστημα που θα την επεξεργαστεί. Ένας τρίτος παράγοντας που θα επιθυμεί να υποκλέψει πληροφορίες θα πρέπει να καταλάβει την φύση των πληροφοριών ,εάν επιθυμεί να εξάγει αληθινά δεδομένα όπως τα στοιχεία ή και η τοποθεσία του χρήστη.

6.11 Security, Privacy and Risks Within Smart Cities: Literature Review and Development of a Smart City Interaction Framework [11]

Η έρευνα αυτή εστιάζει στην μείωση των νομικών ρίσκων για μια έξυπνη πόλη, αλλά και την ασφαλή χρήση των προσωπικών δεδομένων των χρηστών. Επίσης προτείνει τρόπους για την ασφαλή χρήση των υπηρεσιών που συναντάμε στα έξυπνα τηλέφωνα, μέσα από άλλες έρευνες που οι συντάκτες συγκέντρωσαν. Αρχικά, μέσα από την παρουσίαση ενός γράφου, παρατηρούμε πως τα δεδομένα που συγκεντρώνονται στο διαδίκτυο με τη χρήση Internet of Things τεχνολογιών, είναι ευαίσθητα ιδιαίτερα σε επιθέσεις man in the middle, αφού συνήθως, τα τεχνικά χαρακτηριστικά των συσκευών που πραγματοποιούν IoT operations, είναι περιορισμένα σε μνήμη και ταχύτητα. Από μια άλλη μελέτη που παρουσιάζεται, οι συντάκτες παρουσιάζουν την τεχνολογία **FIDO (Fast ID Online)** ως λύση στο πρόβλημα της αυθεντικοποίησης των δεδομένων. Η τεχνολογία αυτή αποτελεί μια cloud υπηρεσία αυθεντικοποίησης, όπου οι διαδικασίες εκτελούνται από συσκευή προς το δίκτυο ή από τη συσκευή απευθείας προς το cloud, μέσω ασφαλών καναλιών επικοινωνίας κρυπτογραφημένα από την υπηρεσία. Η εργασία αναφέρει πολλές ακόμα χρήσεις των IoT σε έξυπνες πόλεις, γι' αυτό εμείς θα εστιάσουμε στο κομμάτι της ασφάλειας. Ο πολυωνυμικός χαρακτήρας των εφαρμογών IoT καλεί τις αρχές να δημιουργήσουν ένα νομικό framework κατά το οποίο θα συνδιάζει τους βασικούς παρονομαστές, αλλά και τις σχέσεις τους με την τεχνολογία. Για παράδειγμα, βλέπουμε πως ανάμεσα στη σχέση εμπιστοσύνης (με την τεχνολογία IoT) και πολίτη, μεσολαβούν προκλήσεις. Ο πίνακας είναι ο ακόλουθος.



Security, Privacy and Risks Within Smart Cities: Literature Review and Development of a Smart City Interaction Framework [11], Fig 3.

6.12 *Parking recommender system privacy preservation through anonymization and differential privacy* [12]

Στην έρευνα αυτή, οι ερευνητές εξετάζουν το πρόβλημα της απρόσκοπτης και ανεξέλεγκτης μεταφοράς των προσωπικών δεδομένων των χρηστών, κατά την χρήση IoT τεχνολογιών, αλλά ιδιαίτερα κατά τη χρήση εφαρμογών έξυπνου πάρκινγκ. Επίσης προσπαθούν να δώσουν λύση στο μείζον αυτό πρόβλημα με δύο τρόπους. Αρχικά, με την ανάλυση του ιστορικού της θέσης πάρκινγκ, με τη χρήση του αλγορίθμου k-anonymity αλλά και με τη χρήση τεχνικών προσθήκης θορύβου, με τεχνικές differential privacy. Το σύστημα της έρευνας αυτής βασίζεται σε δύο εφαρμογές. Η πρώτη ονομάζεται Smart Parking System και αποτελεί τον ρόλο μιας **Trusted Authority**. Όταν ο χρήστης συνδέεται στην εφαρμογή, τα στοιχεία του αποθηκεύονται σε μια **Anonymized DB**. Η βάση δεδομένων αυτή, δηλαδή, χρησιμοποιεί έναν αλγόριθμο που προσθέτει “θόρυβο” στα δεδομένα, προτού αυτά να αποθηκευτούν στην βάση δεδομένων της εφαρμογής. Η δεύτερη εφαρμογή ονομάζεται Parking Recommender System και επικοινωνεί με την ανώνυμη βάση δεδομένων, με σκοπό να αποθηκεύσει τα αλλοιωμένα πλέον δεδομένα των χρηστών, σε κατηγορίες όπως οι “Parking Information”, η “Traffic Information”, η “Sensors Quality” και τέλος “Other Metrics”. Η διαδικασία έχει ως εξής. Ο χρήστης που συνδέεται στην εφαρμογή έξυπνου πάρκινγκ, κάνει ένα αίτημα προς τον cloud server της εφαρμογής “Smart parking system”. Το αίτημα του αποτελείται από το IDi του χρήστη αλλά και την τοποθεσία του. Επειδή όπως είπαμε, η πρώτη εφαρμογή είναι και TA, το κανάλι επικοινωνίας θεωρούμε πως είναι ασφαλές. Αρχικά, η εφαρμογή στέλνει σε μια τρίτη εφαρμογή parking recommender το request του χρήστη, αλλοιωμένο. Στη συνέχεια παίρνει πίσω από την τρίτη εφαρμογή, τα αποτελέσματα της επιλογής και τα προωθεί προς τον χρήστη. Η TA αποθηκεύει τις αλλοιωμένες πληροφορίες του χρήστη στην βάση δεδομένων της, αλλά και άλλες πληροφορίες όπως οι κριτικές των χρηστών, οι χρονοσφραγίδες των συναλλαγών και τα σημεία στάθμευσης. Στη συνέχεια, στέλνει τα δεδομένα αυτά στην δεύτερη εφαρμογή που διαχειρίζεται, την “Parking Recommender System” και δημιουργεί ένα προφίλ για τον χρήστη, ανάλογα με τις προσωπικές του πληροφορίες και προτιμήσεις. Έτσι, δεν θα στείλει τον χρήστη πίσω σε μια θέση πάρκινγκ που έχει αφήσει ο ίδιος κακή κριτική, ή δεν θα στείλει και γενικότερα χρήστες της εφαρμογής σε θέσεις πάρκινγκ που διαθέτουν κακές κριτικές. Για την κρυπτογράφηση των στοιχείων του χρήστη, χρησιμοποιείται η differential privacy, μια προσέγγιση η οποία βασίζεται στην κατανομή Laplace, που προσθέτει θόρυβο στα στοιχεία του χρήστη. Τέλος, η έρευνα κλείνει με πειράματα που έγιναν για k αριθμό χρηστών και στοιχείων, αποδεικνύοντας την λειτουργικότητα του συστήματος.

6.13 Parking Management A blockchain-based privacy-preserving system [13]

Η μελέτη αυτή προτείνει μια μέθοδο μέσα από την οποία ο χρήστης μπορεί να βασιστεί σε μια εφαρμογή έξυπνου πάρκινγκ, με τη χρήση τεχνολογίας blockchain, αναιρώντας την ανάγκη για τρίτες-εφαρμογές να εμπλακούν στην διαδικασία. Οι ερευνητές δόμησαν ένα σύστημα το οποίο χρησιμοποιεί την τεχνολογία **BlockChainOpenSource (BCOS)** , μια προσέγγιση που βοηθά στην έξυπνη και ανώνυμη δημιουργία συμβολαίων που στοχεύει στην ασφαλή δέσμευση θέσεων στάθμευσης για τους χρήστες τη εφαρμογής. Η εφαρμογή που προτείνουν χωρίζεται σε τρία μέρη. Στο πρώτο μέρος εντάσσονται οι οδηγοί αλλά και οι ενοικιαστές θέσεων στάθμευσης. Στο δεύτερο μέρος, εντάσσονται οι έμπιστες οντότητες όπως το κράτος αλλά και άλλες υπηρεσίες έκδοσης ασφαλών πιστοποιητικών. Για να εγγραφεί ένας χρήστης της πρώτης κατηγορίας στο σύστημα, θα πρέπει να επικοινωνήσει μέσω τις εφαρμογής με κάποια οντότητα της δεύτερης κατηγορίας, με αυτοματοποιημένο ή μη τρόπο. Τέλος, η δεύτερη κατηγορία επικοινωνεί με την τρίτη κατηγορία, η οποία αποτελεί το σύνολο του blockchain. Έτσι τα δεδομένα της εφαρμογής ταξιδεύουν στο κύκλωμα, με τη χρήση ασφαλών και έμπιστων καναλιών επικοινωνίας που δημιουργούνται είτε από έμπιστες οντότητες είτε από το ίδιο το κράτος. Στη συνέχεια αποθηκεύονται στο blockchain, αποκεντριοποιώντας με επιτυχία το σύστημα και διασφαλίζοντας την ακεραιότητα των στοιχείων των χρηστών αλλά και προσδίδοντας προστασία και σεβασμό στην ιδιωτικότητα των στοιχείων τους. Επίσης αξίζει να σημειώσουμε πως η σύνδεση της εφαρμογής με την τεχνολογία του blockchain, καθιστά το blockchain μια παντελώς προσβάσιμη βάση δεδομένων, μέσα στην οποία μπορούν να πραγματοποιηθούν με ασφάλεια ενέργειες όπως συναλλαγές χρημάτων, αναλύσεις, έρευνες και όλων των ειδών παρόμοιες εφαρμογές. Η εφαρμογή BCOS βασίζεται στην τεχνολογία Ethereum. Για τις συναλλαγές χρημάτων μισθώσεων των θέσεων στάθμευσης, ακολουθεί η εξής διαδικασία. Το όχημα που επιθυμεί να μισθώσει την θέση στάθμευσης, δημιουργεί μια συναλλαγή με ένα σετ από εισόδους και εξόδους. Κάθε είσοδος αποτελείται από το δημόσιο κλειδί (**PK_s**) της οντότητας που επιθυμεί να στείλει χρήματα (στην περίπτωση αυτή του οδηγού του οχήματος), το ιδιωτικό κλειδί του αποστολέα (**SK_s**), το δημόσιο κλειδί του παραλήπτη (**PK_r**) και το ποσό των χρημάτων σε BCOS συνάλλαγμα (δηλαδή Ethereum). Το ιδιωτικό κλειδί του αποστολέα χρησιμοποιείται για την υπογραφή του συμβολαίου συναλλαγής και το δημόσιο κλειδί του παραλήπτη , για την κρυπτογράφηση της. Τέλος, αξίζει να αναφέρουμε πως στο σύστημα χρησιμοποιούνται μοναδικά συμβόλαια συναλλαγών με ψηφιακή υπόσταση, πράγμα που ενισχύει την ασφάλεια και την ακεραιότητα των στοιχείων της εκάστοτε συναλλαγής.

6.14 PriParkRec: Privacy-Preserving Decentralized Parking Recommendation Service [14]

Στην έρευνα αυτή οι ερευνητές προσεγγίζουν το θέμα της ασφάλειας στις εφαρμογές έξυπνου πάρκινγκ. Δημιουργούν μια εφαρμογή που χρησιμοποιεί την τεχνολογία blockchain και υπόσχεται έναν αποκεντροποιημένο τρόπο κατανομής των πληροφοριών του χρήστη, που προσδίδει αυθεντικότητα των στοιχείων του, ανωνυμότητα και σέβεται την ιδιωτικότητα του. Οι ερευνητές ονόμασαν την εφαρμογή τους **PriParkRec**. Για την επίδειξη της ικανότητας της εφαρμογής τους, χρησιμοποίησαν το **Zero-Knowledge Proof**, την τεχνική **obvious pseudorandom function**, **privacy preserving payment**, **blind certificate authorities** και τέλος **privacy preserving electronic toll collection**. Η εφαρμογή χρησιμοποιεί επίσης Internet of Things τεχνολογίες. Οι ερευνητές διαχωρίζουν αρχικά την εφαρμογή σε 3 βασικές οντότητες, τους **Parking space providers (Pvd)** που αποτελούν τους μισθωτές των θέσεων στάθμευσης. Εδώ να ξεκαθαριστεί πως στην έρευνα συμπεριλαμβάνονται μισθωτές μεμονομένων θέσεων στάθμευσης και όχι ολόκληρων πάρκινγκ. Επίσης, υπάρχουν οι **Parking Space Requesters (Rqt)**, οι οποίοι αποτελούν τους χρήστες - πελάτες της εφαρμογής. Τέλος υπάρχει ο **Parking Service provider (SP)**, ο οποίος αποτελεί τον μεσολαβητή ανάμεσα στις συναλλαγές που εκτελούνται ανάμεσα στις πρώτες δύο οντότητες. Οι Pvd πρέπει να διαθέτουν μια εφαρμογή στο έξυπνο τηλέφωνο τους, μέσα από την οποία θα μπορούν να ελέγχουν τις μισθωμένες θέσεις στάθμευσης τους. Οι Rqt θα πρέπει να διαθέτουν επίσης μια εφαρμογή στο έξυπνο τηλέφωνο τους μέσα από την οποία θα μπορούν να δημιουργούν ένα έξυπνο συμβόλαιο με τον Pvd. Επίσης, θα πρέπει να εγκαταστήσουν στα αυτοκίνητα τους ένα OnBoard Unit (OBU), το οποίο θα συνδέεται με κοντινές Internet of Things τεχνολογίες και θα ενημερώνει περιοδικά τον SP για την τρέχουσα τοποθεσία του οχήματος. Θεωρούμε πως ο SP είναι Trusted Authority. Στην έρευνα, χρησιμοποιείται η προσέγγιση με Zero Knowledge Proof και τα δεδομένα που μεταφέρονται από και προς τον SP, κρυπτογραφούνται με τον αλγόριθμο **Re-Randomized Public-Key Encryption**. Όταν οι χρήστες Rqt ή Pvd συνδέονται με τον SP, στέλνουν ένα request το οποίο αναλαμβάνει μια **registration authority (RA)** που αποτελεί τμήμα του SP. Στους χρήστες διατίθεται ένα δημόσιο κλειδί αλλά και ένα πιστοποιητικό που υπογράφεται από την RA. Το πιστοποιητικό αυτό χρησιμοποιείται για την δημιουργία **queries** τα οποία δημιουργούνται από τους Rqt όταν κάνουν μια αίτηση αναζήτησης θέσης πάρκινγκ, αλλά και από τους Pvd όταν οι ίδιοι θέλουν να καταχωρήσουν την θέση στάθμευσής τους προς μίσθωση. Στη συνέχεια δημιουργούνται ανώνυμα στοιχεία μίσθωσης του ηλεκτρονικού συμβολαίου που θα διεξαχθεί στο περιβάλλον του blockchain. Για παράδειγμα, με τη χρήση του Ethereum, δημιουργείται ένας μοναδικός κωδικός που λειτουργεί ως δημόσιο κλειδί της εκάστοτε συναλλαγής, το οποίο συνδέεται ανώνυμα με το πορτοφόλι του μισθωτή και το οποίο χρησιμοποιεί ο πελάτης για να στείλει ηλεκτρονικά το συνάλλαγμα που αναγράφεται στο ηλεκτρονικό συμβόλαιο. Με την μέθοδο αυτή, διασφαλίζεται η ανωνυμότητα των φυσικών οντοτήτων της εφαρμογής. Επιπρόσθετα, τα προσωπικά στοιχεία траπέξης των οντοτήτων μένουν κρυφά, γεγονός που μπορεί να τα προστατέψει από επιθέσεις του κυβερνοχώρου, όπως η επίθεση Man-in-the-middle. Τέλος, οι ερευνητές στοχεύουν με την προσέγγιση τους αυτή να χρησιμοποιήσουν την αποκεντρομένη blockchain τεχνολογία με σκοπό την μη παραβίαση της ιδιωτικότητας των χρηστών, την κατανομή και κρυπτογράφηση των πληροφοριών τους και την

αυθεντικότητα τους, αφού χρησιμοποιείται για την μελέτη ο Zero Knowledge Proof αλγόριθμος σε συνδιασμό με την κρυπτογράφηση Re-Randomized Public-Key Encryption.

