Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών και Εφαρμοσμένων Επιστημών

Μεταπτυχιακή Διατριβή
Στην Ασφάλεια Υπολογιστών και Δικτύων

Αντιμετώπιση Απειλών Σε Δίκτυο IoT Με Χρήση Τεχνητής Νοημοσύνης Και Blockchain Για Την Γνωστοποίηση Του Βαθμού Εμπιστοσύνης Των IoT Συσκευών

Αθανάσιος Ρήγας

Επιβλέπων Καθηγητής
Σταύρος Σιαηλής

Μάϊος 2019

Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών και Εφαρμοσμένων Επιστημών

Αντιμετώπιση Απειλών Σε Δίκτυο IoT Με Χρήση Τεχνητής Νοημοσύνης Και Blockchain Για Την Γνωστοποίηση Του Βαθμού Εμπιστοσύνης Των IoT Συσκευών

Αθανάσιος Ρήγας

Επιβλέπων Καθηγητής
Σταύρος Σιαηλής

Η παρούσα μεταπτυχιακή διατριβή υποβλήθηκε
προς μερική εκπλήρωση των απαιτήσεων για απόκτηση

μεταπτυχιακού τίτλου σπουδών
στην Ασφάλεια Υπολογιστών και Δικτύων

από τη Σχολή Θετικών και Εφαρμοσμένων Επιστημών
του Ανοικτού Πανεπιστημίου Κύπρου

Μάϊος 2019

Περίληψη

Η ψηφιακή τεχνολογία αποτελεί θεμέλιο για τις σύγχρονες κοινωνίες. Είναι σχεδόν αδιανόητη η επιβίωση μας χωρίς αυτήν, καθώς τα οφέλη από την χρήση της είναι προφανή. Η αμεσότητα στην επικοινωνία και στις συναλλαγές, όπως και η εύκολη πρόσβαση στην πληροφορία, είναι μερικά από τα οφέλη.

Η πολυπλοκότητα της καθημερινότητας, προστάζει, την εξεύρεση νέων τεχνολογιών όπως αυτή του "Διαδίκτυο των πραγμάτων" (IoT). Η τεχνολογία RFID (ταυτοποίηση μέσω ραδιοσυχνοτήτων) που αποτελεί την πρώτη εφαρμογή IoT, είναι ένα καλό παράδειγμα πρακτικής εφαρμογής των IoT.

Η διευκόλυνση που προσφέρει το "Διαδίκτυο των πραγμάτων" στις καθημερινές μας δραστηριότητες, έχει οδηγήσει σε μια άνευ προηγουμένου ενσωμάτωση της παραπάνω τεχνολογίας. Η ενσωμάτωση αυτή, αποτελεί μια πρώτης τάξης ευκαιρία για κυβερνοεπιθέσεις με ευρείες επιπτώσεις, ακόμα και στο επίπεδο της φυσικής μας ασφάλειας. Όπως γίνεται κατανοητό, η ασφάλεια των αντικειμένων IoT, κρίνεται μέγιστης σημασίας.

Η διατριβή αυτή, επικεντρώνεται στην δημιουργία ενός πειραματικού περιβάλλοντος, για την εξεύρεση μιας αποδοτικής λύσης ασφάλειας IoT, έναντι επιθέσεων botnet, με την συνδυαστική χρήση των παρακάτω τεχνολογιών:

1. Εικονικές μηχανές για την εξομοίωση, τόσο των αντικειμένων IoT, όσο και του botnet,

2. Μηχανική μάθηση για την ανάλυση της δικτυακής κίνησης, από και προς, ένα δίκτυο IoT,

3. Blockchain για την αποθήκευση και διάδοση των αποτελεσμάτων της ανάλυσης της δικτυακής κίνησης των IoT.

Τα αποτελέσματα της πειραματικής διαδικασίας είναι ικανοποιητικά. Το ήδη υπάρχον λογισμικό ανοικτού κώδικα, αποδεικνύεται επαρκές για τον πειραματισμό και την μελέτη, σχετικά με την ασφάλεια IoT. Η μηχανική μάθηση φαίνεται να είναι μια πολλά υποσχόμενη τεχνολογία, που μπορεί να βοηθήσει

στην προστασία του "Διαδίκτυο των πραγμάτων" σε ικανοποιητικό επίπεδο. Τέλος, η χρήση blockchain, φαίνεται να είναι κατάλληλη ως αποθηκευτικό/ενημερωτικό μέσο, για μικρό όγκο δεδομένων, προερχόμενο από δίκτυο IoT στην περίπτωση του πειράματος.

Summary

Digital technology is the foundation for modern societies. Our survival, is almost impossible without it, as the benefits of using it are obvious. The immediacy in communication and transactions, and the easy access to information, are some of the benefits offered.

The complexity of everyday life challenges the search for new technologies such as the "Internet of Things" (IoT). RFID technology, which is the first historical application of IoT, is a good example of practical application of the technology itself.

The facility offered by the "Internet of Things" in our daily activities has led to an unprecedented incorporation of the above technology. This integration is a first- class opportunity for cyber-attacks with wide implications, even on the level of our physical security. As is understood, the safety of the IoT objects is of utmost importance.

This thesis, focuses on the creation of an experimental environment, to find a cost- effective security solution against botnets, using the following technologies:

1. Virtual machines for simulating both IoT objects and botnet,

2. Machine learning for network traffic analysis through an IoT network,

3. Blockchain for storing and communicating the results of the IoT web traffic analysis.

The results of the experimental process are satisfactory. Existing open source software, proves to be sufficient for experimentation, and study security. Machine learning seems to be a promising technology that can help in protection of "Internet of Things" at a satisfactory level. Finally, the use of blockchain, appears to be appropriate as a storage/information medium for small volume of data, derived from an IoT network.

Συντμήσεις

ACK	Acknowledgement
AI	Artificial Intelligence
ANN	Artificial Neural Network
C&C	Command & Control
CPU	Central Processing Unit
DDoS	Distributed Denial-of-Service
DNS	Domain Name System
GPU	Graphics Processing Unit
GRE IP	Generic Routing Encapsulation Internet Protocol
HTTP	HyperText Transfer Protocol
ICMP	Internet Control Message Protocol
IDS	Intrusion Detection System
IoT	Internet of Things
IP	Internet Protocol
IPS	Intrusion Prevention System
MB	Megabyte
MIT	Massachusetts Institute of Technology
MQTT	Message Queuing Telemetry Transport
RAM	Random Access Memory
RFID	Radio-Frequency Identification
SYN	Synchronize
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
VSE	Valve Source Exploit

Περιεχόμενα

Κατάλογος Σχημάτων

Κατάλογος Πινάκων

Κεφάλαιο 1
Εισαγωγή

Η τεχνολογία IoT θεωρείται ένα τεράστιο τεχνολογικό βήμα, που θα πρωταγωνιστήσει τόσο στις τεχνολογικές, όσο και στις ερευνητικές εξελίξεις στο άμεσο μέλλον. Η απεριόριστες εφαρμογές του IoT, έχουν ως αποτέλεσμα την ραγδαία ενσωμάτωση του στην σύγχρονη καθημερινότητα. Η ανάγκη των επιχειρήσεων για καινοτομία, ανάπτυξη και εξεύρεση νέων επιχειρηματικών μοντέλων, ωθούν την ταχύτατη τεχνολογική εξέλιξη του IoT.

Η σημαντικότερη παρενέργεια της ανεξέλεγκτης εξέλιξης της τεχνολογίας IoT, είναι η παράβλεψη ταυτόχρονης ανάπτυξης νεών μοντέλων ασφάλειας για αντικείμενα IoT. Η εκτεταμένη επιφάνεια επιθέσεων [1] [57] στο IoT, είναι η αχίλλειος πτέρνα σε ότι αφορά την ασφάλεια του, και αποτελεί την κύρια ανησυχία για την περεταίρω υιοθέτηση του IoT.

Καθίσταται κατανοητό, ότι η εξεύρεση αποδοτικών λύσεων ασφάλειας είναι ακρογωνιαίας σημασίας. Στην βιβλιογραφία που μελετήθηκε (έως 2019) σχετικά με την αντιμετώπιση ζητημάτων ασφάλειας, παρατηρήθηκε μια πληθώρα πειραμάτων ανάλυσης δικτυακής κίνησης IoT με τεχνικές μηχανικής μάθησης, που όμως δεν αναφέρεται στην αρχιτεκτονική πειραματικών συστημάτων, όπως επίσης, δεν αναφέρεται σε προσομοίωση πραγματικών συνθηκών οπού απαιτείται ανάλυση σε πραγματικό χρόνο. Έτσι, τα αντικείμενα μελέτης και διερεύνησης της

παρούσας διατριβής είναι:

1) Πρωτίστως, η δημιουργία ενός πειραματικού περιβάλλοντος για την μελέτη επιθέσεων σε δίκτυο IoT, και συγκεκριμένα επιθέσεων τύπου botnet.

2) Δημιουργία πειραματικού συστήματος, για την διευκόλυνση μελλοντικής έρευνας, σχετικά με αντιμετώπιση απειλών σε IoT δίκτυα.

3) Σχεδιασμός συστήματος εντοπισμού απειλών σε IoT πραγματικού χρόνου.

4) Διερεύνηση δυνατότητας χρήσης της τεχνολογίας blockchain, ως αποδοτικό αποθηκευτικό μέσο πληροφορίων σε ένα σύστημα IoT.

5) Διερεύνηση της χρήσης τεχνικών μηχανικής μάθησης, για την ανάλυση δικτυακής κυκλοφορίας σε δίκτυο IoT.

Η δομή της διατριβής έχει ως εξής:

1) Κεφάλαιο 2: Βιβλιογραφική Ανασκόπηση. Παρατίθεται η μελέτη της σχετικής βιβλιογραφίας, η οποία αποτελεί την ερευνητική βάση πάνω στην οποία θα βασιστεί η διερεύνηση των αντικειμένων μελέτης της διατριβής.

2) Κεφάλαιο 3: Γνωστικό Πλαίσιο Διατριβής. Περιέχει το απαραίτητο γνωστικό υπόβαθρο, ιδιαίτερα σημαντικό για την κατανόηση του πειραματικού σχεδιασμού. Σε αυτό περιλαμβάνεται: α) ανάλυση της τεχνολογίας IoT β) προσδιορισμός του τοπίου ασφάλειας IoT γ) εισαγωγή στην τεχνητή νοημοσύνη και στα είδη μηχανικής μάθησης δ) παρουσίαση της τεχνολογίας blockchain.

3) Κεφάλαιο 4: Πειραματικός Σχεδιασμός. Στο κεφάλαιο αυτό, γίνεται η ανάλυση του πειραματικού σχεδιασμού, καθώς και η λεπτομερής παράθεση των επιμέρους τμημάτων του πειράματος.

4) Κεφάλαιο 5: Πειραματικά Αποτελέσματα. Παρατίθενται τα πειραματικά αποτελέσματα.

5) Κεφάλαιο 6: Συμπεράσματα. Το κεφαλαίο αυτό ολοκληρώνει την διατριβή, και αναφέρονται τα συμπεράσματα του πειράματος, καθώς και προτάσεις για μελλοντικές βελτιώσεις.

Κεφάλαιο 2
Βιβλιογραφική Ανασκόπηση

Η υιοθέτηση του IoT στην καθημερινότητα μας, έρχεται με πολλαπλά οφέλη. Μερικά από αυτά, είναι η αυτοματοποίηση πολύπλοκων και τετριμμένων καθημερινών διεργασιών, η εξοικονόμηση ενέργειας, χρόνου και χρήματος, καθώς και η δημιουργία νέων επιχειρηματικών μοντέλων. Τα παραπάνω πλεονεκτήματα, η σχετική ευκολία ενσωμάτωσης, και το χαμηλό κόστος, οδηγούν σε ευρεία εφαρμογή του IoT, με τον αριθμό των συσκευών να προβλέπεται να φτάσει τα 20 δισεκατομμύρια το 2020.

Όμως, το IoT, πέρα από τα πολλαπλά και πολυδιάστατα οφέλη που προσφέρει, συνδέεται και με αρκετά προβλήματα ασφάλειας όπως: η εμπιστευτικότητα της πληροφορίας, η ιδιωτικότητα και η εμπιστοσύνη. Η μελλοντική σαρωτική υιοθέτηση του «Διαδικτύου των πραγμάτων» καταδεικνύει, τόσο την διόγκωση των προβλημάτων ασφαλείας, όσο και την δυσκολία διαχείρισης των προβλημάτων καθαυτών.

Ο σκοπός της βιβλιογραφικής ανασκόπησης, είναι ο εντοπισμός και η αξιολόγηση ερευνών, που έχουν διεξαχθεί στο πεδίο αντιμετώπισης ζητημάτων ασφάλειας του «Διαδικτύου των πραγμάτων». Πιο συγκεκριμένα, θα διερευνηθεί η ύπαρξη κοινώς αποδεκτής ορολογίας, και προσεγγίσεις σχετικές με την ταξινόμηση απειλών IoT, καθώς και η εφαρμογή τεχνικών Machine Learning -Deep Learning, για τον εντοπισμό απειλών σε IoT. Τέλος, θα διερευνηθεί το πώς έχει χρησιμοποιηθεί η τεχνολογία Blockchain, για την αντιμετώπιση προβλημάτων σε συσκευές IoT.

2.1 Ορολογία Και Ταξινόμηση IoT

Στο [16] προτείνεται ο καθορισμός μίας ενοποιημένης ορολογίας για τα υφιστάμενα, αλλά και για τα επερχόμενα αντικείμενα IoT. Οι ερευνητές μέσω του προσδιορισμού της αρχιτεκτονικής διασύνδεσης αντικειμένων IoT, δίνουν έναν ορισμό για το τί ακριβώς είναι το IoT. Σε συνέχεια του δοθέντος ορισμού, γίνεται κατηγοριοποίηση των διασυνδεδεμένων αντικειμένων βάσει: α) της πηγής ενέργειας, β) του τρόπου επικοινωνίας των αντικειμένων, γ) των λειτουργικών χαρακτηριστικών, δ) των διαθέσιμων διεπαφών των αντικειμένων για την διάδραση του χρήστη με αυτά, ε) των πόρων υλικού και λογισμικού (RAM, CPU). Τέλος, παρατίθενται παραδείγματα ταξινόμησης σύμφωνα με την παραπάνω κατηγοριοποίηση. Η χρήση κοινώς αποδεκτής ορολογίας, όπως επίσης και μιας ευρέως αποδεκτής κατηγοριοποίησης, όπως προτείνεται στην δημοσίευση, διευκολύνει στην ταξινόμηση και στη σύγκριση των IoT, σε μια κοινή βάση, και κατ' επέκταση στην ευκολότερη ταξινόμηση των δυνητικών απειλών σε IoT. Ωστόσο, εκλείπει η συστηματική κατηγοριοποίηση, βάσει των απειλών ανά κατηγορία IoT.

Η χαρτογράφηση του συνολικού τοπίου αδυναμιών που μπορεί να πλήξουν τα IoT, κρίνεται σημαντική για την αντιμετώπιση των απειλών που συνδέονται με αυτές. Στο [15] προτείνεται ταξινόμηση των απειλών σε τέσσερις κατηγορίες, βάσει του επιπέδου -της υποδομής- που πλήττουν: το επίπεδο αντικειμένων IoT, το επίπεδο μεταφοράς, το επίπεδο αποθήκευσης και το επίπεδο διεπαφής. Οι ερευνητές, παραθέτουν ένα σενάριο επίθεσης διασυνδεδεμένων

θερμοστατών, με το οποίο καταδεικνύουν τις βλάβες που μπορεί να προκληθούν σε όλα τα επίπεδα, αλλά και μέτρα μετριασμού των συνεπειών.

Στην δημοσίευση αυτή, σωστά αναφέρεται ότι σε ένα σύστημα διασυνδεδεμένων αντικείμενων IoT, προκειμένου να είναι λειτουργικό, υπάρχει καθιερωμένη «εμπιστοσύνη» μεταξύ των επιμέρους αντικειμένων. Αυτό σημαίνει ότι, αν οποιοδήποτε αντικείμενο εκτεθεί σε επιτυχημένη επίθεση, τότε όλα τα υπόλοιπα διασυνδεδεμένα αντικείμενα εκτίθενται, χάριν της μεταξύ τους

«εμπιστοσύνης». Προτείνονται κάποια μέτρα για την αντιμετώπιση απειλών, όπως «υπογραφή του λειτουργικού», και χρήση HTTPS για την αντιμετώπιση περιπτώσεων όπως, μη εξουσιοδοτημένη εγκατάσταση λειτουργικού, και αποτροπή αποκάλυψης URLs των συσκευών, από μη κρυπτογραφημένη κίνηση διαδικτύου. Τα μέτρα αυτά, ενώ προσφέρουν μία διασφάλιση πριν το επιβλαβές γεγονός, δεν προσφέρουν προστασία στην περίπτωση που κάποιο IoT έχει ήδη εκτεθεί.

2.2 AI-Deep Learning Για Τον Εντοπισμό Απειλών IoT

Η δημιουργία ψηφιακών αποτυπωμάτων -υπογραφών- και η κατηγοριοποίηση κακόβουλου λογισμικού με αυτόματο τρόπο, είναι ένας τομέας με εξαιρετικό ερευνητικό ενδιαφέρον. Οι συμβατικές μέθοδοι υπογραφής malware δεν αρκούν. Ο τεράστιος και αυξανόμενος αριθμός συσκευών που μπορεί να προσβληθεί, και ο ασταμάτητος ρυθμός εμφάνισης νέων τύπων απειλών, επιβάλουν την εύρεση αποδοτικότερων λύσεων.