6.15 Privacy-Aware Fuzzy Skyline Parking Recommendation Using Edge Traffic Facilities [15]

Η μελέτη αυτή αποτελεί κάτι το πρωτάκουστο και πολύ ενδιαφέρον. Οι επιστήμονες έχουν στόχο την δημιουργία μια εφαρμογής έξυπνου πάρκινγκ, η οποία θα προστατεύει τα προσωπικά δεδομένα του χρήστη. Για να το πετύχουν αυτό, βασίστηκαν στις τεχνολογίες Internet of Things, και συγκεκριμένα σε **Edge Traffic Facilities**, δηλαδή σε τεχνολογίες ελέγχου κίνησης των δρόμων, όπως τα φανάρια και οι πινακίδες και τα **RoadSide Units (RSU)**. Επίσης, χρησιμοποίησαν τον αλγόριθμο **fuzzy skyline fusion algorithm**, του οποίου σκοπός είναι να αξιοποιήσει **linguistic variables**, με σκοπό την απευθείας παρακολούθηση των δρόμων, των θέσεων στάθμευσης και άλλων καναλιών οδικής επικοινωνίας. Η χρήση των μεταβλητών αυτών αποτελεί μια διέξοδο από τις μέχρι τώρα γνωστές μεθόδους δόμησης εφαρμογών έξυπνου πάρκινγκ, παρέχοντας απευθείας δεδομένα στον χρήστη με έναν έξυπνο και οικονομικό ως προς την χρήση των δεδομένων τρόπο. Το σχέδιο αυτό, για να λειτουργήσει, απαιτεί υποδομές μιας έξυπνης πόλης. Ο χρήστης επίσης πρέπει να διαθέτει την αντίστοιχη εφαρμογή στο έξυπνο τηλέφωνο του αλλά και σύνδεση στο διαδίκτυο. Η εφαρμογή για να λειτουργήσει, απαιτεί την απευθείας σύνδεση του τηλεφώνου στο διαδίκτυο και όχι κάποια OnBoard συσκευή. Η εφαρμογή λαμβάνει υπ' όψιν 3 τύπους αποκαλούμενους "fuzzy sets", εξ' ου και ο αλγόριθμος που χρησιμοποιείται. Οι αλγόριθμοι "fuzzy" παίρνουν ως είσοδο τις ζωντανές τιμές από πόρους, όπως στην περίπτωσή μας τα RSUs. Ως έξοδο μας δίνουν N δυνατά αποτελέσματα, ανάλογα με την φύση του προβλήματος. Στην έρευνα αυτή, οι ερευνητές αξιοποίησαν τους fuzzy αλγορίθμους ώστε με την βοήθεια των εξόδων τους, να αξιολογούν μια θέση στάθμευσης "X" ως : **"πολύ δύσκολα προσβάσιμη"**, **"αρκετά δύσκολα προσβάσιμη"**, **"δύσκολα προσβάσιμη"**, **"σχετικά προσβάσιμη"**, **"εύκολα προσβάσιμη"** και **"πολύ εύκολα προσβάσιμη"**. Με την βοήθεια αυτού του μοντέλου, υλοποίησαν έναν **cloud server** ο οποίος είναι και **Trusted Authority** και εκτελεί τους αλγορίθμους και τις ανάλογες λειτουργίες, όπως η εδραίωση ενός ασφαλούς καναλιού επικοινωνίας ανάμεσα σε αυτόν, τους χρήστες και τις IoT Edge Traffic τεχνολογίες (RSUs κ.α). Κατά την λειτουργία της εφαρμογής, η τοποθεσία του χρήστη στέλνεται ανώνυμα στην εφαρμογή. Ο χρήστης επιλέγει την τοποθεσία που επιθυμεί να πραγματοποιηθεί η αναζήτηση της θέσης στάθμευσης και στέλνει το αντίστοιχο query στον cloud server. Στον server εκτελούνται οι προαναφερθείσες διαδικασίες και το αποτέλεσμα επιστρέφει στον χρήστη, προτείνοντας του N θέσεις στάθμευσης, ακολουθούμενες από ένα **tag** από τα 6 που αναφέρθηκαν παραπάνω. Όσον αφορά την προστασία των προσωπικών δεδομένων του χρήστη κατά την χρήση της εφαρμογής, οι ερευνητές, δόμησαν την εφαρμογή πάνω στην λογική της

γλωσσολογίας. Η γλωσσολογική αυτή προσέγγιση, ή όπως την αναφέρουν οι ερευνητές, “**linguistic parking information**”, επί της ουσίας, δεν χρειάζεται κανένα από τα προσωπικά στοιχεία του χρήστη, ακριβώς επειδή βασίζεται στις βασικές αρχές της θεωρίας κατευθύνσεων (από το σημείο “Α” στο σημείο “Β”). Μια τρίτη οντότητα που θα επιδιώξει να παρακολουθήσει την εφαρμογή, θα έρθει αντιμέτωπη με μοντέλα και queries της φύσεως “ από το σημείο Α μετακινήσου στο σημείο Β”. Καμία αληθινή συντεταγμένη δεν γίνεται φανερή , αλλά περνούν από την συνάρτηση “Ρ” και κρυπτογραφούνται. Το αποτέλεσμα της συνάρτησης δεν είναι ακριβές τοποθεσία αλλά ένα εύρος χώρου, μέσα στο οποίο αναφέρονται στη συνέχεια τα 6 tag που αναφέρονται παραπάνω. Η πολύ ενδιαφέρουσα αυτή προσέγγιση προστατεύει τον χρήστη από αποθέσεις όπως είναι η sniffing attack. Τέλος, οι χρήστες αναφέρουν πως η εφαρμογή αναπτύχθηκε με τη βοήθεια του OMNET++ και της γλώσσας JAVA.

6.16 Privacy-Preserving Online Parking Based on Smart Contracts [16]

Η μελέτη αυτή εστιάζει στην εφαρμογή ενός σχεδίου, μέσα από το οποίο μια πόλη θα μπορέσει να υιοθετήσει ένα ασφαλές και λειτουργικό σύστημα έξυπνης στάθμευσης, με την χρήση έξυπνων συμβολαίων. Βασίζεται στις αρχές του μοντέλου “Emerging Cooperative Intelligent Transport Services (C-ITS)”, το οποίο μοντέλο όμως δεν μας ενδιαφέρει επί του πρακτέου, αφού οι ερευνητές το εμπλούτισαν σε ένα νέο μοντέλο που, όπως θα δούμε, κλείνει τα κενά ασφαλείας του C-ITS Αρχικά, το σύστημα προϋποθέτει την εγκατάσταση **On-Board Units (OBUs)** στα αυτοκίνητα, αλλά και μια οντότητα **Back Office (BO)**, που έχει την λειτουργικότητα ενός cloud server και η οποία θα εδραιώσει ένα κανάλι επικοινωνίας ανάμεσα στον οδηγό και τα OBUs. Η χρήση των οντοτήτων αυτών και άλλων προαιρετικών που, όπως θα δούμε παρακάτω, μπορούν να δώσουν επιπρόσθετες πληροφορίες για την διαθεσιμότητα των θέσεων στάθμευσης. Με τη χρήση αυτών, οι ερευνητές ορίζουν σε γενικότερες γραμμές ένα “Internet of Vehicles”, που αντιγράφοντας την ιδεολογία των Internet of Things, προτείνει την χρήση τεχνολογικών μέσων με δικτυακή σύνδεση, στην καταγραφή δεδομένων του δρόμου και κατά συνέπεια, την λύση στο πρόβλημα της αναζήτησης θέσεων στάθμευσης, αλλά και άλλων πολλών προβλημάτων όπως ατυχήματα στην πόλη και έξυπνα φανάρια δρόμων. Επί του πρακτέου, τώρα, στο σύστημα που προτείνουν οι συγγραφείς, χρησιμοποιείται η ψηφιακή υπογραφή αλλά και τεχνολογίες blockchain. Το μοντέλο χρησιμοποιεί μία **Trusted Third Party** οντότητα που λειτουργεί ως TA, έναν **Parking Service Provider**, δηλαδή την εφαρμογή μέσα από την οποία θα αναζητούν μισθωμένες και μη θέσεις στάθμευσης και αντίστοιχα για τον μισθωτή των θέσεων στάθμευσης, μια εφαρμογή “**Parking Lot Terminal**”, απ’ όπου θα μπορεί να μισθώνει χώρους που του ανήκουν, προς στάθμευση από οδηγούς. Επίσης, υπάρχει ο “**Parking Agent**”, μια οντότητα που ελέγχει τα συμβόλαια και τις αποδείξεις ανάμεσα στον οδηγό και τον

μισθωτή. Η TTP ορίζει ένα ασφαλές κανάλι επικοινωνίας ανάμεσα στις εφαρμογές PSP και PLT. Ο χρήστης αρχικά συνδέεται με το TTP. Αυτό το κάνει μέσα από την εφαρμογή, η οποία διαθέτει πιστοποιητικό ασφαλείας **από την κυβέρνηση** και θεωρούμε την μεταφορά των στοιχείων κατά την εγγραφή **ασφαλής**. Για κάθε χρήση εκδίδεται ένα διάνυσμα **ai** το οποίο μπορεί να περιέχει το όνομά του, το φύλο, τον κωδικό του OBU που βρίσκεται στο όχημά του, και άλλες ευαίσθητες πληροφορίες. Εάν η αυθεντικοποίηση είναι επιτυχής, στον χρήστη δίνονται ένα μοναδικό σετ από credentials, δηλαδή όνομα και κωδικός (cred(ai)) τα οποία αποδεικνύουν την μοναδικότητά του στο σύστημα και προστατεύουν τον ίδιο από impersonation attack. Με την ίδια διαδικασία εγγράφεται στο σύστημα και ο μισθωτής. Για να κλειδώσει ένας εγγεγραμμένος οδηγός μια θέση στάθμευσης, συνδέεται αρχικά στον PSP. Όταν θα κάνει την επιλογή του, ένα ψευδώνυμο C στέλνεται στον PLT του μισθωτή, το οποίο C δημιουργείται για κάθε διαφορετικό ψηφιακό συμβόλαιο και χρησιμοποιεί τα cred(ai) του χρήστη, που αποτελούν και proof of possession του. Ουσιαστικά το proof (π) αποτελεί το ιδιωτικό κλειδί της συναλλαγής και χρησιμοποιείται για να υπογράψει το ψηφιακό συμβόλαιο. Η PSP οντότητα εκτελεί validation και αφού επαληθευτεί η μοναδικότητα του χρήστη (του κλειδιού του), επικοινωνεί με το υπεύθυνο PLT για να βρει διαθέσιμες θέσεις στάθμευσης στην τοποθεσία που επέλεξε ο χρήστης. Αφού γίνει η επιστροφή των αποτελεσμάτων και η επιλογή του χρήστη, ξεκινά η διαδικασία της πληρωμής. Η απόδειξη της πληρωμής αποθηκεύεται μαζί με το συμβόλαιο που πλέον είναι συμπληρωμένο, στο Blockchain. Το συμβόλαιο στη συνέχεια επιστρέφεται στην εφαρμογή του χρήστη κρυπτογραφημένο και υπογεγραμμένο με τη χρήση του αλγορίθμου **blind signature** αλγορίθμου. Ο χρήστης δεν μπορεί να δει το συμβόλαιο του, όμως γνωρίζουμε πως αποτελείται από το C ψευδώνυμο του, ένα **salt** που είναι μια συμβολοσειρά που θα πολώσει το ψευδώνυμο του χρήστη για πλήρη ακεραιότητα των προσωπικών του δεδομένων, το πιστοποιητικό γνησιότητας του συμβολαίου υπογεγραμμένο από την κρατική αρχή που διαχειρίζεται τον TTP, ένα timestamp και τον τόπο που θα ισχύει το συμβόλαιο, κρυπτογραφημένο ξανά με blind signature. Ο χρήστης πληρώνει ψηφιακά το πάρκινγκ του αποστέλλοντας το συμβόλαιο στον PLT και το ποσό σε έναν μοναδικό κωδικό πληρωμής, στο blockchain (σε Ethereum συνάλλαγμα). Ξανά, με τη χρήση του blockchain, λαμβάνει μια απόδειξη πληρωμής και προχωρά με την διαδικασία της στάθμευσης. Εάν επιθυμεί να αυξήσει τον χρόνο στάθμευσης, η διαδικασία επαναλαμβάνεται στο back end δημιουργώντας νέα συμβόλαια και λαμβάνοντας νέες αποδείξεις πληρωμής. Στην έρευνα αυτή είδαμε την κρυπτογραφία με την τεχνική blind signature αλλά και συναντήσαμε ένα νέο blockchain βασισμένο μοντέλο το οποίο εστιάζει στην διατήρηση της ιδιωτικότητας των δεδομένων του χρήστη αλλά και στην ακεραιότητά τους κατά τη διάρκεια της εγγραφής του στο σύστημα, με τη χρήση κρατικών παραγόντων ασφαλείας. Είδαμε επίσης έναν ασφαλές τρόπο πληρωμής με τη χρήση κρυπτονομισμάτων όπως το Ethereum, που αξιοποιούν πλήρως την τεχνολογία blockchain σε μια προσέγγιση ασφαλών και εύκολων πληρωμών υπηρεσιών στο διαδίκτυο. Το Internet of Vehicles που προτείνεται στην έρευνα αυτή, εάν αξιοποιήσει με έξυπνο τρόπο τις παρούσες αλλά και καινοτόμες τεχνολογίες, θα μπορέσει να δημιουργήσει ένα καθολικό μοντέλο έξυπνων πόλεων όπου θα μειωθούν τα ατυχήματα και οι οδηγοί θα είναι ικανοί να βρίσκουν θέσεις στάθμευσης και να τις δεσμεύουν μακροπρόθεσμα γλυτώνοντας καύσιμο και περιττή κούραση στην διαδικασία αναζήτησης πάρκινγκ.

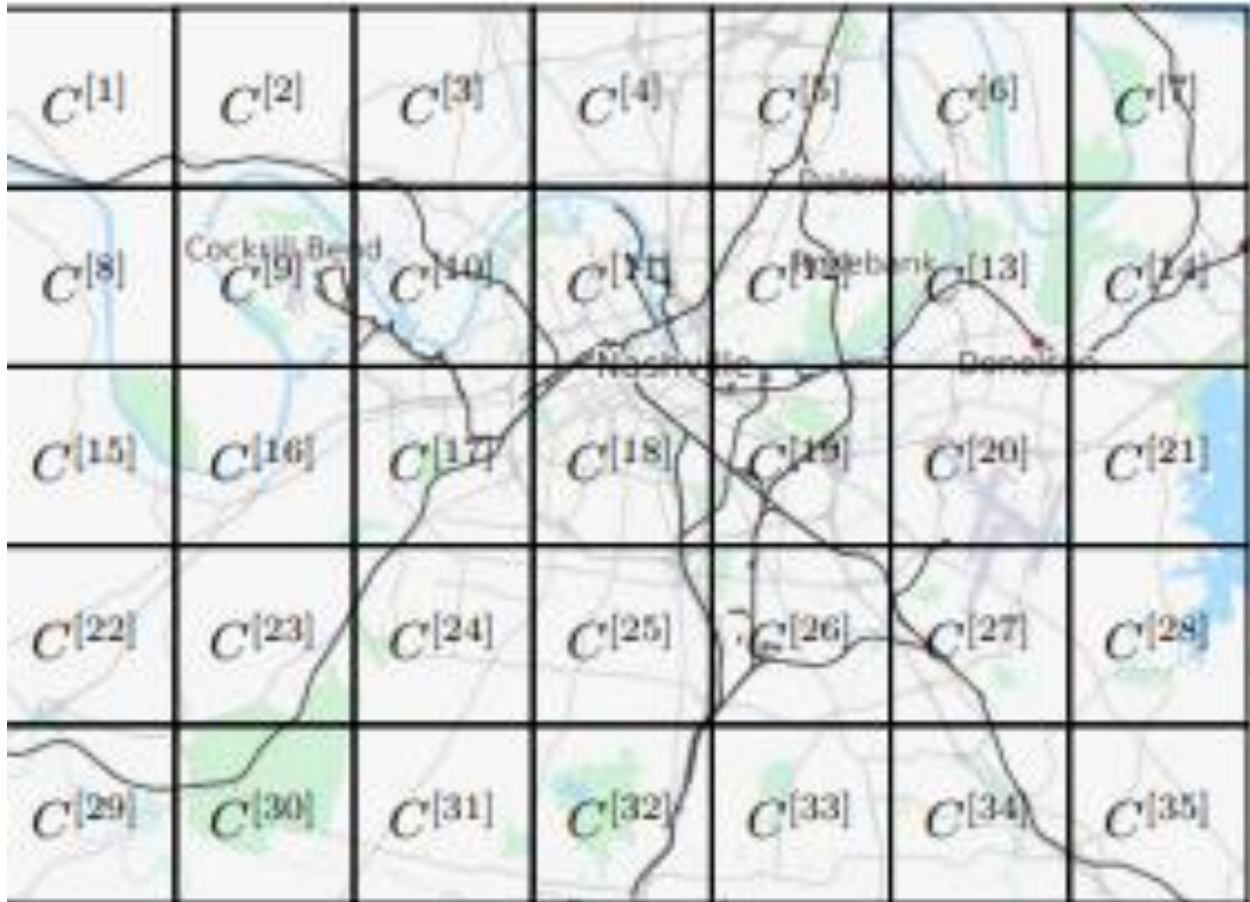
6.17 Privacy-Preserving Smart Parking Navigation Supporting Efficient Driving Guidance Retrieval [17]

Στην μελέτη αυτή, οι ερευνητές δημιούργησαν μια έξυπνη μέθοδο μέσα από την οποία οι οδηγοί μιας έξυπνης πόλης θα μπορούν εύκολα και με ασφάλεια να κατευθυνθούν σε μια θέση στάθμευσης. Για να λειτουργήσει το σχέδιο των ερευνητών, είναι απαραίτητη η παρουσία των παρακάτω οντοτήτων. Αρχικά, τα αυτοκίνητα θα πρέπει να είναι εξοπλισμένα με **On-Board Units (OBUs)**. Οι χρήστες θα πρέπει να έχουν εγκατεστημένη την αντίστοιχη εφαρμογή που θα λειτουργεί ως recommender θέσεων στάθμευσης. Στην άκρη του δρόμου όπου υπάρχουν θέσεις στάθμευσης, θα πρέπει να υπάρχουν **Road-Side Units (RSUs)**, τα οποία θα ανιχνεύουν την διαθεσιμότητα των θέσεων στάθμευσης της περιοχής την οποία καλύπτουν. Επίσης, οι παραπάνω οντότητες θα επικοινωνούν με έναν **cloud server** ο οποίος θα ανταλλάσσει τις πληροφορίες ανάμεσα στις οντότητες. Μια **Trusted Authority** θα υπογράφει τα πιστοποιητικά και θα αναθέτει μοναδικά ID στα RSU και OBU που θα εγγράφονται στο σύστημα. Τα δεδομένα των χρηστών αποθηκεύονται στον cloud server κρυπτογραφημένα με τη βοήθεια του αλγορίθμου **bloom filter** ο οποίος διαστρεβλώνει τα δεδομένα ώστε να τα καταστήσει κρυπτογραφημένα αποτρέποντας επιθέσεις τύπου impersonation attack και διατηρώντας την ιδιωτικότητα του χρήστη της εφαρμογής. Οι OBU κόμβοι είναι συνδεδεμένοι μεταξύ τους σχηματίζοντας ένα δίκτυο που αποκαλείται ευρέως “Vehicular ad hoc network” ή **VANET**. Το κάθε όχημα, μέσα στο καλά προστατευόμενο αυτό δίκτυο, επικοινωνεί με τα κοντινά του RSU και στη συνέχεια με τον cloud server, διαδικασία που έχει σαν αποτέλεσμα να γνωρίζει ο server και κατά συνέπεια ο οδηγός που θα αναζητήσει θέση στάθμευσης, την διαθεσιμότητα ή μη των θέσεων στάθμευσης στην περιοχή του χάρτη που θα επιλέξει να πραγματοποιηθεί η αναζήτηση. Κατά την εγγραφή των συσκευών στον cloud server, η Trusted Authority παράγει ένα σετ τυχαίων κλειδιών και τα υπογράφει χρησιμοποιώντας τον αλγόριθμο **Pointcheval and Sanders Signature**. Στη συνέχεια, κατά την εγγραφή του οδηγού, χρησιμοποιείται το ψηφιακό δίπλωμα οδήγησης του το οποίο η TA υπογράφει χρησιμοποιώντας το **Zero Knowledge Proof of Knowledge Protocol**. Ο οδηγός παίρνει στη συνέχεια υπό την κατοχή του ένα σετ κλειδιών υπογεγραμμένο από την TA. Για την αναζήτηση θέσης στάθμευσης, ο οδηγός στέλνει στον cloud server ένα query κρυπτογραφημένο με τον αλγόριθμο του Diffie Hellman. Ο server αποκρυπτογραφεί το μήνυμα χρησιμοποιώντας το master key που έχει λάβει από την TA και επικοινωνεί με το κοντινότερο RSU. Το RSU επιστρέφει ένα δικό του query κρυπτογραφημένο με τον αλγόριθμο AES το οποίο περιέχει τις διαθέσιμες θέσεις. Τέλος ο οδηγός προχωρά στην πληρωμή της θέσης στάθμευσης εάν εκείνη είναι μισθωμένη, στέλνοντας τα προσωπικά του στοιχεία στην “τρίτη” εφαρμογή πληρωμών, διαστρεβλωμένα με τη χρήση του **bloom filter**

algorithm, ο οποίος εκτελείται offline στην συσκευή του χρήστη για μέγιστη ασφάλεια. Το σύστημα που προτείνουν οι ερευνητές είναι σχεδιασμένο ώστε να χρησιμοποιεί τις τεχνολογίες που μπορούν να προσφέρουν οι έξυπνες πόλεις με τον σκοπό να λύσει το χρόνιο πρόβλημα των οδηγών με έναν ασφαλές και σεβόμενο προς την ιδιωτικότητά τους τρόπο.

6.18 Privacy-Preserving Smart Parking System Using Blockchain and Private Information Retrieval [18]

Στην μελέτη αυτή, οι ερευνητές προτείνουν μια μέθοδο έξυπνου πάρκινγκ που ξεφεύγει από τα συνηθισμένα κεντροποιημένα συστήματα και προσφεύγει στην τεχνολογία blockchain. Η έρευνα βασίζεται στην ανορθόδοξη προσέγγιση η οποία συλλέγει ζωντανά δεδομένα από τον δρόμο με την χρήση fog nodes που όμως επικοινωνούν με τον server μέσα από το blockchain (**blockchain nodes**), μετατρέποντας το σε ένα ασφαλές κανάλι επικοινωνίας. Η τεχνολογία blockchain που χρησιμοποιείται στην έρευνα δεν είναι το καθολικό blockchain που όλοι γνωρίζουμε, αλλά ένα μικρότερο σε αριθμό κόμβων blockchain το οποίο δημιουργείται από το πλήθος των ιδιοκτητών των πάρκινγκ και ονομάζεται **Consortium Blockchain Network**. Οι οντότητες που αναφέρονται είναι οι παρακάτω. Ένα **Key Distribution Center (KDC)** που είναι υπεύθυνο για την δημιουργία και την διανομή κλειδιών ανάμεσα στις οντότητες του συστήματος. **Parking Lot Owners (POs)** που αποτελούν τους ιδιοκτήτες των πάρκινγκ αλλά και το σύνολο των Internet of Things συσκευών που διατίθενται σε κάθε χώρο πάρκινγκ. Αρχικά, το KDC δημιουργεί πιστοποιητικά για τους Parking Owners και ιδιωτικά κλειδιά για τους οδηγούς. Οι ιδιοκτήτες πάρκινγκ, περιοδικά, ενημερώνουν το blockchain με την διαθεσιμότητα των θέσεων στάθμευσης στους χώρους πάρκινγκ τους. Η συνολική έκταση που καλύπτει το σχέδιο χωρίζεται σε N γεωγραφικές τοποθεσίες. Για λόγους κατανόησης, θα ακολουθήσει η εικόνα που χρησιμοποιούν οι ερευνητές στην μελέτη τους.



Παράδειγμα κατανομής του χώρου για την εργασία [18]

Όπως βλέπουμε, στο παράδειγμα, στο οποίο απεικονίζεται το Nashville των Η.Π.Α., το σχέδιο προϋποθέτει την κατανομή αυτή, ώστε να μην δίνεται σαφές τοποθεσία PO στο διαδίκτυο, μεγιστοποιώντας την ανωνυμότητα και την ιδιωτικότητα των οντοτήτων της εφαρμογής. Όταν ο οδηγός θέλει να μισθώσει κάποια θέση στάθμευσης, στέλνει μέσω της εφαρμογής που πρέπει να διαθέτει, το query με την γεωγραφική τοποθεσία που αναγράφεται παραπάνω. Μέσω του blockchain, το query πηγαίνει κατευθείαν στην περιοχή και προσπαθεί να κάνει match με τα υπάρχοντα κριτήρια, δηλαδή με την παρούσα διαθεσιμότητα των θέσεων στάθμευσης των πάρκινγκ που βρίσκονται σε εκείνη την περιοχή. Αφότου βρεθεί το best match, η διαδικασία μεταβαίνει στην φάση πληρωμής, στην οποία ο PO στέλνει τον μοναδικό κωδικό πληρωμής μέσω του blockchain, με τον οδηγό να καλείται να πληρώσει σε κρυπτονομίσματα. Η μέθοδος αυτή δεν απαιτεί την διάδοση των προσωπικών στοιχείων του οδηγού αλλά και του ιδιοκτήτη των πάρκινγκ, διασφαλίζοντας την ιδιωτικότητα των οντοτήτων, την ανωνυμότητα τους αλλά και την ακριβήτητα των προσωπικών τους στοιχείων. Κατά την εγγραφή των οδηγών στο σύστημα, το KDC αναθέτει IDι στους οδηγούς και η ταυτοποίηση γίνεται με το **Zero Knowledge Proof of Knowledge Protocol**. Για την δημιουργία των ιδιωτικών κλειδιών, επιλέγεται ένας τυχαίος

ακέραιος αριθμός a_i , ένας για κάθε οντότητα. Η δημιουργία των κλειδιών γίνεται με τη χρήση του **random selection** αλγόριθμου.

6.19 PSSBP: A Privacy-preserving Scope-query Searchable Encryption Scheme Based on Blockchain for Parking Lots Sharing in Vehicular Networks [19]

Στην μελέτη αυτή, οι ερευνητές υλοποίησαν ένα σύστημα το οποίο βοηθά στην εύρεση πάρκινγκ με έναν δίκαιο και ασφαλές τρόπο, ξεφεύγοντας από την μέχρι τώρα αντιμετώπιση του προβλήματος από τον μέσο εργαζόμενο μιας υπεραστικής κοινωνίας. Οι εργαζόμενοι στις μέρες μας αναγκάζονται να μισθώνουν χρόνια θέσεις πάρκινγκ σε ιδιωτικά πάρκινγκ, κοντά στον τόπο εργασίας τους ώστε να γλυτώνουν από την περιαγωγή και την αναζήτηση σε καθημερινό υπόβαθρο. Οι ερευνητές προτείνουν μια λύση στο πρόβλημα αυτό, με την χρήση **scope-queries** ψηφιακών συμβολαίων, που θα βασίζονται σε κρυπτογραφημένα στοιχεία των οντοτήτων σε συνδυασμό με vehicular networks. Για την διασφάλιση της ιδιωτικότητας των στοιχείων των χρηστών, συναντούμε την χρήση του **Cuckoo filter** αλλά και του Pedersen commitment που έχουμε δει και σε παραπάνω έρευνες. Στο σύστημα χρησιμοποιείται επίσης **Dynamic Group Signature** για την αποτελεσματική υπογραφή ψηφιακών πιστοποιητικών εγκυρότητας των χρηστών, μέθοδος που ενισχύει την ασφάλεια και συντελεί στην διατήρηση της ανωνυμότητας των χρηστών σεβόμενη της ιδιωτικότητας των στοιχείων τους. Το σύστημα προϋποθέτει επίσης την χρήση **Road-Side Units**, αλλά και μιας **Trusted Authority** που θα υπογράφει και θα εκδίδει με ασφάλεια πιστοποιητικά και κλειδιά για τις οντότητες του συστήματος. Σε πρώτο στάδιο, για την εγγραφή των RSU στο σύστημα, η TA εκδίδει έναν τυχαίο αριθμό r . Ο αριθμός αυτός χρησιμοποιείται στον **Dynamic Group Signature** με την χρήση του οποίου η TA εκδίδει ένα σετ κλειδιών για κάθε μονάδα RSU. Στη συνέχεια εκδίδει ένα δημόσιο κλειδί για κάθε γκρουπ ιδιοκτητών πάρκινγκ, και ένα ιδιωτικό κλειδί για κάθε ιδιοκτήτη πάρκινγκ ξεχωριστά και τα υπογράφει με το ιδιωτικό της κλειδί. Η ίδια διαδικασία γίνεται και για τους οδηγούς. Στην εφαρμογή που θα κατέχουν οι οδηγοί και οι ιδιοκτήτες πάρκινγκ, τα μοναδικά σετ κλειδιών τους τους αποστέλλονται μέσω του ασφαλές καναλιού επικοινωνίας blockchain και στη συνέχεια δημιουργείται τοπικά για τον καθένα μια μοναδική τους διεύθυνση στο blockchain. Περιοδικά, ο ιδιοκτήτης στέλνει ένα query στο blockchain που δείχνει την διαθεσιμότητα των θέσεων στάθμευσης. Το ίδιο και το RSU το οποίο διαθέτει δικτυακή σύνδεση. Η ανταλλαγή πληροφοριών γίνεται με τη χρήση του blockchain. Η τοποθεσία του οδηγού αλλά και των ιδιοκτητών που θέλουν να δημοσιεύσουν τους χώρους στάθμευσής τους, μετατρέπεται σε συντεταγμένες ($Local\ x$, $Local\ y$) οι οποίες κρυπτογραφούνται τοπικά με την χρήση του Cuckoo filter, διαδικασία που πραγματοποιείται στις εφαρμογές τους. Αντίστοιχα, το query που θα στείλει ο οδηγός που επιθυμεί να βρεί θέση πάρκινγκ, θα είναι κρυπτογραφημένο πριν

οδηγηθεί στο blockchain. Η επαλήθευση του αιτήματος του ψηφιακού συμβολαίου γίνεται από την TA η οποία αποκρυπτογραφεί τις τοπικά δημιουργημένες τιμές. Για τον χρόνο διάρκειας της θέσης στάθμευσης, χρησιμοποιείται το Pedersen commitment στο οποίο υπολογίζεται το αποκρυπτογραφημένο timestamp του συμβολαίου του οδηγού και αφαιρείται από το επίσης αποκρυπτογραφημένο timestamp διαθεσιμότητας που όρισε ο ίδιος ο χρήστης και υπέγραψε στη συνέχεια ψηφιακά ο ιδιοκτήτης της θέσης στάθμευσης. Τέλος, η τιμή υπολογίζεται συναρτήσει του χρόνου στάθμευσης και η πληρωμή γίνεται με τη βοήθεια του μοναδικού κωδικού blockchain που έχει εκδοθεί αρχικά από την TA για τους ιδιοκτήτες χώρων στάθμευσης. Σε περίπτωση υπαίθριας θέσης στάθμευσης που όμως είναι μισθωμένη, η TA εκδίδει και υπογράφει με τη βοήθεια του Dynamic Group Signature, N σετ κλειδιών αντίστοιχα με τον αριθμό των RSU αλλά M πιστοποιητικά με τη μορφή διανύσματος για κάθε χώρο στάθμευσης που εμπεριέχεται στην εμβέλεια του εκάστοτε RSU. Στην μελέτη αυτή, παρατηρήσαμε έναν πολύπλοκο συνδυασμό τεχνικών κρυπτογράφησης και προσθήκης θορύβου, που στοχεύουν στον ομαλό συνδυασμό της εύρεσης στάθμευσης σε ιδιωτικούς και κοινόχρηστους χώρους. Το σχέδιο αυτό είναι αποκεντριοποιημένο και υλοποιείται με τη βοήθεια ψηφιακών συμβολαίων, γεγονός που προσδίδει ασφάλεια και σέβεται την ακεραιότητα των δεδομένων των χρηστών, την ιδιωτικότητα τους αλλά και διατηρεί την ανωνυμότητα των στοιχείων τους όπως η τοποθεσία τους αφού αξιοποιεί την τεχνολογία blockchain και την δημιουργία προσωπικών διευθύνσεων αποστολής και παραλαβής δεδομένων.