Οι σύγχρονες αντιϊκές λύσεις, δεν φαίνονται να είναι αποτελεσματικές για την άμεση προστασία των χρηστών, καθώς η ενημέρωση των αντιϊκών καθαυτών είναι «χειροκίνητη», άρα χρονοβόρα διαδικασία, με την αποτελεσματικότητα των προγραμμάτων προστασίας να επαφίεται ακριβώς στην άμεση ενημέρωση τους.

Στην έρευνα [11] προτείνεται μια μέθοδος deep learning -με χρήση deep belief network (DBN)- για την δημιουργία υπογραφών, ανεξάρτητη από τα εξιδεικευμένα χαρακτηριστικά του επιβλαβούς λογισμικού, άλλα και από τροποποιήσεις στον πηγαίο κώδικα των malware. Αυτό συνεπάγεται μεγαλύτερη επιτυχία σχετικά με τον εντοπισμό κακόβουλου λογισμικού απ' ότι συμβαίνει με τα ήδη υπάρχοντα αντιϊκά προγράμματα.

Η παραπάνω προσέγγιση φαίνεται να είναι αποδοτική για συγκεκριμένες οικογένειες malware που χρησιμοποίησαν οι ερευνητές (Zeus, Carberp, SpyEye, Cidox, Andromeda και DarkComet) για την εκπαίδευση των μοντέλων κατηγοριοποίησης, αλλά, πόσο αποδοτική είναι σε κατηγόριες όπως: Conficker, CryptoWall, HackerDefender, Hiddad κ.α. Συνεπώς, υπάρχει αρκετό έδαφος για βελτίωση των μεθόδων κατηγοριοποίησης και ταξινόμησης επιβλαβούς λογισμικού.

Η έκθεση «Cisco 2017 Annual Cybersecurity Report» αναφέρει ότι το 95% των malware αρχείων που αναλύει η Cisco, είχαν μέγιστη ηλικία 24 ώρες. Ο μη άμεσος εντοπισμός νέων τύπων κακόβουλου λογισμικού, αφήνει τους χρήστες εκτεθειμένους σε ανυπολόγιστες ζημίες. Η κλασσική προσέγγιση κατηγοριοποίησης, με την δημιουργία ψηφιακής υπογραφής για κάθε malware ξεχωριστά, είναι μη αποδοτική, αφενός μεν λόγω των μεγάλου αριθμού malware αφετέρου δε, λόγω των απαιτούμενων υπολογιστικών πόρων. Η ψηφιακή αποτύπωση malware βάσει συμπεριφορικών χαρακτηριστικών, φαίνεται να αποτελεί τη λύση στα παραπάνω προβλήματα, όπως προτείνεται στο [27]. Οι ερευνητές στο πείραμα τους, χρησιμοποίησαν ένα σύνολο δεδομένων αποτελούμενο από 48 οικογένειες malware με 29.269 παραλλαγές, και για κάθε παραλλαγή, από 5 δείγματα κατά μέσο όρο. Από αυτό το σύνολο, παρήγαγαν 146.345 υπογραφές, με την παραδοσιακή μέθοδο ψηφιακής αποτύπωσης. Μετά την εφαρμογή της μεθοδολογίας τους, οι υπογραφές για τις 48 οικογένειες κακόβουλου λογισμικού, έφτασαν τις 146. Η ακρίβεια εντοπισμού επιβλαβούς λογισμικού, με μικρές τροποποιήσεις/παραλλαγές σε σχέση με το δείγμα εκπαίδευσης, ήταν επιτυχής για πάνω από το 80% των οικογενειών των πειραματικών δεδομένων, με την ακρίβεια για παραλλαγές «zero day» και πραγματικά «zero day» (πραγματικά είναι αυτά για τα οποία δεν υπάρχει υπογραφή) να είναι λιγότερο από 70% και 30% αντίστοιχα.

Η ερευνητική υπόθεση στο [27] είναι, ότι η χρήση συμπεριφορικών χαρακτηριστικών για την δημιουργία ψηφιακής αποτύπωσης malware, είναι αποδοτική σε όρους υπολογιστικών πόρων, αλλά και ταχύτητας εντοπισμού απειλών. Η έρευνα αυτή πράγματι, δείχνει σημαντική διαφορά, τόσο στους απαιτούμενους πόρους συστήματος -απαιτούνται λιγότεροι- όσο και στην ταχύτητα εντοπισμού malware, στα υποκείμενα, σε απειλές συστήματα, με την χρήση της προτεινόμενης μεθοδολογίας. Ωστόσο, η εν λόγω έρευνα, κάνει ελάχιστες αναφορές για εφαρμογή σε IoT. Η πρακτική ενσωμάτωση της ανωτέρω κατηγοριοποίησης απειλών, παρουσιάζεται ιδιαίτερα ωφέλιμη σε ότι αφορά την εξοικονόμηση υπολογιστικών πόρων σε IoT αντικείμενα.

2.3 Blockchain Και IoT

Η τεχνολογία Blockchain είναι πιο δημοφιλής από ποτέ. Ο λόγος για την τόσο μεγάλη δημοτικότητα, είναι μια συγκεκριμένη εφαρμογή του, τα κρυπτονομίσματα και τα δυνητικά κέρδη σε όσους επενδύουν σε αυτά, με το Bitcoin να ηγείται. Στην ουσία του το blockchain, είναι μια κατανεμημένη δομή δεδομένων -distributed data structure- όπου αντιγράφεται και διανέμεται στα μέλη ενός δικτύου. Αυτή η δομή, λειτουργεί ως ένα αρχείο, στο οποίο παρατίθενται χρονολογικά, συναλλαγές που έχουν πραγματοποιηθεί από τα μέλη του δικτύου. Το ποιο σημαντικό χαρακτηριστικό του Blockchain, είναι η αδιάβλητη φύση του, ήτοι, οι καταχωρήσεις στο αρχείο καταγραφής συναλλαγών δεν μπορούν να τροποποιηθούν.

Η αξία των κρυπτονομισμάτων, μπορεί στο μέλλον να φθίνει, αλλά η αξία του Blockchain είναι αδιαμφισβήτητη. Η εγγενής ασφάλεια, καθώς και η κατανεμημένη αρχιτεκτονική του, κάνουν αυτήν την τεχνολογία κατάλληλη, για μια πληθώρα εφαρμογών, που απαιτούν ασφαλή διάδραση/συναλλαγές σε μη ασφαλή δίκτυα, όπου στα μέλη τους, η μεταξύ τους εμπιστοσύνη, δεν είναι δεδομένη.

Στην δημοσίευση [10] δίνεται ορισμός του Blockchain, και εξήγηση του τρόπου λειτουργείας του. Στην συνέχεια, αναφέρονται διάφορα σενάρια εφαρμογής του σε IoT: αναβάθμιση

λογισμικού IoT, εκμετάλλευση του Blockchain δικτύου για την δημιουργία αγοράς υπηρεσιών μεταξύ IoT αντικειμένων, και πληρωμές μέσω κρυπτονομισμάτων, παρακολούθηση διαμετακόμισης εμπορευμάτων με καταγραφή των ενδιάμεσων σταθμών μεταφοράς τους σε Blockchain κα. Τέλος οι ερευνητές, αναφέρονται σε ζητήματα που άπτονται της δυσκολίας εφαρμογής του Blockchain σε IoT, αλλά και σε τρόπους αντιμετώπισης των δυσκολιών αυτών.

Στην παραπάνω δημοσίευση, σκιαγραφείται το τοπίο Blockchain, ως προς το πώς μπορεί να βοηθήσει στην ασφάλεια των IoT, να διευκολύνει την διαμοίραση πόρων και υπηρεσιών, αλλά και να αυτοματοποιήσει με κρυπτογραφικό τρόπο χρονοβόρες ρουτίνες. Ωστόσο, δεν γίνεται αναφορά σε εφαρμογές της τεχνολογίας Blockchain σε περιπτώσεις όπως, εκμετάλλευση αδυναμιών IoT, και τρόποι περιορισμού ζημίας σε ένα δίκτυο αντικειμένων IoT.

Στο άρθρο [33] εκτίθενται απόψεις, σχετικά με ποιους τρόπους η τεχνολογία Blockchain μπορεί να ενισχύσει την ασφάλεια των IoT. Μέσα από αρκετά παραδείγματα πρακτικής εφαρμογής του Blockchain σε IoT, γίνεται σαφές, ότι στο άμεσο μέλλον, θα διαδραματίσει πρωταγωνιστικό ρόλο σε ότι αφορά την ασφάλεια, σε όλο το φάσμα του τεχνολογικού τοπίου. Η εφαρμογή του Blockchain σε περιπτώσεις όπως, IBM Watson IoT, Provenance [1], Filament [2] κ.α. αποδεικνύει, το ζωηρό ενδιαφέρον, τόσο της ενσωμάτωσης της προαναφερθείσας τεχνολογίας στο «Διαδίκτυο των Πραγμάτων» όσο και στην δημιουργία νέων οικονομιών.