6.20 SecSPS: A Secure and Privacy-Preserving Framework for Smart Parking Systems [20]

Στην έρευνα αυτή, οι ερευνητές δημιούργησαν μια μέθοδο έξυπνης εύρεσης θέσης πάρκινγκ, η οποία αξιοποιεί πλήρως τεχνολογίες Internet of Things με ασφαλή τρόπο που χρησιμοποιεί το μοντέλο της αμοιβαίας χειραψίας (mutual authentication mechanism), με σκοπό να πραγματοποιηθεί η εν λόγω διαδικασία με τη μέγιστη ασφάλεια. Στο σχέδιο αυτό, χρησιμοποιούνται **Parking Guidance Information systems (PGI)**, τα οποία είναι συσκευές συνδεδεμένες στο διαδίκτυο και πάντα σε transmission mode, με μοναδικό σκοπό να ενημερώνουν ανά πάσα στιγμή για την διαθεσιμότητα κοινόχρηστων θέσεων στάθμευσης, παρόμοια με RSU. Το μοντέλο αυτό επιτρέπει επίσης στους χρήστες να προπληρώσουν μια θέση στάθμευσης με σκοπό να πραγματοποιηθεί η κράτηση της για ένα επιλεγμένο χρονικό διάστημα. Η αρχιτεκτονική που χρησιμοποιείται στο σχέδιο είναι η “publish/subscribe” κατά την οποία μπορούν ασύγχρονα πολλές συσκευές IoT να επικοινωνήσουν μεταξύ τους. Στην περίπτωσή μας, οι publishers αποτελούν τις υπηρεσίες στάθμευσης, ιδιωτικές ή δημόσιες, ενώ οι subscribers είναι οι οδηγοί που ενδιαφέρονται για το θέμα, ακριβώς επειδή ενδιαφέρονται να μισθώσουν μια θέση στάθμευσης. Οι publishers και οι subscribers έχουν αντίστοιχες

εφαρμογές στα έξυπνα τηλέφωνα τους. Για την εδραίωση ενός ασφαλούς καναλιού επικοινωνίας ανάμεσά τους, χρησιμοποιείται το Ίντερνετ, με την βοήθεια του πρωτοκόλλου **TLS**. Το TLS επιλέχθηκε επειδή η σύνδεση ανάμεσα στους publishers και στους subscribers γίνεται μόνο μια φορά, γεγονός που μειώνει σημαντικά το κόστος σε ενέργεια και δύναμη των IoT τεχνολογιών που θα συντελέσουν το επιθυμητό αποτέλεσμα. Στο σχήμα αυτό, υπάρχουν οι παρακάτω οντότητες. Αρχικά, οι θέσεις στάθμευσης, θα πρέπει να είναι εξοπλισμένες με **sensor nodes**, τα οποία θα ελέγχουν την διαθεσιμότητά τους. Μια **smart gateway** θα επιτρέπει την σύνδεση των publishers/subscribers και θα λειτουργεί στον **cloud server ή broker**. Το κάθε αυτοκίνητο που επιθυμεί να σταθμεύσει, θα στέλνει μια χειραψία μέσω της εφαρμογής στο κοντινότερο **sensor node**, η οποία θα αναμεταδίδεται στη συνέχεια με τον publisher της θέσης στάθμευσης. Το TLS πρωτόκολλο, που θα υλοποιηθεί μέσα στον broker θα εδραιώσει την ασφαλή σύνδεση και στη συνέχεια θα γίνει η ανταλλαγή των στοιχείων publishers/subscribers. Η διαδικασία αυτή, από και προς τον broker γίνεται κρυπτογραφημένα αφού οι publishers/subscribers στέλνουν ένα συγκεκριμένο Handshake που μόνο ο broker μπορεί να αποκρυπτογραφήσει. Όταν ο publisher κάνει publish το query των ελεύθερων θέσεων στάθμευσης, θα εκτελέσει την ίδια διαδικασία αντίστροφα, ώστε να εδραιωθεί πρώτα το κανάλι επικοινωνίας με τον broker, στη συνέχεια με τον subscriber ο οποίος θα λάβει το μήνυμα κρυπτογραφημένο από τον broker πλέον, με την λίστα των διαθέσιμων θέσεων στάθμευσης. Εκτός από την TLS handshake, ο client (publisher και subscriber) θα χρειαστεί να αξιολογήσει την εγκυρότητα του broker, εάν δηλαδή συνομιλεί με τον broker ή όχι. Αυτό επιτυγχάνεται με τη χρήση του **X.509 certificate**, το οποίο πιστοποιητικό στέλνει σαν response ο broker στην εφαρμογή του client. Τέλος, ο χρήστης δεσμεύει μια θέση στάθμευσης αφότου εδραιωθεί με ασφάλεια η επικοινωνία publisher/subscriber, στέλνοντας στον publisher ένα t1/reservation που δεσμεύει μία θέση για χρονικό διάστημα t1, τόσο όσο επιλέξει ο χρήστης. Για την πληρωμή της θέσης, θα χρησιμοποιηθούν τρίτες εφαρμογές από μοναδικά κλειδιά που θα εκδόσει ο broker στους publishers/subscribers. Έτσι, παρατηρούμε μια μέθοδο η οποία καθολικά, σέβεται την ανωνυμότητα των οντοτήτων της, την ιδιωτικότητα των στοιχείων τους και προστατεύει, όπως ερευνάται, από επιθέσεις τύπου **man-in-the-middle attack, phishing attack, replay attack, broker hijack** και **shoulder-surfing attack**.

6.21 Secure and Reliable Parking Protocol Based on Blockchain for VANETs [21]

Στην έρευνα αυτή, οι μελετητές επιχείρησαν να λύσουν ένα πρόβλημα που παρατηρείται σε πολλές εφαρμογές έξυπνου πάρκινγκ, στις οποίες μπορεί ένα άτομο να μισθώσει πολλαπλές θέσεις στάθμευσης (**multi-reservation attack**). Προτείνουν λοιπόν, μια μέθοδο υλοποίησης μιας εφαρμογής έξυπνου πάρκινγκ, η οποία λύνει το πρόβλημα αυτό, με την βοήθεια **Vehicular ac-**

hoc Networks (VANETs), αλλά και της τεχνολογίας blockchain, μέσω των οποίων ορίζουν ένα πρωτόκολλο **συνδεδεμένων ομαδικών υπογραφών (linked group signatures)**. Για την υλοποίηση του μοντέλου αυτού, απαιτούνται υποδομές μιας έξυπνης πόλης, δηλαδή μια **Trusted Authority**, που θα εκδίδει πιστοποιητικά για τις οντότητες του μοντέλου, **OBUs και RSUs** που θα εκτελούν τις διαδικασίες που είδαμε στο κεφάλαιο της γενικής αρχιτεκτονικής. Επίσης, χρησιμοποιείται ένας **Global Server** ο οποίος διαθέτει τον ρόλο του **cloud server** και είναι υπεύθυνος για τις κρατήσεις των θέσεων στάθμευσης που θα πραγματοποιούν οι οδηγοί από την εφαρμογή στα έξυπνα τηλέφωνα τους. Επίσης ο GS είναι υπεύθυνος για την ζωντανή παρακολούθηση και συλλογή συχνά ανανεώσιμων δεδομένων όπως η διαθεσιμότητα θέσεων, τεχνική που επιτυγχάνεται με την δημιουργία τοπικών βάσεων δεδομένων για κάθε ιδιωτικό χώρο στάθμευσης. Τέλος, χρησιμοποιείται ένας **Local Server (LS)**, μοναδικός για κάθε ιδιωτικό χώρο πάρκινγκ του οποίου ο ρόλος είναι η διαχείριση τοπικά των θέσεων στάθμευσης, η δρομολόγησή τους σε περιπτώσεις κρατήσεων αλλά και η ενημέρωση της τοπικής βάσης δεδομένων που βρίσκεται στον GS. Όλες οι οντότητες του συστήματος συνδέονται με την TA και παίρνουν μοναδικά σετ κλειδιών υπογεγραμμένα από αυτή, αλλά και ένα μοναδικό IDi για εκείνα. Το ID τους χρησιμοποιείται για την περιαγωγή των δεδομένων στο blockchain παίρνοντας τον ρόλο της διεύθυνσης. Να σημειωθεί επίσης πως το σύστημα blockchain είναι τοπικό και δεν αναφέρεται στο καθολικό blockchain που εκμεταλλεύονται μεγάλες τεχνολογίες όπως το Ethereum. Χωρίζεται σε 2 μέρη, το sub-chain που είναι υπεύθυνο για την καταγραφή των δεδομένων των ιδιωτικών χώρων στάθμευσης, και το main-chain μέσα από το οποίο μετακινούνται σε ένα ευρύτερο φάσμα (πχ από και πριν τον GS) οι πληροφορίες των sub-chains. Η εγγραφή των οντοτήτων στον GS γίνεται σε γκρούπ των οποίων τα μέλη ανατίθεται ένα ζευγάρι κλειδιών. Κάθε γκρούπ κλειδιών κρυπτογραφείται με έναν αλγόριθμο συμμετρικής κρυπτογράφησης όπως ο AES για επιπλέον ασφάλεια. Το hash των κλειδιών του κάθε γκρούπ αποθηκεύεται στον GS και χρησιμοποιείται σε συνδιασμό με τα δημόσια κλειδιά της κάθε οντότητας για λόγους διπλής επαλήθευσης. Ο οδηγός που επιθυμεί να χρησιμοποιήσει την εφαρμογή, συνδέεται με τους κωδικούς που του ανατέθηκαν στην εγγραφή. Για να πραγματοποιήσει μια κράτηση θέσης, στέλνει ένα κρυπτογραφημένο με το δημόσιο κλειδί του request στον GS, μέσω του main-chain. Ο GS, αφού επαληθεύσει την εγκυρότητα του κλειδιού, ελέγχει τις τοπικές βάσεις δεδομένων των LS που αντιστοιχούν στο αίτημα του οδηγού. Του επιστρέφει την διαθεσιμότητα των N κοντινών πάρκινγκ και ο χρήστης το χρησιμοποιεί για να πληρώσει το ποσό της μίσθωσης στον μοναδικό κωδικό του main-blockchain που αντιστοιχεί στο εκάστοτε πάρκινγκ (η address του local server του πάρκινγκ συνδέεται με το blockchain). Επομένως, με την χρήση ασφαλών τεχνικών κράτησης και πληρωμής, ο χρήστης μπορεί να πραγματοποιήσει μια κράτηση και να πληρώσει χωρίς να αποκαλυφτούν τα προσωπικά του δεδομένα στο διαδίκτυο. Με τη χρήση του μοντέλου αυτού, η τοποθεσία του χρήστη περνά στον GS με την ασφαλή χρήση του δικτύου των OBU-RSU που όπως έχουμε δει, συνδέονται σε ένα αποκεντροποιημένο σύστημα blockchain όπου όλη η πληροφορία μεταδίδεται από και προς διευθύνσεων, καλύπτοντας τα προσωπικά στοιχεία του οδηγού αλλά και του ιδιοκτήτη χώρων στάθμευσης, σεβόμενοι της ιδιωτικότητας των φυσικών οντοτήτων.

6.22 Secure Automated Valet Parking: A Privacy-Preserving Reservation Scheme for Autonomous Vehicles [22]

Η μελέτη αυτή αφορά μια έξυπνη πόλη, όπου τα οχήματα της θα διαθέτουν τεχνολογίες αυτόματου πιλότου, στην προσπάθεια να δημιουργηθεί το σύστημα του “αυτόματου παρκαδόρου” (**automated valet**). Ο παρκαδόρος θα είναι ένα λογισμικό, το οποίο θα συνεργάζεται με τις τεχνολογίες IoT της έξυπνης πόλης. Ο οδηγός θα αφήνει το αυτοκίνητό του σε μια τοποθεσία της αρεσκείας του και το αυτοκίνητο, θα μεταβαίνει μόνο του σε μια θέση στάθμευσης την οποία ο οδηγός έχει μισθώσει προηγουμένως. Μια τέτοια πρωτοπόρα ιδέα όμως έχει κάποια πολύ σοβαρά κενά ασφαλείας όπως η “double-reservation attack”, στην οποία μπορεί ένας οδηγός να μισθώσει περισσότερες από μια θέσεις στάθμευσης, στερώντας τες έτσι από άλλους οδηγούς. Οι ερευνητές, με τη χρήση των **Zero Knowledge Proof of Knowledge** πρωτοκόλλων αλλά και με την τεχνική **proxy signature**, παρουσιάζουν μια λύση σε αυτό το τόσο συγκεκριμένο πρόβλημα. Οι οντότητες που θα πρέπει να είναι παρούσες στο σύστημα, είναι οι εξής. Αρχικά, ένα **Autonomous Vehicle (AV)**, το οποίο θα μπορεί με την βοήθεια αισθητήρων να περιηγηθεί μόνο του, να παρκάρει και να διαθέτει κάποιο είδος cellular network. Επίσης, ο **Parking Service Provider (PSP)** αποτελεί ένα σύνολο υπηρεσιών όπως η εύρεση θέσεων στάθμευσης, η κράτηση τους και άλλες υπηρεσίες. Θα παρέχεται από μια εταιρία που θα συνεργάζεται με την αυτοκινητοβιομηχανία του AV και θα παρέχει επίσης αντίστοιχη εφαρμογή στο έξυπνο κινητό του οδηγού. Επίσης, ένα **Parking Lot Terminal (PLT)**, που αποτελεί το τμήμα διαχείρισης του ιδιοκτήτη του χώρου στάθμευσης και το σύνολο των συσκευών IoT (κάμερες, αισθητήρες κ.λπ) που θα μπορούν να δώσουν μια καθαρή εικόνα για την τρέχουσα διαθεσιμότητα των θέσεων στάθμευσης στον χώρο. Σε πρώτη επαφή, το κάθε PLT συνδέεται στο PSP. Ο PSP δημιουργεί **bilinear maps** και χρησιμοποιεί 3 hash functions, σε συνδυασμό με το δημόσιο του κλειδί και έναν τυχαίο αριθμό α , ώστε να δημιουργήσει 3 παραμέτρους ασφαλείας, μέσα από τις οποίες δημιουργεί ένα master private key. Στη συνέχεια δημιουργεί ένα σετ ανώνυμων κλειδιών για τον κάθε εγγεγραμμένο χρήστη που όμως διαρκούν μια μέρα και θα ανανεώνονται κάθε μέρα αυτόματα. Οι PLT που θέλουν να συνδεθούν στο PSP δημιουργούν ένα σετ από στοιχεία (όνομα, κωδικός) και τα στέλνουν στον PSP. Στη συνέχεια ο PSP με αυτοματοποιημένο τρόπο, εκτελεί ελέγχους IoT για να αξιολογήσει τον χώρο στάθμευσης. Εάν ο χώρος είναι πλήρως εξοπλισμένος, ο PSP υπογράφει τα credentials που όρισε ο PLT και αποθηκεύει το hash τους στην βάση δεδομένων του. Με παρόμοιο τρόπο δημιουργεί και ο οδηγός έναν προσωπικό του λογαριασμό. Η υπηρεσία θα απαιτεί μια συνδρομή που ο χρήστης θα πληρώνει με τη βοήθεια τρίτων παραγόντων (π.χ. Apple Pay). Όταν ο χρήστης θέλει να μισθώσει μια θέση στάθμευσης, στέλνει ένα query με τα στοιχεία εγγραφής

του **ανώνυμα** ως προς τα αληθινά στοιχεία του, στον PSP. Ο PSP επαληθεύει τον οδηγό με τη χρήση του Zero Knowledge Proof of Knowledge Protocol. Αν η επαλήθευση γίνει με επιτυχία, αξιολογεί το query του και του επιστρέφει ανάλογα αποτελέσματα. Εάν η διαδικασία πετύχει, ο χρήστης μεταβαίνει με το AV του στον ανάλογο τόπο την υποσχόμενη χρονική περίοδο και το όχημά του μεταβαίνει με μια μέγιστη ταχύτητα των 30km/h στον χώρο στάθμευσης. Μια ορισμένη χρονική περίοδο πριν τη λήξη της μίσθωσης της θέσης, στο έξυπνο τηλέφωνο του χρήστη έρχεται μια ειδοποίηση στην οποία ο χρήστης πρέπει να ανταποκριθεί. Εάν ανταποκριθεί, το αυτοκίνητό του θα επιστρέψει σε αυτόν. Εάν όχι, το αυτοκίνητό θα μετακινηθεί σε κάποια δημόσια αρχή, αφού για να λειτουργήσει ένα τέτοιο μοντέλο, το κράτος θα πρέπει να έχει άμεση σχέση για την διασφάλιση της τήρησης των ψηφιακών συμβολαίων. Ο χρήστης βέβαια μπορεί εάν η θέση δεν είναι κρατημένη, να ανανεώσει την διαδικασία αυτή και το αυτοκίνητο του να μείνει στην θέση για μεγαλύτερο χρονικό διάστημα. Στην πολύ ενδιαφέρουσα αυτή έρευνα, είδαμε έναν αποτελεσματικό τρόπο με τον οποίον οι οδηγοί των AV θα μπορούν να αξιοποιήσουν στο έπακρο τις ιδιότητες των οχημάτων τους, αποφεύγοντας καθολικά την διαδικασία της στάθμευσης, με έναν ασφαλές και σεβόμενο προς την ιδιωτικότητα τους τρόπο.