Εν συνεχεία ο αρθρογράφος, αναφέρεται στις προκλήσεις που το Blockchain δύναται να αντιμετωπίσει. Τις κατατάσσει σε τέσσερις ομάδες: α) Αύξηση ζήτησης χωρητικότητας δικτύου και συνοδευόμενου κόστους, λόγω αύξησης των συσκευών IoT, β) Μη αποδοτική αρχιτεκτονική IoT, γ) Προβλήματα διαθεσιμότητας υπηρεσιών και δικτύου, δ) Ζητήματα κακόβουλης χειραγώγησης της πληροφορίας που διέρχεται των IoT αντικειμένων. Το άρθρο αποτελεί μία αισιόδοξη ματιά, σε ότι αφορά την χρήση Blockchain, για την ενίσχυση της

[1] https://www.provenance.org/
[2] https://filament.com/

ασφάλειας στο «Διαδίκτυο των Πραγμάτων». Όμως, δεν θα πρέπει να θεωρηθεί πανάκεια. Υπάρχουν ακόμα προβλήματα που πρέπει να λυθούν, όπως για παράδειγμα, εύρεση ασφαλών τρόπων αποθήκευσης διαπιστευτηρίων ειδικά για IoT συστήματα που διαχειρίζονται περιουσιακά αγαθά, αλλά και καθορισμός διαδικασίας αντιστροφής, μιας επαληθευμένης Blockchain συναλλαγής.

2.4 IOTA Και IoT

Η ενσωμάτωση τεχνολογιών «distributed ledger» [40] για την ενίσχυση της ασφάλειας των IoT αντικειμένων, είναι ένας τομέας με ενεργό ερευνητικό ενδιαφέρον. Οι αδυναμίες των ήδη υπαρχουσών τεχνολογιών, οδηγούν, τόσο στην εξέλιξή τους, όσο και στην εξεύρεση νέων λύσεων. Η εξέλιξη σε ότι αφορά την τεχνολογία Blockchain, είναι αναπόφευκτη. Για παράδειγμα, η χρήση του Bitcoin [41] σε IoT, συνδέεται με μειονεκτήματα λόγω της λειτουργικής του φύσης. Ένα πολύ σημαντικό μειονέκτημα είναι ότι, κάθε συναλλαγή στην υποδομή Bitcoin, ανεξάρτητα της αξίας της, επιβαρύνεται με έξοδα συναλλαγής. Το κοστολογικό αυτό μοντέλο δεν είναι βιώσιμο, για τον λόγο ότι η αξία συναλλαγής μεταξύ IoT αντικειμένων, τις περισσότερες φορές, θα είναι μικρότερης αξίας από τα έξοδα της ίδιας της συναλλαγής.

Μια ιδιαίτερα ενδιαφέρουσα τεχνολογία, που υπόσχεται να λύσει τα προβλήματα του Blockchain, και προσδιορίζεται ως το «Κρυπτονομίσματα των IoT» είναι το IOTA [34]. Η κύρια διαφορά του με το Blockchain, είναι ότι μια συναλλαγή στο IOTA δίκτυο δεν χρειάζεται «ενδιάμεσους» -miners [7]- για να επιβεβαιώσουν την ορθότητα των συναλλαγών (η απαραίτητη ύπαρξη της εργασίας των miners επιφέρει κοστολογική επιβάρυνση σε κάθε συναλλαγή). Η ενσωμάτωση μιας νέας συναλλαγής στο δίκτυο IOTA, απαιτεί τον έλεγχο και την επιβεβαίωση δύο έτερων συναλλαγών. Η διεργασία ενσωμάτωσης, καθώς και τα στοιχεία της νέας συναλλαγής, δημιουργούν μια αδιάβλητη δέσμη πληροφορίας. Η πληροφορία αυτή, αποτελεί το σύνολο της νέας συναλλαγής που αποθηκεύεται στο δίκτυο IOTA, και η οποία έπειτα θα χρησιμοποιηθεί για την επιβεβαίωση επόμενων συναλλαγών.

Ο διαφορετικός σχεδιασμός του IOTA (μη χρήση τεχνολογίας Blockchain), ακριβώς επειδή δεν απαιτεί «Μπλοκ» και miners για την επικύρωση των συναλλαγών, αλλά απαιτεί μόνο την επιβεβαίωση δύο έτερων συναλλαγών, σημαίνει την ταχύτατη διεκπεραίωση των συναλλαγών καθαυτών, πράγμα πολύ σημαντικό για την λειτουργία του IoT. Η ταχύτητα αυτή θα αυξάνει, καθώς θα προστίθενται νέες συναλλαγές στο δίκτυο IOTA.

Στον αντίποδα των πλεονεκτημάτων, υπάρχουν μειονεκτήματα, που συνδέονται περισσότερο με το ότι η τεχνολογία αυτή είναι σχετικά νέα, παρά με την μη σωστή υλοποίηση της. Στο [60] ο αρθρογράφος υποστηρίζει ότι η ασφάλεια του IOTA είναι τρωτή, στην περίπτωση που κάποιος επιτιθέμενος κατέχει το 33% της ισχύος κατακερματισμού του δικτύου. Αυτό έχει ως συνέπεια, το IOTA να είναι ευάλωτο σε επιθέσεις «hash power attack» - ανάλογη ευαλωτότητα υφίσταται και σε δίκτυα της οικογένειας Blockchain [8]. Ο οργανισμός IOTA το αναγνωρίζει, και υποστηρίζει ότι η συγκεκριμένη αδυναμία θα εξαλειφθεί, όταν στο δίκτυο προστεθούν συναλλαγές. Για να αντιμετωπισθεί αυτή η τρωτότητα σε αυτό το πρώιμο στάδιο, επιτελούνται ειδικού τύπου συναλλαγές από τον ίδιο τον οργανισμό, μέσω αυτόματης διεργασίας, προκειμένου να αυξηθεί ο όγκος του δικτύου, πράγμα που θα σημαίνει, προστασία από επιθέσεις του προαναφερθέντα τύπου. Από το σημείο που το δίκτυο θα είναι ασφαλές, η διεργασία εκτέλεσης «ειδικού τύπου» συναλλαγών θα παροπλισθεί. Το ερώτημα που ανακύπτει λοιπόν είναι, το πόσο αποκεντρωμένο είναι το IOTA, από την στιγμή που οι πρώτες συναλλαγές εκτελούνται κεντρικά από τον ίδιο τον οργανισμό που συντηρεί την υποδομή IOTA.

Η υποδομές κατανεμημένου καθολικού [12] που βασίζονται στο Blockchain έχουν αδυναμίες. Οι βασικότερες, σχετίζονται με την ταχύτητα διεκπεραίωσης συναλλαγών, και το κόστος εκτέλεσης αυτών. Ωστόσο, είναι δοκιμασμένες για την ασφάλεια τους σε πραγματικές συνθήκες, με πολλές και διαφόρων ειδών υλοποιήσεις, σε ποικίλους τομείς. Επιπροσθέτως, είναι πραγματικά «αποκεντρωμένης» αρχιτεκτονικής. Τα παραπάνω μειονεκτήματα του IOTA, δείχνουν ότι η ενσωμάτωση του στο IoT, ενδέχεται να δημιουργήσει περισσότερα προβλήματα από αυτά που υπόσχεται να λύσει.

2.5 Blockchain Αντί Παραδοσιακών Βάσεων Δεδομένων

Γιατί η χρήση υποδομής κατανεμημένου καθολικού, είναι προτιμότερη από την χρήση παραδοσιακών βάσεων δεδομένων στο IoT; Παρατηρούμε τα τελευταία χρόνια, ραγδαία εξέλιξη στις υποδομές νέφους. Τα οφέλη [24] της νεφοϋπολογιστικής (cloud computing) είναι πολλά: χαμηλό κόστος, παράλληλη επεξεργασία, επεκτασιμότητα, ασφάλεια κ.α. Σε ότι αφορά τις βάσεις δεδομένων σε υποδομή νέφους, θα πρέπει να αναφέρουμε ένα σημαντικό πλεονέκτημα τους, την ανά πάσα στιγμή διαθεσιμότητα τους, ιδιαίτερα χρήσιμο χαρακτηριστικό, όταν αφορά χρήση αποθηκευτικού μέσου σε IoT.

Ωστόσο, οι παραδοσιακές βάσεις δεδομένων στο νέφος, ενώ προσφέρουν ουσιώδη πλεονεκτήματα, δεν είναι το καταλληλότερο μέσο αποθήκευσης σε υλοποιήσεις IoT. Οι λόγοι συνοψίζονται παρακάτω:

- Στις παραδοσιακές βάσεις δεδομένων, η αποθήκευση των δεδομένων, ο έλεγχος και η συντήρηση τους, επιτελείται "κεντρικά", σε αντίθεση με τις κατανεμημένες. Ο "κεντρικός" έλεγχος μπορεί να αποβεί καταστροφικός στην περίπτωση εκμετάλλευσης αδυναμίας του συστήματος,

- Η ακεραιότητα και η διαφάνεια, είναι κύρια εγγενή χαρακτηριστικά των κατανεμημένων βάσεων δεδομένων. Κάθε χρήστης μπορεί να είναι σίγουρος ότι τα δεδομένα σε μια κατανεμημένη βάση, είναι αναλλοίωτα, και μπορεί να επαληθεύει οποιαδήποτε συναλλαγή ανά πάσα στιγμή.

- Οι παραδοσιακές βάσεις, επιτρέπουν λειτουργείες δημιουργίας, ανάγνωσης, ενημέρωσης και διαγραφής δεδομένων "εκ σχεδιασμού", ενώ οι κατανεμημένες, επιτρέπουν λειτουργίες δημιουργίας και ανάγνωσης μόνο.

2.6 Σύνοψη

Από την παρατεθείσα βιβλιογραφία, παρατηρείται έντονο ενδιαφέρον της επιστημονικής κοινότητας σε ότι αφορά το IoT, αλλά και στα ζητήματα ασφάλειας που ανακύπτουν από την εφαρμογή του. Η ενσωμάτωση του Blockchain στα IoT για την ενίσχυση της ασφάλειας τους είναι πολλά υποσχόμενη, και κατά συνέπεια αποτελεί πρόσφορο έδαφος σε νέες ιδέες και προσεγγίσεις.

Από την σχετική βιβλιογραφία, παρατηρούμε ότι υπάρχει κενό αναφορικά με την συνδυαστική ενσωμάτωση IoT, Blockchain και Machine Learning για την προστασία του πρώτου από απειλές.

Ειδικότερα, τα ερωτήματα που ανακύπτουν είναι:

1) Είναι υπαρκτή η ανάγκη περεταίρω κατηγοριοποίησης των IoT βάσει απειλών;

2) Ποια τα μέτρα αντιμετώπισης στην περίπτωση επιτυχούς επίθεσης σε ένα, ή και περισσότερα αντικείμενα IoT, προκειμένου να περιοριστεί η απειλή;

3) Πόσο, και με ποιες προσεγγίσεις, μπορεί να βελτιωθούν οι μηχανισμοί ανίχνευσης απειλών στο «Διαδίκτυο των πραγμάτων» σε ότι αφορά την έγκαιρη ενημέρωση τους με νέους τύπους απειλών, αλλά και στην επιτυχία ανίχνευσης;

4) Λαμβάνοντας υπόψιν τους περιορισμένους υπολογιστικούς πόρους των IoT, υπάρχουν βέλτιστες προσεγγίσεις -σε όρους υπολογιστικών πόρων- για τον εντοπισμό απειλών;

5) Είναι δόκιμη η χρήση Blockchain για την προστασία δικτύου IoT και αν ναι, με ποιους τρόπους μπορεί να υλοποιηθεί μια βιώσιμη λύση;

Η έρευνα έχει ως στόχο, την εύρεση μιας ολιστικής λύσης εντοπισμού απειλών, και πρόληψης εξάπλωσης τους σε δίκτυο IoT με την βοήθεια τεχνολογίας Blockchain. Για την υλοποίηση θα πρέπει:

- Να βελτιωθούν οι ήδη υπάρχοντες τρόποι εντοπισμού απειλών, με τεχνικές Machine Learning.

- Να μελετηθεί το Blockchain, για την εξεύρεση τρόπου χρήσης του για την ασφάλεια των IoT.

- Να χρησιμοποιηθεί η απλούστερη, και πιο αποδοτική αρχιτεκτονική ενσωμάτωσης.

Κεφάλαιο 3
Γνωστικό Πλαίσιο Διατριβής

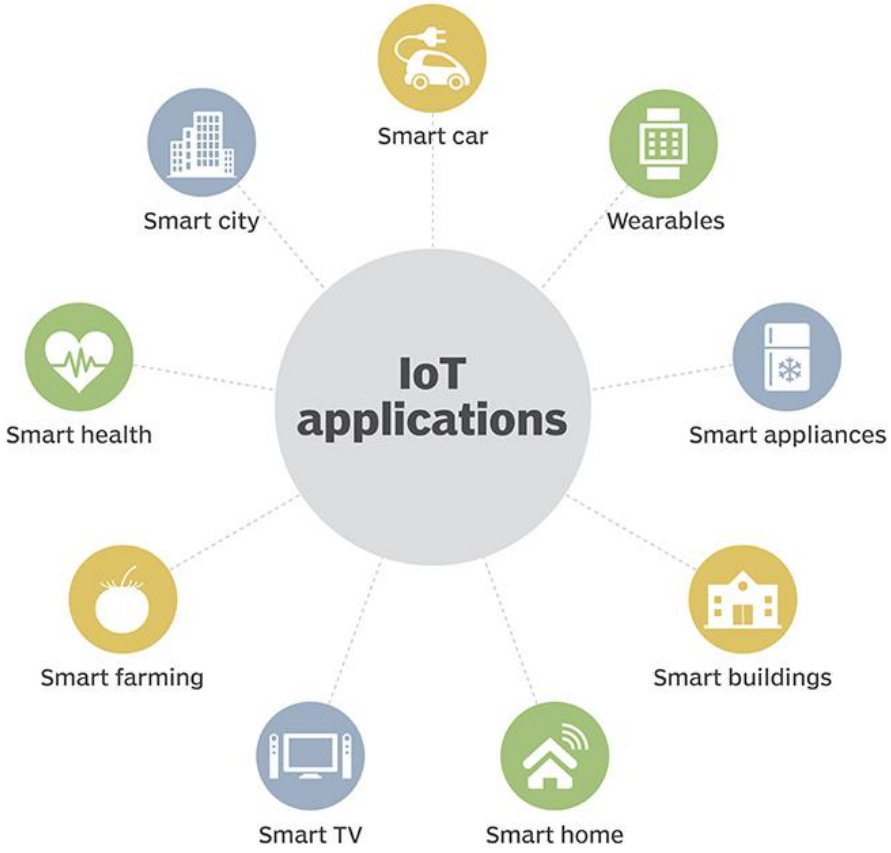
Για την καλύτερη κατανόηση της διατριβής, είναι απαραίτητη η παρουσίαση του τεχνολογικού υπόβαθρου, και εν γένει των επιμέρους τεχνολογικών επιλογών, που συνθέτουν το πειραματικό τμήμα της διατριβής. Έτσι, στο κεφάλαιο αυτό θα αναλυθούν:

- Η τεχνολογία IoT.
- Οι σχετικές με το IoT απειλές.
- Η τεχνολογία μηχανικής μάθησης.
- Η τεχνολογία blockchain (τεχνολογία κατανεμημένης εγγραφής)

3.1 Η Τεχνολογία IoT

Το IoT (Διαδίκτυο των Πραγμάτων), αναφέρεται στα αντικείμενα που είναι διασυνδεδεμένα στο διαδίκτυο. Πιο συγκεκριμένα, το IoT αναφέρεται σε ετερόκλιτα διασυνδεδεμένα αντικείμενα, με δυνατότητα μεταφοράς δεδομένων χωρίς ανθρώπινη παρέμβαση [19]. Επί της ουσίας, το IoT επιτρέπει σε συσκευές ενός δικτύου (κλειστού ή μη) να επικοινωνούν με άλλες συσκευές -οιουδήποτε τύπου- στο ίδιο ή έτερο δίκτυο. Τα διασυνδεδεμένα αυτά αντικείμενα, μπορεί να είναι συστήματα αυτοματισμού οικίας, φορητά συστήματα και αντικείμενα, φορητά συστήματα παρακολούθησης υγείας, αισθητήρες κίνησης σε οχήματα κ.α. Βλέπουμε επιτυχημένη εφαρμογή της παραπάνω τεχνολογίας, σε καταναλωτικά αγαθά