6.23 Sharing Economy: Implementing Decentralized Privacy-Preserving Parking System [23]

Στην μελέτη αυτή, οι ερευνητές προτείνουν μια μέθοδο έξυπνης μίσθωσης θέσεων στάθμευσης, με την χρήση της τεχνολογίας blockchain. Η μέθοδος τους υπόσχεται να διατηρήσει την ανωνυμία των οδηγών, χρησιμοποιώντας το πρωτόκολλο **Zero Knowledge Proof of Knowledge**, αλλά και τεχνικές **differential privacy**. Στη συνέχεια, για να επιβεβαιώσουν την αποτελεσματικότητα του μοντέλου τους, το εφαρμόζουν σε 3 από τα πιο γνωστά δίκτυα blockchain, το **Ethereum**, το **EOS** και το **Tron**. Η ασφάλεια του συστήματος δεν επιτυγχάνεται με τις συνηθισμένες τεχνικές κρυπτογραφίας που γνωρίζουμε, αλλά με δύο τρόπους. Τα **commitment schemes**, στα οποία μια οντότητα μπορεί να μεταδώσει μια πληροφορία προς μια “μυστική” οντότητα, μια οντότητα που δεν γνωρίζει τίποτα για αυτήν. Τα **zero knowledge proofs**, τα οποία αποτελούν κρυπτογραφικά πρωτόκολλα και δίνουν την δυνατότητα σε μια οντότητα ή ένα σύνολο οντοτήτων, να αποδείξουν πως ισχύει μια συνθήκη, σε μια άλλη ανεξάρτητη οντότητα. Να σημειωθεί πως οι δυο οντότητες δεν γνωρίζουν τίποτα η μια για την άλλη. Στο παρόν μοντέλο, πρέπει να είναι παρόντα τα λεγόμενα “Smart Parking Barriers”, τα οποία θα είναι επί της ουσίας μπάρες από χώρους στάθμευσης που θα διαθέτουν σύνδεση στο διαδίκτυο και ένα μοναδικό address που θα τα καθιστά διαθέσιμα στο blockchain. Το address τους θα αποτελείται από μια τιμή η οποία με τη μορφή διανύσματος θα περιέχει ανά πάσα στιγμή τον αριθμό των διαθέσιμων θέσεων στον χώρο στάθμευσης. Ο αριθμός αυτός θα

ενημερώνεται κάθε φορά που θα ανοιγο-κλείνει η μπάρα, από την εσωτερική (μια θέση αδειάζει) ή από την εξωτερική (μια θέση δεσμεύεται) μεριά. Οι χρήστες αλλά και οι ιδιοκτήτες χώρων στάθμευσης, θα πρέπει να διαθέτουν μια εφαρμογή στα έξυπνα κινητά τους τηλέφωνα. Όταν οι οδηγοί επιθυμούν να μισθώσουν μια θέση, θα δημιουργήσουν με τη βοήθεια της εφαρμογής, ένα έξυπνο συμβόλαιο και θα το στείλουν στο blockchain. Στο συμβόλαιο θα περιέχεται το ποσό που θα πρέπει να καταβληθεί ώστε να μισθωθεί η θέση στάθμευσης σε έναν συγκεκριμένο χώρο στάθμευσης, μαζί με ένα commitment. Η υπηρεσία πληρωμής που θα είναι τύπου “Anonymous Payments Mechanism” και θα αποτελεί μια τρίτη υπηρεσία, θα λάβει το συμβόλαιο και θα το προωθήσει μαζί με **proof of payment** στον λογαριασμό του ιδιοκτήτη των χώρων στάθμευσης. Στη συνέχεια αφού θα αξιολογηθεί η εγκυρότητα του συμβολαίου με τον συνδυασμό των πρωτοκόλλων που είδαμε πιο πάνω, θα σταλεί το ποσό του οδηγού προς τον ιδιοκτήτη, στη μορφή **tokens** για να διατηρηθεί η ανωνυμότητα του ποσού της συναλλαγής. Τέλος, ο ιδιοκτήτης θα ενημερώσει (η διαδικασία αυτή γίνεται αυτόματα) τον μηχανισμό δέσμευσης και θα εμφανίζεται σε εφαρμογές άλλων χρηστών η χρονική διάρκεια που θα είναι δεσμευμένη η εν λόγω θέση. Αυτό θα γίνεται επι-πρόσθετα από τον μηχανισμό της μπάρας, ώστε να γνωρίζουν οι επόμενοι οδηγοί το επόμενο διαθέσιμο χρονικό διάστημα που θα μπορούν να μισθώσουν μια θέση στο εκάστοτε πάρκινγκ. Η μέθοδος αυτή αποτελεί ακόμα ένα παράδειγμα της χρήσης των τεχνολογιών blockchain στην αποκεντροποίηση του συστήματος της έξυπνης στάθμευσης. Σε ένα αποκεντροποιημένο σύστημα, οι χρήστες μπορούν να απολαμβάνουν τα οφέλη των υπηρεσιών, χωρίς να χρειάζεται οι ίδιοι να μοιράζονται τα προσωπικά τους δεδομένα στον κυβερνοχώρο. Επίσης, η μη χρήση κρυπτογραφικών τεχνικών και η αντικατάστασή τους με τα πρωτόκολλα ZKPoK και Commitment Schemes, καθιστά το σύστημα αρκετά πιο ελαφρύ και εύκολο στην υλοποίηση και σίγουρα αποτελεί μια από τις πιο γρήγορες εν καιρώ τεχνικές που χρησιμοποιούνται στις προσπάθειες επίλυσης του προβλήματος αναζήτησης σταθμεύσεως.

6.24 Smart Parking with Fair Selection and Imposing Higher Privacy Constraints in Parking Owner and Driver Information [24]

Στην έρευνα αυτή, ο συντάκτης προσπαθεί να δώσει λύση στο πρόβλημα του πάρκινγκ σε υπεραστικές κοινωνίες, στις οποίες λόγω άγνοιας των πολιτών, πολλαπλές θέσεις στάθμευσης αγνοούνται. Στην εν λόγω μελέτη, προτείνει επίσης ένα μοντέλο το οποίο είναι ασφαλές και θα βασίζεται στις τεχνολογίες blockchain, καθιστώντας το δίκαιο για τους οδηγούς, αξιόπιστο αλλά και ασφαλές. Ο συντάκτης τονίζει επίσης την αναξιοπιστία που πιστεύει πως κείται σε άλλα παρόμοια μοντέλα που χρησιμοποιούν έναν cloud

server, και εκμεταλλεύονται τα Vehicular ad hoc networks, συμπεραίνοντας πως παρόμοια συστήματα είναι ευάλωτα σε στιγμές αδυναμίας ή παύσης λειτουργίας του cloud server στον οποίο βασίζονται. Τη λύση στο πρόβλημα προτείνει με τη χρήση των εξής οντοτήτων. Αρχικά, στο **blockchain**, πληροφορίες όπως τα parking requests θα κρυπτογραφούνται και θα αποθηκεύονται. Επίσης, χρησιμοποιούνται **RSUs** τα οποία αποτελούν ένα άμεσο και ασφαλές κανάλι επικοινωνίας ανάμεσα στον οδηγό και στο blockchain. Επίσης, έχουν την ιδιότητα να επαληθεύουν το request του οδηγού πριν το στείλουν στο blockchain, αλλά και του επιστρέφουν το αποτέλεσμα ενός Parking spot machine, μιας ψηφιακής μηχανής δηλαδή που θα δεσμεύσει σε φυσικό επίπεδο την θέση στάθμευσης του οδηγού. Εδώ αξίζει να σημειωθεί πως το μοντέλο αυτό λειτουργεί υπό την προϋπόθεση πως όλα τα οχήματα που αφορά είναι ηλεκτρικά και διαθέτουν διαδικτυακή σύνδεση. Τέλος, μια έμπιστη αρχή (**Trusted Authority**), είναι υπεύθυνη για την δημιουργία ζεύγων κλειδιών για οδηγούς που επιθυμούν να εγγραφούν στο σύστημα. Στην φάση της εγγραφής, οι οδηγοί που επιθυμούν να εγγραφούν στο σύστημα θα πρέπει να ταυτοποιηθούν με κάποιον τρόπο που θα οριστεί από την TA. Ο τρόπος αυτός μπορεί να είναι κάποιο κρατικό έγγραφο, αφού υποθέτουμε πως η TA είναι ελεγχόμενη οντότητα από το κράτος. Στη συνέχεια τους ανατίθεται ένα ζεύγος κλειδιών που θα χρησιμοποιείται στα RSU για την ταυτοποίηση τους και την αποκρυπτογράφηση του parking request τους. Για να δημοσιευτεί μια θέση στάθμευσης στο μοντέλο, θα πρέπει αρχικά να μετατραπεί σε γράφημα του οποίου οι συντεταγμένες θα στέλνονται ως έχουν στο blockchain. Όταν ο οδηγός επιθυμεί να μισθώσει μια θέση στάθμευσης, θα στέλνει ένα request στο κοντινότερο RSU που όπως είπαμε θα ελέγχεται. Στο request θα υπάρχει το εύρος στον χάρτη που θα επιθυμεί να βρεί μια θέση στάθμευσης, με την μορφή διανύσματος συντεταγμένων. Στη συνέχεια, θα επιστρέφει στο RSU η λίστα με τα matching parking lots, από το blockchain και ο χρήστης θα περνά στην διαδικασία της μίσθωσης. Η μίσθωση θα γίνεται ανώνυμα από τρίτες εφαρμογές. Στην έρευνα αυτή, είδαμε για άλλη μια φορά ένα μοντέλο υλοποιημένο σε blockchain περιβάλλον. Στα συστήματα αυτά, προστατεύεται η ιδιωτικότητα του οδηγού αλλά και διατηρείται η ανωνυμότητά του. Από την όψη της κρυπτογράφησης, χρησιμοποιήθηκαν απλές τεχνικές ψηφιακής υπογραφής από την έμπιστη αρχή και τίποτα περισσότερο, αφού τα δεδομένα που εισέρχονται και εξέρχονται στο blockchain είναι ριζικά κρυπτογραφημένα. Τέλος, η τοποθεσία του χρήστη αλλά και ο χάρτης που αποτελεί το σύνολο των πάρκινγκ, έχουν μετατραπεί σε γράφημα του οποίου οι συντεταγμένες είναι εξίσου κρυπτογραφημένες.

6.25 Smart City IoT Platform Respecting GDPR Privacy and Security Aspects [25]

Στην έρευνα αυτή, παρουσιάζεται ένα πολύπλοκο και ολοκληρωμένο μοντέλο που αφορά τις έξυπνες πόλεις. Οι ερευνητές αναφέρονται στο μοντέλο **Snap4City** ως ένα ολοκληρωμένο σχέδιο μέσα από την εκμετάλλευση του οποίου θα δοθεί η δυνατότητα σε μια πόλη να εκσυγχρονιστεί με τις τεχνολογίες Internet of Things και να υιοθετήσει τον όρο **Internet of Everything (IoE)** όπως θα εξηγηθεί παρακάτω. Σε μια συνηθισμένη πόλη, συναντάμε πολλές συσκευές οι οποίες εκτελούν συγκεκριμένες λειτουργίες ασύγχρονα. Χαρακτηριστικά παραδείγματα τέτοιων συσκευών είναι τα φανάρια στους δρόμους, ή οι μετρητές ρεύματος και νερού που βρίσκουμε σε πολυκατοικίες. Το μοντέλο που προτείνουν οι ερευνητές προϋποθέτει την αντικατάσταση των παλαιών συσκευών με νέες σύγχρονες συσκευές οι οποίες θα συνδέονται σε ένα τοπικό δίκτυο και στη συνέχεια στο διαδίκτυο ώστε να μπορούν να μεταδίδουν την πληροφορία που φέρουν προς τον αντίστοιχο φορέα που θα την αξιοποιήσει άμεσα και εύκολα. Όπως είναι προφανές, η υλοποίηση ενός τέτοιου μοντέλου σε μια πόλη, θα ωθήσει και στην αντικατάσταση των πατροπαράδοτων μεθόδων εύρεσης πάρκινγκ. Ο οδηγός πλέον θα μπορεί να βασιστεί σε ένα σύστημα πλήρως εξοπλισμένο και διαμορφωμένο έτσι ώστε να χρησιμοποιεί κάθε δυνατή πληροφορία που του είναι διαθέσιμη (πληροφορίες από κάμερες, φανάρια, αισθητήρες χώρων στάθμευσης κ.α.) για να δώσει στον χρήστη την δυνατότητα να κατευθυνθεί με ευκολία σε μια θέση στάθμευσης. Το μοντέλο που προτείνουν οι ερευνητές θα έχει τις παρακάτω ιδιότητες. Αρχικά, θα υποστηρίζει πολλούς και διαφορετικούς τύπους IoT Brokers. Με την χρήση αλγορίθμων μηχανικής μάθησης, θα μπορεί το μοντέλο να “μαθαίνει” και νέα είδη συσκευών που θα συνδέονται σε αυτό. Θα εκτελεί αλγορίθμους κατηγοριοποίησης σε συνδυασμό με μοντέλα εκπαιδευμένα με τη βοήθεια αλγορίθμων μάθησης με ή χωρίς επίβλεψη. Επίσης, θα βρίσκεται σε θέση να εγγυάται την αξιοπιστία του δικτύου συνδεσιμότητάς των συσκευών σε αυτό, μέσα από επαληθευμένες συνδέσεις εγγυημένες από τρίτες εφαρμογές όπως το **AWS** και το **IoT Azure**. Επίσης, ενημερώνει τους χρήστες για τα επίπεδα ασφαλείας των συσκευών που θα συνδέουν εκείνοι στο framework, και αν οι συσκευές τους αυτές θα καλύπτονται από θέματα ασφαλείας στο σύστημα. Ακόμη, θα παρέχεται συνεχής υποστήριξη της ασφάλειας του συστήματος από ειδικούς ερευνητές και εμπειρογνώμονες. Τέλος, το μοντέλο θα έχει open part και closed part όσον αφορά τον κώδικα λειτουργίας του, προσκαλώντας έτσι προγραμματιστές να βοηθήσουν στην ανάπτυξή του και λαμβάνοντας στη συνέχεια κάποια χρηματική απολαβή, ακόμη και πρόσληψη στην ομάδα που συγκροτεί συλλογική αυτή προσπάθεια. Από πλευρά κρυπτογραφίας, οι ερευνητές επέλεξαν τους αλγορίθμους **X.509 certificate** για την

έκδοση ψηφιακών πιστοποιητικών εγκυρότητας των cloud server που θα αποθηκεύεται η πληροφορία. Επίσης για την διασφάλιση της εμπιστευτικότητας χρησιμοποιείται το πρωτόκολλο SSL/TLS κατά την μεταφορά αρχείων στο σύστημα.