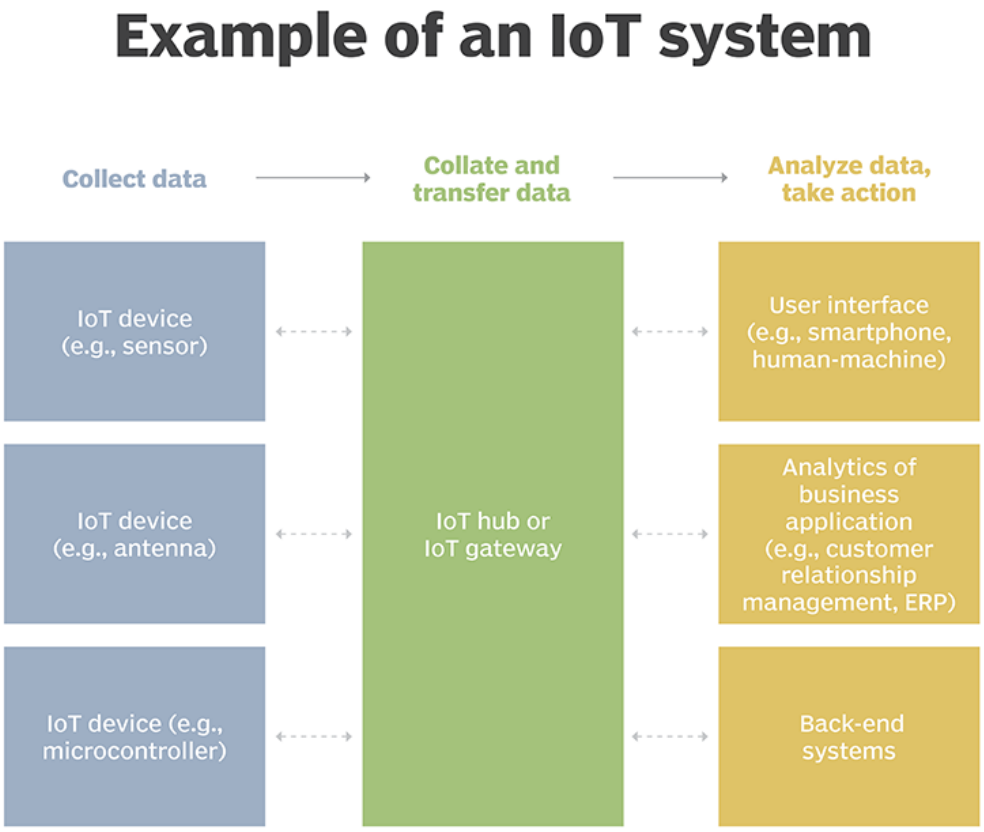
και υπηρεσίες [43], στον τομέα της υγείας, στις μεταφορές και την επικοινωνία, καθώς επίσης σε βιομηχανικές εφαρμογές (Σχήμα 3.1 σελίδα 15).



Σχήμα 3.1: Εφαρμογές IoT.

Το σχετικά χαμηλό κόστος και η ευκολία ενσωμάτωσης του IoT, οδηγούν ολοένα και περισσότερες εταιρείες και οργανισμούς στην χρήση IoT, με στόχο την μείωση του

λειτουργικού κόστους, την αύξηση της ποιότητας των προσφερόμενων υπηρεσιών, αλλά και την δημιουργία νέων επιχειρηματικών μοντέλων (Σχήμα 3.2 σελίδα 16).



Σχήμα 3.2: Παράδειγμα συστήματος IoT.

3.1.1 Απαρχή του IoT

Ο όρος Internet of Things πρωτοεμφανίστηκε το 1999 [58] από τον Kevin Ashton, σε παρουσίαση του στην στη εταιρεία P&G [58]. Ιστορικά, το πρώτο IoT Αντικείμενο, ήταν ένας αυτόματος πωλητής Coca Cola [3] στο πανεπιστήμιο Carnegie Mellon University.

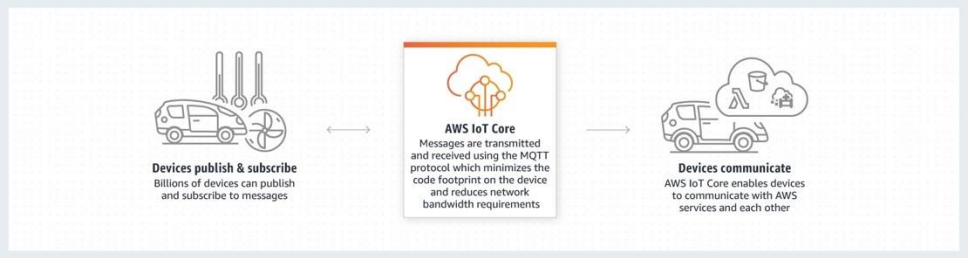
[3] https://www.cs.cmu.edu/~coke/history_long.txt

Απομακρυσμένοι χρήστες μπορούσαν να δουν την διαθεσιμότητα, αλλά και την θερμοκρασία των αναψυκτικών του αυτόματου αυτού πωλητή. Το 1990 ο John Romkey, δημιούργησε την πρώτη συσκευή -τοστιέρα- που έδινε την δυνατότητα στον χρήστη να την ελέγχει μέσω διαδικτύου [56]. Ένα από τα μεγαλύτερα βήματα προς την εκτεταμένη αποδοχή της νέας αυτής τεχνολογίας, ήταν η ανακοίνωση ευρείας εμπορικής διάθεσης "έξυπνου ψυγείου", από την εταιρεία LG. Το ψυγείο αυτό, μπορούσε να "δει" αν τα αποθηκευμένα τρόφιμα χρειάζονταν αναπλήρωση.

3.1.2 Λειτουργεία

Ένα IoT αντικείμενο έχει ενσωματωμένο επεξεργαστή, αισθητήρες αλλά και "εξοπλισμό", για την συλλογή, επεξεργασία και αποστολή των δεδομένων που συλλέγει, με την βοήθεια των αισθητήρων του.

Τα αντικείμενα IoT, μοιράζονται τις συλλεχθείσες πληροφορίες, με αρκετούς τρόπους. Ένας τρόπος, είναι η διασύνδεση των αντικειμένων σε εξειδικευμένες IoT πλατφόρμες, όπως την Amazon IoT [4] (Σχήμα 3.3 σελίδα 17). Άλλος τρόπος, είναι η αποστολή δεδομένων σε μια κεντρική συσκευή, με την χρήση πρωτόκολλων επικοινωνίας χαμηλών απαιτήσεων, όπως το MQTT. Έπειτα, τα δεδομένα αυτά, είτε αναλύονται τοπικά, είτε προωθούνται σε πλατφόρμες υπολογιστικής νέφους.



Σχήμα 3.3: Amazon IoT.

[4] https://aws.amazon.com/iot/

Πέρα όμως από την σύνδεση των IoT με εξειδικευμένες πλατφόρμες, ή με ένα κεντρικό μέσο, τα αντικείμενα καθαυτά μπορούν να επικοινωνούν μεταξύ τους, και ενεργούν βάσει των ανταλλασσόμενων πληροφοριών. Έτσι, πραγματοποιούν εργασίες χωρίς ανθρώπινη παρέμβαση. Για παράδειγμα, ένα "έξυπνο" θερμόμετρο, μπορεί να ενεργοποιήσει τον κλιματισμό ενός χώρου, υπολογίζοντας τον αριθμό των ατόμων που βρίσκονται σε αυτό, χωρίς καμία απολύτως παρέμβαση.

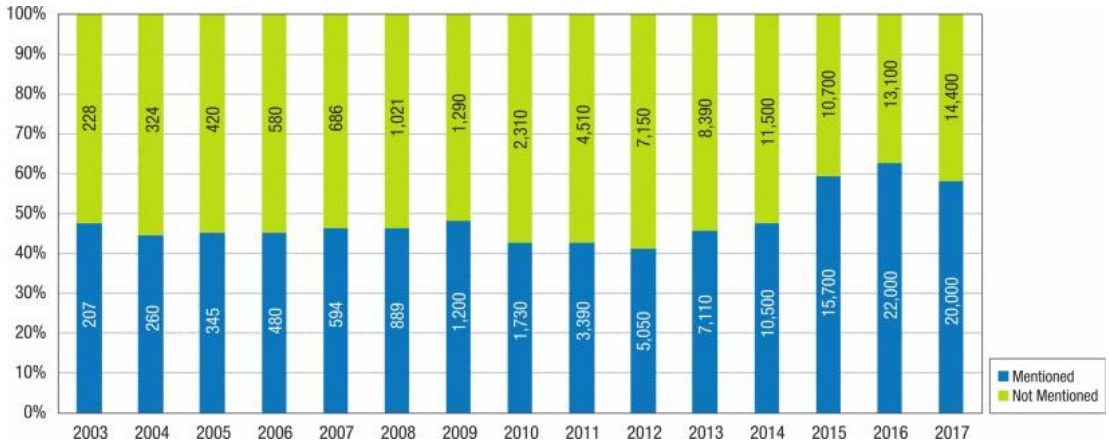
3.1.3 Το Μέλλον

Η εξέλιξη του Διαδικτύου των Πραγμάτων, προβλέπεται να είναι πολυεπίπεδη και σαρωτική. Οι τεχνολογικές εξελίξεις, θα επιτρέψουν ακόμα μεγαλύτερη διείσδυση της τεχνολογίας, με θετικές οικονομικές και κοινωνικές επιπτώσεις. Ωστόσο, ο αριθμός των IoT αντικειμένων που υπάρχει σήμερα είναι μικρός, αν αναλογιστούμε τον αριθμό των καθημερινών αντικειμένων που μπορούν να "μετατραπούν" σε IoT [36]. Με αυτό το σκεπτικό, βλέπουμε ότι έχουμε τεράστιο χώρο για έρευνα και εξέλιξη στο επίπεδο της αρχιτεκτονικής, των πρωτοκόλλων επικοινωνίας, των εφαρμογών, της ασφάλειας, της προστασίας, της ιδιωτικότητας, και μελλοντικών εφαρμογών της εν λόγω τεχνολογίας [32].