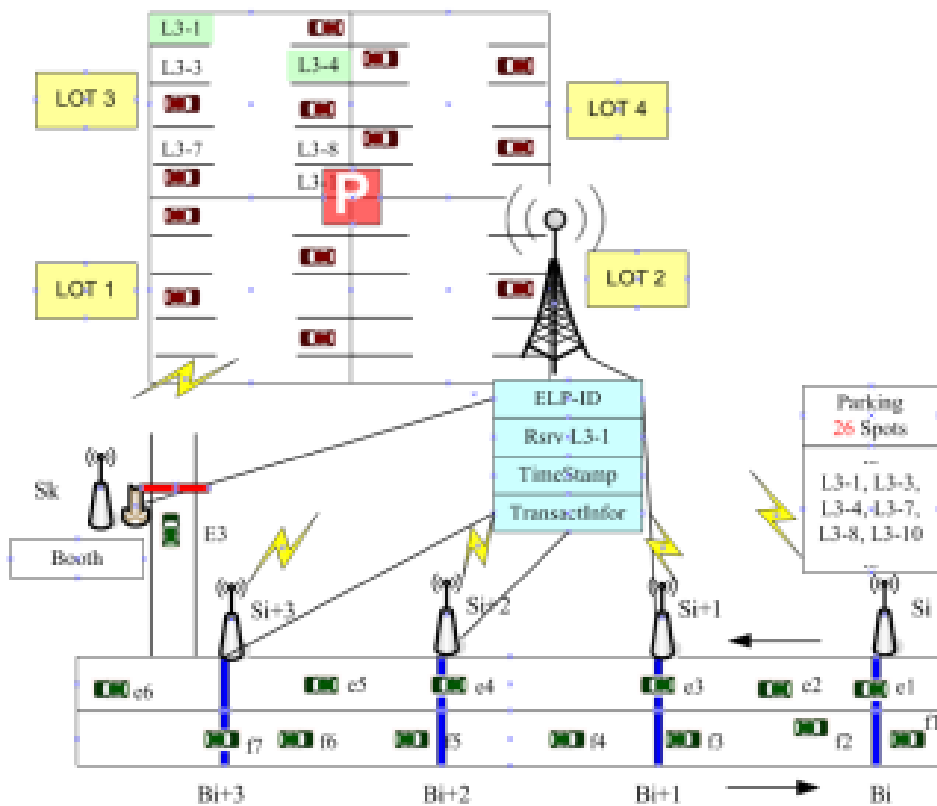
6.26 Smart Parking System With Privacy Preservation and Reputation Management Using Blockchain [26]

Στην μελέτη αυτή, οι συντάκτες δημιούργησαν ένα σύστημα έξυπνης εύρεσης πάρκινγκ, με την δημιουργία ενός τοπικά διαχειρίσιμου δικτύου blockchain, που θα εκτείνεται ανάμεσα στους ιδιωτικούς χώρους στάθμευσης που θα το συγκροτούν. Τα οχήματα των οδηγών δεν απαιτείται να διαθέτουν σύνδεση στο διαδίκτυο αφού ο οδηγός θα μπορεί να αξιοποιήσει το μοντέλο με την εγκατάσταση της αντίστοιχης εφαρμογής στο έξυπνο κινητό τηλέφωνό του. Επίσης, για την πλήρης λειτουργία του μοντέλου, πρέπει να βρίσκεται παρόν ένα **Key Distribution Center**, το οποίο θα είναι υπεύθυνο για την αυθεντικοποίηση των χρηστών κατά την διαδικασία της εγγραφής τους στο σύστημα, αλλά και την ανακατεύθυνση των πληροφοριών τους, όπως οι κρατήσεις τους, στο blockchain. Αρχικά, το KDC εκδίδει ένα σετ κλειδιών για το κάθε parking lot, με τη χρήση του **Schnorr Multi-Signature Algorithm** και υπογράφει τα δημόσια κλειδιά με τη χρήση της **short randomizable signature**. Παρομοίως, ο οδηγός στέλνει τα στοιχεία του στο KDC κρυπτογραφημένα μέσα από το ασφαλές κανάλι επικοινωνίας (blockchain), και αποκτά το ζεύγος κλειδιών υπογεγραμμένο από το KDC με τον ίδιο τρόπο. Στην έρευνα αυτή, ο χάρτης χωρίζεται σε $C(n)$ μέρη στα οποία εκτελείται η ανακατεύθυνση μέσω του blockchain, όταν ο οδηγός πραγματοποιεί μια αναζήτηση μέσω της εφαρμογής. Η αναζήτηση γίνεται με την αποστολή ενός query από τον οδηγό, το οποίο περιέχει την γεωγραφική συντεταγμένη που επιθυμεί να αναζητήσει πάρκινγκ. Η συντεταγμένες έχουν μετατραπεί σε διανύσματα και συνοδεύονται στο query μαζί με το δημόσιο κλειδί του οδηγού που είναι υπογεγραμμένο από το KDC. Τέλος, στον χρήστη επιστρέφουν τα αντίστοιχα αποτελέσματα αφού η διαθεσιμότητα των χώρων στάθμευσης γίνεται γνωστή και τακτά ενημερωμένη στο blockchain από τα parking lots. Η διαδικασία απόκρυψης των τοποθεσιών των πάρκινγκ και των οδηγών εντάσσεται στην κατηγορία των **private information retrieval techniques**. Τέλος το σύστημα περνά με ασφάλεια σε address-based τρίτες εφαρμογές πληρωμής, μέσα από την οποία μπορεί ο χρήστης να πληρώσει την μισθωμένη του θέση ανώνυμα. Το σύστημα αυτό σέβεται την ιδιωτικότητα

των στοιχείων του χρήστη αφού χρησιμοποιεί τεχνικές για να αποκρύψει τα στοιχεία του αλλά και την τοποθεσία του.

6.27 SmartParking: A Secure and Intelligent Parking System Using NOTICE [27]

Στην έρευνα αυτή, οι ερευνητές υλοποίησαν ένα μοντέλο το οποίο δίνει λύση στο πρόβλημα αναζήτησης πάρκινγκ με έναν έξυπνο και ασφαλή τρόπο. Η μελέτη τους αποτελεί την ανάλυση του μοντέλου τους, ονόματι “NOTICE”, το οποίο επιτρέπει στους οδηγούς να πραγματοποιήσουν μια κράτηση θέσης εύκολα άμεσα αλλά και με ασφάλεια. Το μοντέλο αυτό μπορεί να λειτουργήσει σε κοινόχρηστους χώρους είτε αυτοί είναι ελεύθερη προς χρήση είτε απαιτούν κάποια μίσθωση. Η υπηρεσία θα μπορεί να υλοποιηθεί και από ιδιωτικούς χώρους στάθμευσης (πάρκινγκ) όμως θα πρέπει να διαθέτουν τον κατάλληλο εξοπλισμό (αισθητήρες κ.α.) που όπως θα δούμε παρακάτω είναι καθοριστικός στη λειτουργία του χώρου στάθμευσης. Οι χώροι στάθμευσης πρέπει να είναι εξοπλισμένοι με έναν μαγνητικό εξοπλισμό ο οποίος θα ενημερώνει. Οι δρόμοι της πόλης που θα επιλέξει να υλοποιήσει το σχέδιο αυτό, θα είναι επίσης εξοπλισμένοι με κάποιους κάθετους ως προς το οδόστρωμα μαγνητικούς μηχανισμούς, οι οποίοι θα μεταδίδουν στον server του συστήματος την άμεση εικόνα των αυτοκινήτων που μετακινούνται από και προς τις διαθέσιμες θέσεις στάθμευσης. Από πρακτικής απόψεως, οι οδηγοί θα πρέπει να διαθέτουν την αντίστοιχη εφαρμογή στα έξυπνα τηλέφωνα τους. Ένας cloud server θα επικοινωνεί με τον μαγνητικό εξοπλισμό, ο οποίος θα διαθέτει δικτυακή σύνδεση. Οι μαγνητικά εξοπλισμένοι δρόμοι θα βρίσκονται πριν τους κοινόχρηστους χώρους πάρκινγκ. Όταν τα οχήματα που θα μεταβαίνουν σε έναν δρόμο μαγνητικά εξοπλισμένο θα **στρίψουν** βγαίνοντας από την πορεία τους για να μεταβούν στο πάρκινγκ, ένας μηχανισμός θα δεσμεύει μια θέση για το όχημά τους. Για την καλύτερη κατανόηση του μοντέλου, παρέχεται η παρακάτω εικόνα από τους συντάκτες της έρευνας.



[27] Μοντέλο NOTICE

Ο κάθε χώρος στάθμευσης θα διαθέτει έναν local server ο οποίος με τη χρήση του διαδικτύου θα πραγματοποιεί μια ασφαλής σύνδεση με σκοπό να ενημερώνει την εφαρμογή για την διαθεσιμότητα των θέσεων στάθμευσης. Η μελέτη αυτή δεν απαιτεί την χρήση κρυπτογραφικών τεχνικών. Αυτό συμβαίνει διότι δεν απαιτείται στο εύρος της καμία μορφή επαλήθευσης και κανένας διαμοιρασμός των προσωπικών στοιχείων των οδηγών. Το σύστημα γνωρίζει την τοποθεσία του κάθε αυτοκινήτου με την χρήση των μαγνητικών αισθητήρων. Το μοντέλο αυτό αποσκοπεί σε έναν δίκαιο διαμοιρασμό των θέσεων στάθμευσης για τους οδηγούς, αφού ο οδηγός μπορεί στιγμιαία να πραγματοποιήσει μια κράτηση της θέσης που εντόπισε οπτικά. Σκοπός του συστήματος δεν είναι η χρόνια εκμίσθωση θέσεων αλλά ο δίκαιος διαμοιρασμός των θέσεων σε όσα οχήματα βρέθηκαν στον μαγνητικά εξοπλισμένο χώρο νωρίτερα από κάποια άλλα.

6.28 SRSP: A Secure and Reliable Smart Parking Scheme With Dual Privacy Preservation [28]

Στην μελέτη αυτή, οι ερευνητές επιδιώκουν να λύσουν τα προβλήματα ασφαλείας των εφαρμογών έξυπνου πάρκινγκ, μέσα από την δημιουργία ασφαλών καναλιών επικοινωνίας και την χρήση **διπλών** μεθόδων κρυπτογράφησης και επαλήθευσης των οντοτήτων του συστήματος. Στην μελέτη αυτή, αναγκαία είναι η ύπαρξη μιας **Trusted Authority** (έμπιστης αρχής), η οποία θα είναι υπεύθυνη για την έκδοση ζεύγων κλειδιών που θα ανατίθενται στις οντότητες. Είναι επίσης υπεύθυνη για την επαλήθευση των οντοτήτων με την χρήση της ψηφιακής υπογραφής. Τα οχήματα θα πρέπει να κατέχουν σύνδεση στο διαδίκτυο και την δυνατότητα να συνδέονται στα αρμόδια **fog nodes**. Σε κάθε όχημα που θα πραγματοποιεί εγγραφή στο σύστημα, θα ανατίθενται ένα ψευδώνυμο **pseudoDi** το οποίο θα εκτελεί τον ρόλο του ID για το όχημα, με σκοπό να επικοινωνεί με τα fog nodes με ασφάλεια. Για το δεύτερο στρώμα ασφαλείας, παρών θα είναι ένας **Pseudonym Changer**, ο οποίος θα λειτουργεί στον **cloud server** που θα είναι συνδεδεμένες όλες οι οντότητες. Σκοπός του θα είναι να αλλάζει αυτόματα το pseudoDi των οχημάτων, και να ενημερώνει τα fog nodes για τις αλλαγές που πραγματοποιήθηκαν στα ψευδώνυμα. Κατά την εγγραφή στο σύστημα, η TA εκδίδει σετ κλειδιών για όλες τις οντότητες με την χρήση της ίδιας διαδικασίας. Επιλέγει ένα τυχαίο ιδιωτικό κλειδί i και χρησιμοποιώντας την τεχνική **bilinear pairing**, παράγει ένα δημόσιο κλειδί αντίστοιχα. Όταν ο οδηγός επιθυμεί να πραγματοποιήσει μια κράτηση, στέλνει ένα query στον parking server. Κατά την δημιουργία του query, το όχημα δημιουργεί με την χρήση του ψευδωνύμου του ένα προσωρινό δημόσιο κλειδί. Υπογράφει στη συνέχεια το query του με τη χρήση του **Zero Knowledge Proof of Knowledge Protocol** και το στέλνει στον parking server. Ο server αποκρυπτογραφεί και ελέγχει την εγκυρότητα της υπογραφής του query που έχει υπογραφεί με ένα υπογεγραμμένο ψευδο-κλειδί παραγόμενο από την TA. Εάν η επαλήθευση γίνει με επιτυχία, αναζητά το αντίστοιχο fog node και επιστρέφει το αποτέλεσμα στην εφαρμογή του οδηγού. Η διαδικασία ολοκληρώνεται με την πληρωμή του οδηγού στο σημείο του πάρκινγκ. Η έρευνα αυτή αποτελεί ακόμη ένα παράδειγμα της ασφαλούς αξιοποίησης των IoT τεχνολογιών ώστε να δημιουργήσουν ένα αποτέλεσμα σεβόμενο προς την ιδιωτικότητα του οδηγού και την ακεραιότητα των προσωπικών του στοιχείων.

6.29 Implementation of Public-Key Infrastructure for Smart Parking System Using MQTT Protocol [29]

Στη έρευνα αυτή, οι συντάκτες υλοποίησαν ένα μοντέλο έξυπνου πάρκινγκ το οποίο επιτυγχάνει την ασφάλεια με τον συνδιασμό των τεχνικών του **Zero Knowledge Proof of Knowledge Protocol**

και της **Elliptic Curve Cryptography**. Επίσης, χρησιμοποιήθηκε το πρωτόκολλο **MQTT** με σκοπό την εδραίωση ενός ασφαλές καναλιού επικοινωνίας ανάμεσα στον οδηγό και το σύστημα πάρκινγκ. Το μοντέλο μπορεί να εκφραστεί σε δύο βήματα. Σεβόμενοι του τρόπου λειτουργίας του ZKP μπορούμε να ορίσουμε τους οδηγούς ως “αυτούς που εκτελούν την ερώτηση” και τους ιδιοκτήτες των χώρων πάρκινγκ ως “αυτούς που θα την επαλυθεύσουν”. Όταν ένας αισθητήρας που αναπαριστά ένα **fog node**, εντοπίσει ένα όχημα, εδραιώνει μια ασφαλή σύνδεση ανάμεσα στο όχημα και τον parking server. Μόλις η σύνδεση εδραιωθεί, ο οδηγός μεταδίδει το request του στον parking server. Την επικοινωνία εδραιώνει ο MQTT broker, ο οποίος λαμβάνει μια τυχαία τιμή από τον “subscriber” οδηγό, την υπογράφει και την στέλνει στη συνέχεια στον “publisher” parking server.

Κεφάλαιο 7 : Σύγκριση μεθόδων

Στο προηγούμενο κεφάλαιο μελετήσαμε εκτενώς ένα σύνολο από μεθόδους μέσα από τις οποίες, ερευνητές ανά την εμφύλιο επιχείρησαν να παρουσιάσουν ένα μοντέλο έξυπνου πάρκινγκ. Στις μελέτες χρησιμοποιήθηκαν πολλές και διαφορετικές αρχιτεκτονικές που μπορεί να διαφέρουν από το καθολικό σχέδιο που είδαμε στο κεφάλαιο 3. Είναι σημαντικό, ως επίλογος της πτυχιακής εργασίας, να αναπαραστήσουμε την πληροφορία που μόλις λάβαμε μέσα από την κατανομή της και στη συνέχεια την προβολή της με την μορφή διαγραμμάτων. Έτσι θα μπορέσουμε με μεγαλύτερη ευκολία να αξιολογήσουμε την συχνότητα των κοινών αρχιτεκτονικών, τις κοινές μεθόδους που χρησιμοποίησαν οι συντάκτες αλλά και την **κρυπτογραφία** που χρησιμοποιήθηκε στις πολλές και διαφορετικές έρευνες.

Ακολούθως, θα παρουσιάσουμε το έργο με ταξινομημένο και καθαρό τρόπο. Ο σκοπός της διαδικασίας αυτής είναι να φτάσουμε σε ένα νέο καθολικό μοντέλο αρχιτεκτονικής αλλά και να εστιάσουμε καλύτερα στις πιο συχνά χρησιμοποιημένες τεχνικές κρυπτογραφίας, τεχνικές που βασίστηκαν οι ερευνητές στην συλλογική τους προσπάθεια για μια λειτουργική και πλήρως ασφαλισμένη εφαρμογή. Στη συνέχεια ακολουθεί ο πίνακας αλλά και οι κατηγορίες με βάση τις οποίες θα εξεταστούν οι έρευνες. Το .xlsx αρχείο είναι διαθέσιμο [εδώ](#).

7.1 Σύγκριση ως προς την κρυπτογραφία

Στον παρακάτω πίνακα παρατηρούμε τις μεθόδους κρυπτογράφησης που χρησιμοποιήθηκαν στις παραπάνω μελέτες.

Αριθμός Έρευνας	Μέθοδος Κρυπτογράφησης
[1]	NOT INCLUDED
[2]	Local Differential Privacy with Elliptic Curve Cryptography
[3]	Point to Point Protocol
[4]	Bilinear Pairing
[5]	Diffie-Hellman with Elliptic Curve & Zero Knowledge Proof
[6]	Bilinear Pairing & Hashmap & Random Selection Algorithm
[7]	Bloom filters
[8]	Pedersen Commitment & TESLA Protocol & TLS Protocol
[9]	Zero Knowledge Proof of Knowledge Protocol & AES & Bloom filtes
[10]	NOT INCLUDED
[11]	NOT INCLUDED
[12]	Differential Privacy & Laplace Distribution
[13]	Zero Knowledge Proof of Knowledge Protocol
[14]	Zero Knowledge Proof of Knowledge Protocol & Obvious Pseudorandom Function & Re-Randomized Public-Key Encryption
[15]	Fuzzy Skyline Fusion Algorithm &
[16]	Proof of Possession
[17]	Bloom filters & Pointcheval and Sanders Signature & Zero Knowledge Proof of Knowledge Protocol & Diffie Hellman & Bloom filter
[18]	Zero Knowledge Proof of Knowledge Protocol & Random Selection Algorithm
[19]	Dynamic Group Signature & Cuckoo filter & Pedersen commitment
[20]	TLS Protocol & X.509 certificate
[21]	Linked Group Signatures & AES
[22]	Zero Knowledge Proof of Knowledge Protocol & Proxy Signature & Bilinear maps
[23]	Zero Knowledge Proof of Knowledge Protocol & Differential Privacy & Commitment Schemes
[24]	NOT INCLUDED
[25]	X.509 certificate & SSL/TLS Protocol
[26]	Schnorr Multi-Signature Algorithm & Short Randomizable Signature
[27]	NOT NEEDED
[28]	Zero Knowledge Proof of Knowledge Protocol & Bilinear Pairing

[29]	Zero Knowledge Proof of Knowledge Protocol & Elliptic Curve Cryptography & MQTT Protocol
------	--

Στον πίνακα αυτόν, παρατηρούμε τις μεθόδους κρυπτογράφησης που χρησιμοποιήθηκαν στις έρευνες που μελετήσαμε. Παρατηρούμε την συχνή χρήση του Zero Knowledge Proof of Knowledge αλγορίθμου. Αυτό οφείλεται στην εύκολη χρήση του, στην προσπάθεια να κρυπτογραφηθεί πληθώρα δεδομένων η οποία, σε μια συντριπτική πλειοψηφία των περιπτώσεων όπως θα δούμε παρακάτω, μεταδιδόταν με την χρήση της τεχνολογίας blockchain.

7.2 Σύγκριση ως προς την αρχιτεκτονική

Στον παρακάτω πίνακα παρατηρούμε την αρχιτεκτονική που χρησιμοποιήθηκε στις μελέτες.

Αριθμός Έρευνας	Χρήση Αρχιτεκτονικής
[1]	OCR & Pattern Recognition with IoT Cameras for License Plate
[2]	IoT scheme
[3]	IoT scheme & GPRS & IEEE 802.15.4
[4]	IoT scheme & VANET
[5]	Smartphone Testbed
[6]	IoT scheme
[7]	IoT scheme & blockchain
[8]	IoT scheme
[9]	IoT scheme & VANET
[10]	IoT scheme & Trust Monitoring
[11]	Literature Review
[12]	IoT scheme & Anonymized DB
[13]	IoT scheme & blockchain
[14]	IoT scheme & blockchain
[15]	IoT scheme
[16]	IoT scheme & Smart Contracts
[17]	IoT scheme & Smart Contracts & VANET
[18]	IoT scheme & blockchain
[19]	IoT scheme & blockchain
[20]	IoT scheme & Mutual Handshake Mechanism
[21]	IoT scheme & blockchain
[22]	IoT scheme & Auto-piloted Vehicles
[23]	IoT scheme & blockchain
[24]	IoT scheme & blockchain & VANET
[25]	IoT scheme
[26]	IoT scheme & blockchain
[27]	IoT scheme
[28]	IoT scheme
[29]	IoT scheme

Παρατηρούμε πως χρησιμοποιείται σε όλα σχεδόν τα μοντέλα, η προσέγγιση Internet of Things, σύμφωνα με την οποία, το μοντέλο του έξυπνου πάρκινγκ υλοποιείται με την βοήθεια αισθητήρων που θα διαθέτουν σύνδεση στο διαδίκτυο και θα μεταδίδουν αλλά και θα δέχονται με ασφάλεια πληροφορία.

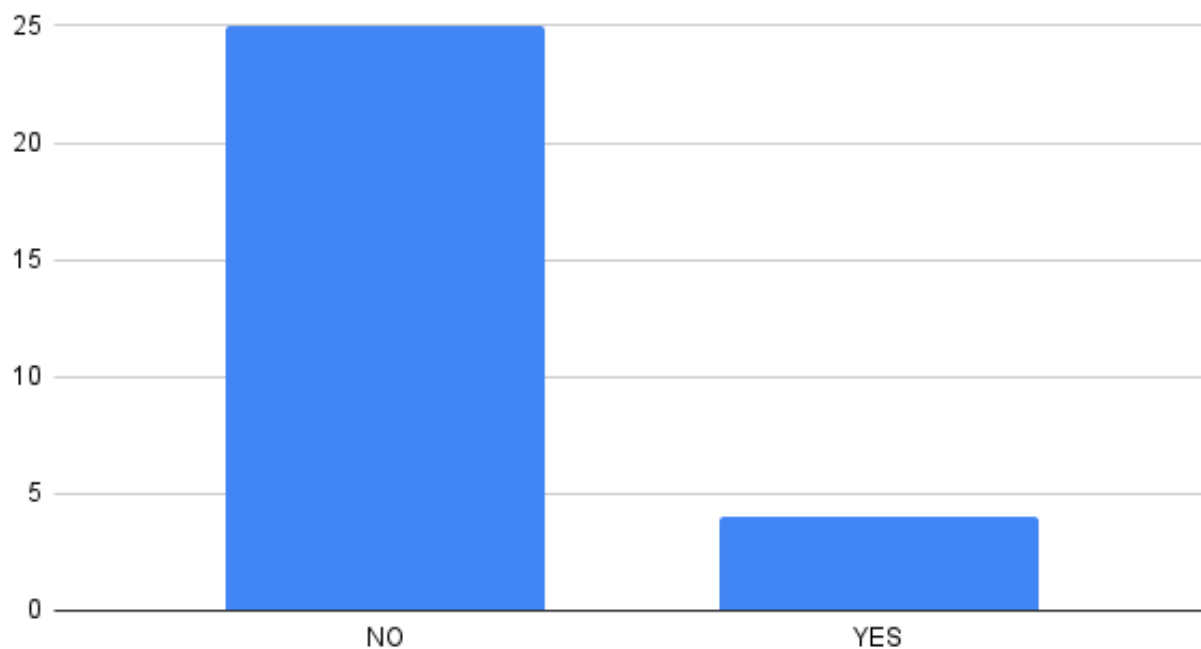
7.3 Σύγκριση ως προς τη χρήση Elliptic Curve Cryptography

Η τεχνική αυτή της κρυπτογραφίας είναι βολική για συσκευές με περιορισμένη μνήμη και υπολογιστική ισχύς, διότι καταφέρουν να ελαττώσουν το μήκος κλειδιού αλλά και να παράγουν ένα ισοδύναμο με το 1/9 των απαιτούμενων bits. Παρ' ολ' αυτά, διαπιστώθηκε πως η τεχνική αυτή δεν χρησιμοποιήθηκε σε μεγάλο φάσμα από τους ερευνητές των μοντέλων έξυπνου πάρκινγκ.

Αριθμός Έρευνας	Χρήση Elliptic Curve
[1]	NO
[2]	YES
[3]	NO
[4]	NO
[5]	YES
[6]	NO
[7]	NO
[8]	YES
[9]	NO
[10]	NO
[11]	NO
[12]	NO
[13]	NO
[14]	NO
[15]	NO
[16]	NO
[17]	NO
[18]	NO
[19]	NO
[20]	NO
[21]	NO
[22]	NO
[23]	NO
[24]	NO
[25]	NO
[26]	NO
[27]	NO
[28]	NO
[29]	YES

Για την καλύτερη προβολή του αποτελέσματος, παρατίθενται παρακάτω μια οπτική απεικόνιση του πίνακα σε μορφή γράφου.

Elliptic Curve Cryptography in Smart Parking Applications



Απεικόνιση με την μορφή γραφήματος, των μελετών ανάλογα με την χρήση της *Elliptic Curve Cryptography*.

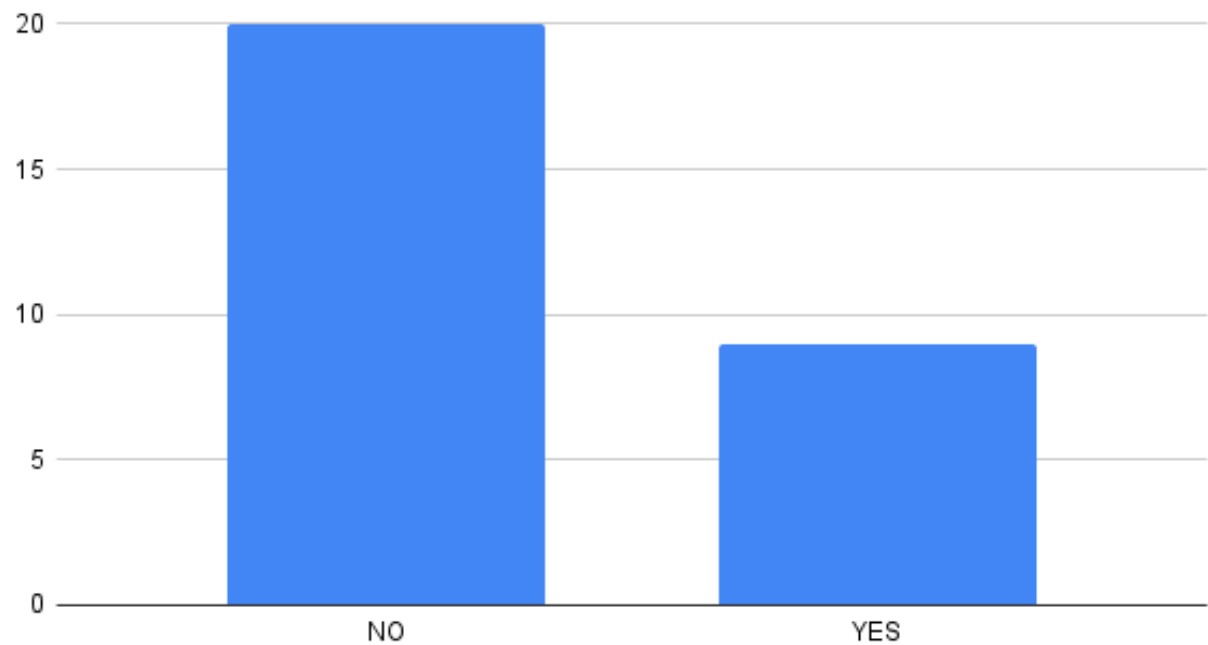
7.4 Σύγκριση ως προς την χρήση Blockchain

Κατά την πορεία της πτυχιακής εργασίας, παρατηρήθηκε πως πολλοί ερευνητές στήριξαν τις μελέτες τους στην τεχνολογία blockchain. Η τεχνολογία αυτή, στο έπακρο της εξέλιξής της, μπορεί να βοηθήσει πολλές εφαρμογές να μεταδίδουν και να αποθηκεύουν τα δεδομένα τους σε ένα ασφαλές και άμεσα προσβάσιμο δίκτυο. Ο πίνακας των ερευνών που αξιοποίησαν την τεχνολογία blockchain φαίνεται παρακάτω.

Αριθμός Έρευνας	Χρήση blockchain
[1]	NO
[2]	NO
[3]	NO
[4]	NO
[5]	NO
[6]	NO
[7]	YES
[8]	NO
[9]	NO
[10]	NO
[11]	NO
[12]	NO
[13]	YES
[14]	YES
[15]	NO
[16]	YES
[17]	NO
[18]	YES
[19]	YES
[20]	NO
[21]	NO
[22]	NO
[23]	YES
[24]	YES
[25]	NO
[26]	YES
[27]	NO
[28]	NO
[29]	NO

Για την καλύτερη απεικόνιση του αποτελέσματος της σύγκρισης, ακολουθεί παρομοίως με πριν, το αντίστοιχο γράφημα των αποτελεσμάτων.

Blockchain Technology Usage in Smart Parking Applications



Γράφημα χρήσης της τεχνολογίας blockchain στις επιστημονικές μελέτες.

7.5 Άλλες συγκρίσεις

Αφού συγκρίναμε με επιτυχία τους κύριους παράγοντες των άρθρων, θα κλείσουμε την έρευνα μας με την παράθεση μεγαλύτερων πινάκων, στους οποίους παραθέτονται κάποιες επιπρόσθετες μετρήσεις. Η εξονυχιστική μελέτη των ερευνών που είδαμε στο 6ο κεφάλαιο, γεννά την ανάγκη για συλλογή των κοινών παραγόντων μέσα από τους οποίους οι ερευνητές έφτασαν έκαστοι στα επιθυμητά τους αποτελέσματα. Το αποτέλεσμα της εργασίας αυτής θα πρέπει να αποσκοπεί και στην ανάλυση της κρυπτογραφίας των μοντέλων πάνω στα οποία πραγματοποιήθηκε η μελέτη. Οι κοινοί παράγοντες αυτοί είναι οι παρακάτω:

- **Οι αλγόριθμοι επαλήθευσης ή υπογραφής των πιστοποιητικών/κλειδιών** που χρησιμοποιήθηκαν στις έρευνες. Όπως θα δείτε στον παρακάτω πίνακα, κάποια κελιά έχουν την τιμή “CUSTOM”. Αυτό συμβαίνει επειδή, για την μεγιστοποίηση της ασφάλειας, οι αντίστοιχοι ερευνητές μετέτρεψαν ήδη υπάρχοντες αλγόριθμους πιστοποίησης σε νέους, είτε δημιούργησαν από το μηδέν δικές τους τεχνικές μέσα από τις οποίες θα ελέγχεται η αυθεντικότητα των στοιχείων που απαιτούνται για κάθε διαδικασία αυθεντικοποίησης. Τέλος, στα κελιά που αναγράφεται το “NOT INCLUDED” σημαίνει πως στην συγκεκριμένη αναφορά δεν αναφέρεται με σαφήνεια ο τρόπος αυθεντικοποίησης των οντοτήτων.
- **Η χρήση δικτύων VANET (Vehicular ad-hoc networks)**, συμπεριλαμβάνεται στον πίνακα επειδή παρατηρήθηκε η εκτενής χρήση τους στα μοντέλα, αλλά κυρίως στα μοντέλα που απαιτούσαν την χρήση **ηλεκτρικών οχημάτων** με προ-εγκατεστημένα εργαλεία κρυπτογραφημένης γνωστοποίησης της τοποθεσίας του οχήματος.
- **Η χρήση RSU και OBU μονάδων αντίστοιχα**. Οι οντότητες αυτές συμπεριλήφθηκαν στους πίνακες επειδή είναι ενδιαφέρον να μελετήσουμε τις αλλαγές στις χρήσεις τους ανά έρευνα. Για παράδειγμα, στην έρευνα [22] παρατηρείται η χρήση RSU μονάδων αλλά όχι OBU. Επομένως το συγκεκριμένο μοντέλο έχει αναπτύξει κάποιον διαφορετικό τρόπο για να γνωρίζει την τοποθεσία του οχήματος, προφανώς με την χρήση του GPS ή GPRS που βρίσκεται στο έξυπνο τηλέφωνο του οδηγού.