3.2 Ασφάλεια Και IoT

Ο τεράστιος διασυνδεδεμένος αριθμός IoT αντικειμένων στο διαδίκτυο, εκθέτει έναν τεράστιο όγκο δεδομένων. Όπως γίνεται κατανοητό, αυτή η τεράστια έκθεση, αποτελεί την αχίλλειο πτέρνα των IoT. Η δυνητική ζημία σε ασφάλεια, αλλά και ιδιωτική ζωή, είναι τεράστια και μη μετρήσιμη. Οι επιθέσεις του Mirai botnet το 2016 στον πάροχο νεφοϋπολογιστικής υποδομής OVH, καθώς και η επίθεση στην εταιρεία Dyn το ίδιο έτος, δείχνουν ξεκάθαρα το επίπεδο ευαλωτότητας, και το μέγεθος της ζημίας που μπορεί να προκληθεί στο IoT [31].

Το ερευνητικό ενδιαφέρον για την ασφάλεια του IoT, είναι αυξανόμενο. Το κύριο ερευνητικό βάρος, δίνεται στους τομείς αρχιτεκτονικής ασφάλειας, εντοπισμός εισβολής, δικανική, ιδιωτικότητα, ασφάλεια επικοινωνίας μεταξύ άλλων [49] (Σχήμα 3.4 σελίδα 19).



Σχήμα 3.4: Internet of things (IoT) research articles that explicitly mention the term "security".

3.2.1 Τοπίο Ασφάλειας IoT

Οι στόχοι για την ασφάλεια του IoT μπορούν να συνοψισθούν: στην εμπιστευτικότητα, την ακεραιότητα και την διαθεσιμότητα των δεδομένων -CIA [45]. Οτιδήποτε μπορεί να απειλήσει τις παραπάνω "περιοχές" ασφάλειας, μπορεί να προκαλέσει σοβαρή βλάβη στο σύστημα IoT.

Με γνώμονα τους παραπάνω στόχους, παρατηρούμε απειλές σε πολλαπλά επίπεδα. Αναλυτικότερα, στο επίπεδο εφαρμογής βλέπουμε:

- Επίθεση κακόβουλου κώδικα, malicious code injection, ο κακόβουλος χρήστης εισάγει στο σύστημα κακόβολο λογισμικό για την υποκλοπή ή/και των χειρισμό των δεδομένων του ανυποψίαστου χρήστη.

- Επίθεση DDoS - Denial of service attack, ο κακόβουλος χρήστης διακόπτει την κανονική λειτουργεία του συστήματος. Θεωρείται η μεγαλύτερη ευπάθεια του συστήματος.

- Επίθεση Phishing, ο κακόβουλος χρήστης, μέσω ηλεκτρονικού ταχυδρομείου, αποσπά από το ανυποψίαστο θύμα ευαίσθητες πληροφορίες, όπως, συνθηματικά χρήστη, αριθμούς πιστωτικών καρτών κ.α.

- Επίθεση Sniffing, ο κακόβουλος χρήστης, με την χρήση ειδικού λογισμικού, διαβάλει την δικτυακή κίνηση του θύματος, με σκοπό την απόσπαση ευαίσθητων πληροφορίων ή/και την διακοπή επικοινωνίας/συνδεσιμότητας του συστήματος του θύματος.

Έπειτα παρατηρούμε προβλήματα σχετικά με την ασφάλεια:

- Η πιστοποίηση της ταυτότητας σε ένα σύστημα IoT, μπορεί να αποτελέσει μεγάλο πρόβλημα, καθώς ο τεράστιος αριθμός αντικειμένων/χρηστών, μπορεί να "κρύψει" την είσοδο κακόβουλου χρήστη.

- Η διαχείριση τεράστιου όγκου δεδομένων. Οι υπάρχουσες υποδομές διαχείρισης δεδομένων δεν επαρκούν. Η ανεπάρκεια αυτή, μπορεί να οδηγήσει σε απώλεια ή/και την υποκλοπή δεδομένων, κατά την διάρκεια της διαδικασίας επικοινωνίας IoT αντικειμένων.

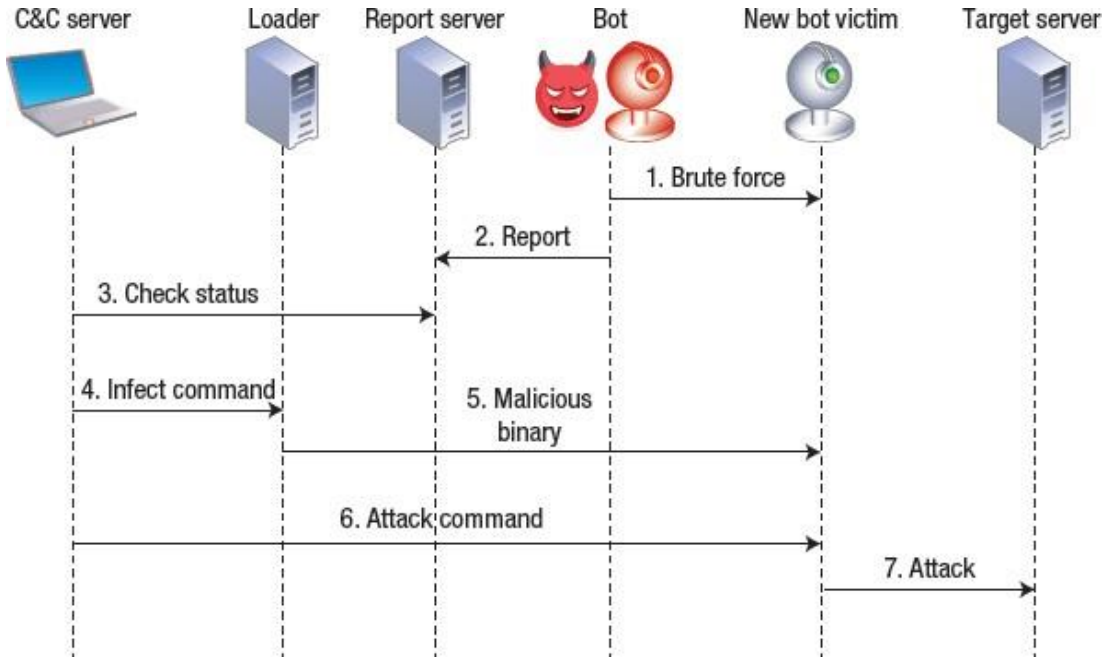
- Η αποθήκευση και η ανάκτηση δεδομένων, μπορεί να αποδειχθεί προβληματική στην κλίμακα μεγέθους των δικτύων IoT, αν λάβουμε υπόψιν ότι, τόσο κατά στην αποθήκευση, όσο και κατά την ανάκτηση τους, θα πρέπει να υπάρχουν αποδοτικοί μηχανισμοί, που να διασφαλίζουν το απόρρητο των χρηστών, και την ακεραιότητα των δεδομένων καθαυτών.

- Οι ευπάθειες λογισμικού. Το "κακογραμμένο" λογισμικό, είναι μια συνηθισμένη ευπάθεια, όπου ο κακόβουλος χρήστης, μπορεί να εκμεταλλευτεί για την επίτευξη επιθέσεων.

Βλέπουμε λοιπόν, ότι ο "χάρτης" ασφάλειας του IoT είναι αχανής [57]. Για τους σκοπούς όμως της παρούσας διατριβής, θα επικεντρώσουμε σε μια οικογένεια απειλών IoT, στα botnets.

3.2.2 Botnets

Ο σκοπός διακύβευσης αντικειμένων IoT, είναι η συμπερίληψη τους σε ένα botnet. Το botnet είναι ένα δίκτυο υπολογιστών, το οποίο αποτελείται από "μολυσμένες" συσκευές, οι οποίες ελέγχονται από κακόβουλο λογισμικό (Σχήμα 3.5 σελίδα 21).



Σχήμα 3.5: Botnet actions flow.