Στις επόμενες σελίδες ακολουθούν οι πίνακες που προαναφέρθηκαν αντίστοιχα των αναφερόμενων ερευνών τους.

Αριθμός Έρευνας	Αλγόριθμοι υπογραφής
[1]	NOT_INCLUDED
[2]	NOT_INCLUDED
[3]	CUSTOM
[4]	CUSTOM
[5]	Local_Authentication
[6]	Random_Selection
[7]	BBS_Group_Signature
[8]	ThirdParty_ProVerif
[9]	PS_Signature
[10]	NOT_INCLUDED
[11]	NOT_INCLUDED
[12]	CUSTOM
[13]	CUSTOM
[14]	Blind_Certificate
[15]	CUSTOM
[16]	CUSTOM
[17]	Pointcheval_and_Sanders_Signature
[18]	CUSTOM
[19]	Dynamic_Group_Signature
[20]	X.509_certificate
[21]	AES
[22]	Proxy_Signature
[23]	Blind_Certificate
[24]	CUSTOM
[25]	CUSTOM
[26]	Short_Randomizable_Signature
[27]	NOT_INCLUDED
[28]	CUSTOM
[29]	CUSTOM

Πίνακας σύγκρισης των αλγορίθμων αυθεντικοποίησης στις έρευνες.

Αριθμός Έρευνας	Χρήση VANET
[1]	NO
[2]	YES
[3]	NO
[4]	YES
[5]	NO
[6]	NO
[7]	YES
[8]	YES
[9]	YES
[10]	NO
[11]	NO
[12]	YES
[13]	NO
[14]	NO
[15]	NO
[16]	NO
[17]	YES
[18]	NO
[19]	YES
[20]	NO
[21]	YES
[22]	YES
[23]	NO
[24]	YES
[25]	YES
[26]	NO
[27]	NO
[28]	NO
[29]	NO

Πίνακας χρήσης Vehicular ad-hoc Networks (VANET)

Αριθμός Έρευνας	Χρήση_RSU_fog_node_magnet	Χρήση_OBU
[1]	NO	NO
[2]	NO	NO
[3]	YES	NO
[4]	YES	YES
[5]	NO	NO
[6]	YES	NO
[7]	YES	YES
[8]	YES	YES
[9]	YES	YES
[10]	YES	NO
[11]	NO	NO
[12]	YES	YES
[13]	YES	NO
[14]	NO	YES
[15]	YES	YES
[16]	YES	YES
[17]	YES	YES
[18]	YES	NO
[19]	YES	NO
[20]	YES	NO
[21]	YES	YES
[22]	YES	NO
[23]	YES	NO
[24]	YES	NO
[25]	YES	YES
[26]	YES	NO
[27]	YES	NO
[28]	YES	NO
[29]	YES	NO

Πίνακας χρήσης RSU, OBU, fog nodes και μαγνητικών μονάδων υποβοήθησης IoT στα μοντέλα.

Κεφάλαιο 8 : Επίλογος

Στην πτυχιακή εργασία αυτή, εξετάσαμε εκτενώς το πρόβλημα του έξυπνου πάρκινγκ, μέσα από την ανάλυση ενός αριθμού επιστημονικών εργασιών που επιχείρησαν να δώσουν λύση στο πρόβλημα. Αρχικά ορίσαμε ένα γενικό μοντέλο, με το οποίο θα μπορούν να ταυτοποιηθούν τα περισσότερα από τα μοντέλα που είδαμε στη συνέχεια. Στη συνέχεια ορίσαμε κάποιους από τους στόχους που θα πρέπει το κάθε μοντέλο έξυπνου πάρκινγκ να πετυχαίνει. Έπειτα, αναφερθήκαμε στις πιο δημοφιλείς επιθέσεις που εμφανίζονται στις εφαρμογές έξυπνου πάρκινγκ, με σκοπό να κατατοπίσουμε τον αναγνώστη και να του προσφέρουμε μια πλήρη εικόνα του κινδύνου των επιθέσεων. Στη συνέχεια αναφερθήκαμε στις συγκεντρωμένες έρευνες, μέσα στις τις οποίες συναντήσαμε πολλές και διαφορετικές προσεγγίσεις του ίδιου προβλήματος. Τέλος, πραγματοποιήθηκε μια σύγκριση των μεθόδων που είδαμε στις μελέτες, με σκοπό την οπτικοποίηση του προβλήματος αλλά και των επιλεχθεισών λύσεων από τους ερευνητές.

Προσωπικά, η πτυχιακή αυτή με βοήθησε να αναγνωρίσω τον σημαντικό ρόλο που θα αποτελέσουν οι τεχνολογίες Internet of Things στο κοντινό μέλλον. Πολλοί άνθρωποι θα μπορούν να εργαστούν στην ανάπτυξη κώδικα σε κανάλια blockchain και να καλύψουν τις ανάγκες τους με την χρήση των IoT. Είναι σαφές πως οι τεχνολογίες IoT αλλά και το ανερχόμενο αστέρι 5G θα φέρουν την επανάσταση σε μια νέα πραγματικότητα όπου οι βασικές καθημερινές ανάγκες θα καλύπτονται εύκολα και ακόπιαστα.

Κεφάλαιο 9 : Βιβλιογραφία

- <https://www.businessinsider.com/stolen-data-of-533-million-facebook-users-leaked-online-2021-4>
- <https://www.igi-global.com/dictionary/background-knowledge-attacks/43024>

[1] Awad Saleh Alharbi, Mohammad Yamin, G.D. Halikias, Adnan Abi Sen, International Journal of Information Technology (2021), Web-based framework for Smart Parking Applications

[2] Aawis Abdul Khaliq, Adeel Anjum, Abdul Basit Ajmal, Julian L. Webber (Senior Member IEEE), Abolfazl Mehbodniya (Senior Member IEEE) and Shawal Khan (2022), A Secure and Privacy Preserved Parking Recommender System Using Elliptic Curve Cryptography and Local Differential Privacy

[3] Ilhan Aydin, Mehmet Karakose, Ebru Karakose, Firat University, Turkey (2017), A Navigation and Reservation Based Smart Parking Platform Using Genetic Optimization for Smart Cities

[4] Rongxing Lu[†], Xiaodong Lin[‡], Haojin Zhu[§], and Xuemin (Sherman) Shen[†] [†]Dept. of Electrical and Computer Engineering, University of Waterloo, Waterloo, Ontario, Canada N2L 3G1 [‡]Faculty of Business and Information Technology, University of Ontario Institute of Technology, Oshawa, Ontario, Canada [§]Dept. of Computer Science and Engineering, Shanghai Jiao Tong University, Shanghai, P.R. China (2009), An Intelligent Secure and Privacy-Preserving Parking Scheme Using Vehicular Communications

[5] Ioannis Chatzigiannakis ^{a,b,*}, Andrea Vitaletti ^a, Apostolos Pyrgelis ^c, ^a Department of Computer, Control, and Management Engineering (DIAG), Sapienza University of Rome, Italy, ^b Computer Technology Institute & Press “Diophantus” (CTI), Greece ^c Department of Computer Science, University College London (UCL), UK, Computer Communications (2016), A privacy-preserving smart parking system using an IoT elliptic curve

based security platform

[6] Liehuang Zhu , Member, IEEE, Meng Li , Student Member, IEEE, Zijian Zhang , Member, IEEE, Zhan Qin, Member, IEEE, IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, VOL. 17, NO. 4 (2020), ASAP: An Anonymous Smart-Parking and Payment Scheme in Vehicular Networks

[7] Can Zhang , Liehuang Zhu , Member, IEEE, Chang Xu , Chuan Zhang , Kashif Sharif , Member, IEEE, Huishu Wu, and Hannes Westermann, IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, VOL. 69, NO. 6 (2020), BSFP: Blockchain-Enabled Smart Parking With Fairness, Reliability and Privacy Protection

[8] Xiaoyu Zhang, Hong Zhong , Chunyang Fan, Irina Bolodurina, and Jie Cui , Senior Member, IEEE, 1930 IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 17, (2022), CBACS: A Privacy-Preserving and Efficient Cache-Based Access Control Scheme for Software Defined Vehicular Networks

[9] Lin, Xiaodong, Ni Jianbing, Shen Xuemin, Identity Privacy Protection in Smart Parking Navigation

[10] YASIR SALEEM , (Member, IEEE), PABLO SOTRES , SAMUEL FRICKER, (Member, IEEE), CARMEN LOPEZ DE LA TORRE, NOEL CRESPI , (Senior Member, IEEE), GYU MYOUNG LEE , (Senior Member, IEEE), ROBERTO MINERVA , AND LUIS SANCHEZ, IoTRec: The IoT Recommender for Smart Parking System

[11] Elvira Ismagilova & Laurie Hughes & Nripendra P. Rana & Yogesh K. Dwivedi, Security, Privacy and Risks Within Smart Cities: Literature Review and Development of a Smart City Interaction Framework

[12] Yasir Saleem, Mubashir Husain Rehmani ,Noel Crespi, Roberto Minerva, Parking recommender system privacy preservation through anonymization and differential privacy

[13] Jiayi Hu, Debiao He, Qinglan Zhao, and Kim-Kwang Raymond Choo, Parking Management A blockchain-based privacy-preserving system.

[14] Zengpeng Li , Mamoun Alazab , Senior Member, IEEE, Sahil Garg , and M. Shamim Hossain , Senior Member, IEEE, PriParkRec: Privacy-Preserving Decentralized Parking Recommendation Service

[15] Yinglong Li , Fan Liu, Jiaye Zhang, Tieming Chen , Hong Chen, Senior Member, IEEE, and Weiru Liu, Privacy-Aware Fuzzy Skyline Parking Recommendation Using Edge Traffic Facilities

[16] Petr Dzurenda dzurenda@vutbr.cz Brno University of Technology Czech Republic Carles Anglès-Tafalla carles.angles@urv.cat Universitat Rovira i Virgili Spain Sara Ricci ricci@vutbr.cz Brno University of Technology Czech Republic Lukas Malina malina@vutbr.cz Brno University of Technology Czech Republic, Privacy-Preserving Online Parking Based on Smart Contracts

[17] Jianbing Ni , Student Member, IEEE, Kuan Zhang , Member, IEEE, Yong Yu , Member, IEEE, Xiaodong Lin , Fellow, IEEE, and Xuemin Shen , Fellow, IEEE, Privacy-Preserving Smart Parking Navigation Supporting Efficient Driving Guidance Retrieval

[18] Wesam Al Amiri* , Mohamed Baza* , Karim Banawan† , Mohamed Mahmoud* , Waleed Alasmay‡ , Kemal Akkaya§ *Department of Electrical and Computer Engineering, Tennessee Tech University, Cookeville, TN, USA †Department of Electrical Engineering, Faculty of Engineering, Alexandria University, Alexandria, Egypt ‡Department of Computer Engineering, Umm Al-Qura University, Makkah, Saudi Arabia §Department of Electrical and Computer Engineering, Florida International University, Miami, FL, USA, Privacy-Preserving Smart Parking System Using Blockchain and Private Information Retrieval

[19] Qi Tang¹ , Jiachen Shen^{1*} , Zhenfu Cao^{1,2*} , Xiaolei Dong¹ ¹Shanghai Key Laboratory of Trustworthy Computing, East China Normal University, Shanghai, China ²Cyberspace Security Research Center, Peng Cheng Laboratory, Shenzhen Email:

51194501170@stu.ecnu.edu.cn, {jcshe, zfc, dongxiaolei}@sei.ecnu.edu.cn, PSSBP: A Privacy-preserving Scope-query Searchable Encryption Scheme Based on Blockchain for Parking Lots Sharing in Vehicular Networks

[20] Ali Alqazzaz, Ibrahim Alrashdi, Esam Aloufi, Mohamed Zohdy, Hua Ming, SecSPS: A Secure and Privacy-Preserving Framework for Smart Parking Systems

[21] Yan Zhang^{1,2}, Lei Zhang^{*,1,2}, Burong Kang^{1,2}, Yue Ma^{1,2}, Tong Chen^{1,2}
¹Engineering Research Center of Software/Hardware Co-design Technology and Application, Ministry of Education ²Shanghai Key Laboratory of Trustworthy Computing, School of Software Engineering East China Normal University, Shanghai, China, Secure and Reliable Parking Protocol Based on Blockchain for VANETs

[22] Cheng Huang , Student Member, IEEE, Rongxing Lu , Senior Member, IEEE, Xiaodong Lin , Fellow, IEEE, Secure Automated Valet Parking: A Privacy-Preserving Reservation Scheme for Autonomous Vehicles

[23] Nejc Rozman ~ Faculty of Mechanical Engineering University of Ljubljana, Slovenia nejc.rozman@fs.uni-lj.si Marko Corn Faculty of Mechanical Engineering University of Ljubljana, Slovenia marko.corn@fs.uni-lj.si Janez Diaci Faculty of Mechanical Engineering University of Ljubljana, Slovenia janez.diaci@fs.uni-lj.si, Sharing Economy: Implementing Decentralized Privacy-Preserving Parking System

[24] B. Vivekanadam Senior Lecturer, Faculty of Computer Science and Multimedia, Lincoln University College, Malaysia, Smart Parking with Fair Selection and Imposing Higher Privacy Constraints in Parking Owner and Driver Information

[25] CLAUDIO BADI , PIERFRANCESCO BELLINI , ANGELO DIFINO , AND PAOLO NESI , (Member, IEEE) Department of Information Engineering, University of Florence, 50121 Florence, Italy, Smart City IoT Platform Respecting GDPR Privacy and Security Aspects

[26] MAHMOUD M. BADR ¹ , WESAM AL AMIRI² , MOSTAFA M. FOUDA ^{3,7}, (Senior Member, IEEE), MOHAMED M. E. A. MAHMOUD ¹ , (Senior Member, IEEE), ABDULAH

JEZA ALJOHANI 4,6, (Member, IEEE), AND WALEED ALASMARY 5 , (Senior Member, IEEE), Smart Parking System With Privacy Preservation and Reputation Management Using Blockchain

[27] Gongjun Yan, Stephan Olariu, Michele C. Weigle, Mahmoud Abuelela, SmartParking: A Secure and Intelligent Parking System Using NOTICE

[28] Chengzhe Lai , Member, IEEE, Qian Li , Graduate Student Member, IEEE, Haibo Zhou , Senior Member, IEEE, and Dong Zheng, SRSP: A Secure and Reliable Smart Parking Scheme With Dual Privacy Preservation

[29] Rajilal Manathala Vijayan, R. Ezhilarasie and A. Umamakeswari, Implementation of Public-Key Infrastructure for Smart Parking System Using MQTT Protocol