Οι κυβερνοεγκληματίες χρησιμοποιούν ειδικό λογισμικό, για την παράκαμψη συστημάτων ανίχνευσης, και πρόληψης εισβολών συνδεδεμένων συσκευών. Έτσι, επιτυγχάνουν μη εξουσιοδοτημένη πρόσβαση, και έλεγχο των συσκευών, τις οποίες "εντάσσουν" στο δίκτυο botnet. Ο έλεγχος του botnet επιτελείται από απόσταση [46]. Ενώ αρχικά τα botnets

αποτελούνταν από μολυσμένους προσωπικούς υπολογιστές, το μηδενικό επίπεδο ασφάλειας των δικτύων IoT, αποτέλεσε πρόσφορο έδαφος για κυβερνοεπιθέσεις. Οι μεγαλύτερες σύγχρονες επιθέσεις botnet, πραγματοποιήθηκαν από botnets που αποτελούνταν κυρίως από IoT αντικείμενα. Τα botnets χρησιμοποιούνται για την υποκλοπή δεδομένων, για την απομακρυσμένη πρόσβαση και έλεγχο συσκευών, για ην αποστολή ανεπιθύμητων μηνυμάτων, αλλά και για "κατανεμημένη επίθεση άρνησης εξυπηρέτησης" DDoS.

3.2.3 Mirai Botnet

Το botnet που χρησιμοποιείται κατά το πείραμα της παρούσας διατριβής, είναι το Mirai Botnet [31]. Το κακόβουλο αυτό λογισμικό, αποτελείται από τα παρακάτω μέρη:

- Το bot. Είναι υπεύθυνο για την μετάδοση του κακόβουλου λογισμικού, και για την αρχικοποίηση επίθεσης, μόλις λάβει εντολή από το άτομο που ελέγχει το δίκτυο bot.

- Τον διακομιστή εντολών και ελέγχου (C&C). Υπεύθυνο για τον κεντρικό έλεγχο και διαχείριση του botnet, καθώς και για την ενορχήστρωση νέων DDoS επιθέσεων.

- Τον "φορτωτή" -loader. Υπεύθυνο για την διάδοση των κακόβουλων εκτελέσιμων αρχείων σε νέα θύματα.

- Τον διακομιστή αναφοράς -report server. Υπεύθυνο για την διατήρηση βάσης δεδομένων για όλα το bot στο δίκτυο.

Το Mirai σαρώνει τυχαία δημόσιες IP διευθύνσεις στις πόρτες 23 και 2323. Σκόπιμα αποκλείονται ορισμένες διευθύνσεις, όπως αυτή του Department of Defense, προφανώς για την αποφυγή προσέλκυσης προσοχής από μεγάλους κρατικούς οργανισμούς, οι οποίοι θα μπορούσαν να καταστείλουν μια επιτυχημένη επίθεση.

Τα βήματα επίθεσης που ακολουθεί το Mirai είναι:

- Το bot δοκιμάζει διαπιστευτήρια (username-password) από συγκεκριμένη λίστα, σε πλημμελώς προστατευμένες IoT συσκευές.

- Μόλις το bot εντοπίσει τα σωστά διαπιστευτήρια, και διεισδύσει στο IoT αντικείμενο, μεταδίδει τα χαρακτηριστικά της συσκευής στον διακομιστή αναφοράς.

- Έπειτα, μέσω του διακομιστή εντολών και ελέγχου, ελέγχει για πιθανά νέα θύματα.

- Αφού αποφασιστεί ποιες συσκευές θα μολυνθούν, ο διαχειριστής του κακόβουλου δικτύου, δίνει εντολή στον "φορτωτή" για μόλυνση νέων συσκευών.

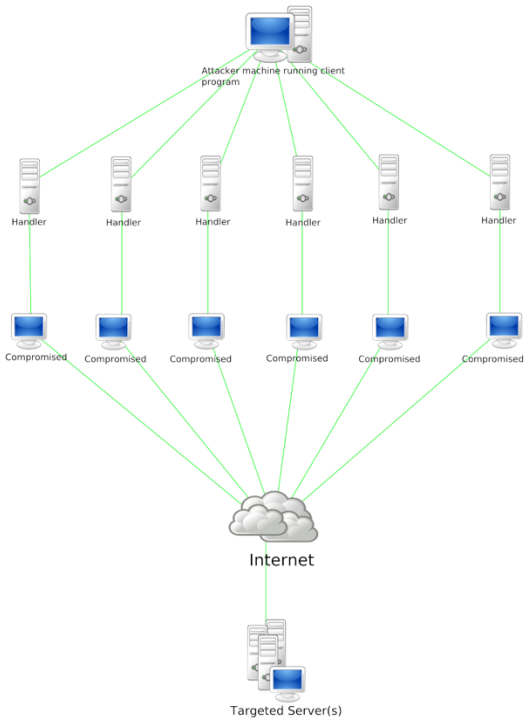
- Ο "φορτωτής" συνδέεται με την νέα συσκευή θύμα, και δίνει εντολή κατεβάσματος του κακόβουλου λογισμικού. Μετά την επιτυχημένη μόλυνση του IoT αντικειμένου, το αντικείμενο αυτό είναι έτοιμο να λάβει εντολές επίθεσης, από τον διακομιστή εντολών και ελέγχου.

- Ο διαχειριστής του botnet, δίνει εντολή στο δίκτυο για την εκκίνηση επίθεσης προς συγκεκριμένο στόχο/διακομιστή. Το Mirai έχει την δυνατότητα για τις επιθέσεις: UDP flood, VSE flood, DNS flood, SYN flood, ACK flood, TCP STOMP flood, GRE IP flood, GREETH flood, UDPPLAIN flood and HTTP flood.

3.2.4 Επιθέσεις DDoS

Οι επιθέσεις DDoS, πλήττουν το επίπεδο της διαθεσιμότητας των δεδομένων. Είναι κατανεμημένου τύπου επίθεση, που αποσκοπεί στην άρνηση παροχής υπηρεσίας από το εκτεθειμένο/μολυσμένο υπολογιστικό πόρο. Οι επιθέσεις αυτές, εξαντλούν τους πόρους δικτύου ή/και την χωρητικότητα του εκτεθειμένου συστήματος. Αυτό οδηγεί σε περιορισμό της πρόσβασης στον πόρο με σειρά αρνητικών συνεπειών (Σχήμα 3.6 σελίδα 24).

Στην επίθεση DDoS, στον ρόλο του εισβολέα είναι ένα δίκτυο bot. Το botnet μπορεί να αποτελείται από αρκετές δεκάδες έως αρκετές χιλιάδες υπολογιστές ή αλλιώς zombies, μολυσμένους από κακόβουλο λογισμικό. Έτσι, το δίκτυο αυτό στέλνει ακατάπαυστα αιτήματα προς στο εξυπηρετητή στόχο, καθιστώντας τον έτσι μη λειτουργικό. Προς το παρόν, δεν υπάρχουν ικανοποιητικά μέσα αντιμετώπισης των επιθέσεων DDoS. Παράλληλα με την έρευνα για την αντιμετώπιση του προβλήματος των κατανεμημένων επιθέσεων, που αποσκοπούν στην άρνηση παροχής υπηρεσιών, παρατηρούμε την συνεχή εμφάνιση νέων τύπων DDoS επιθέσεων [1] [42].



Σχήμα 3.6: Botnet diagram showing a DDoS attack.

Διακρίνουμε τρεις γενικές κατηγορίες DDoS επιθέσεων [17]:

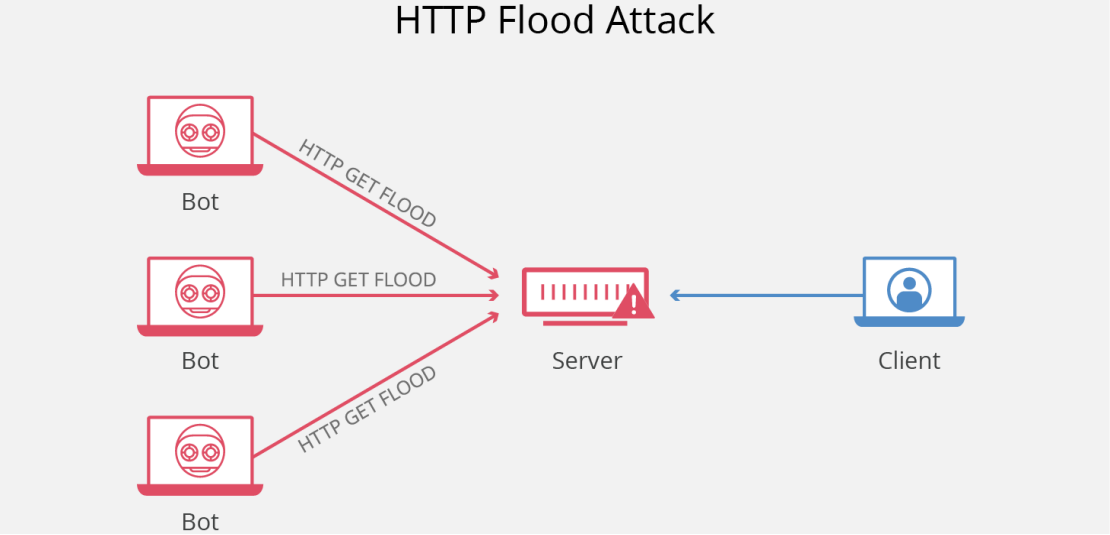
- Επιθέσεις βάσει όγκου. Περιλαμβάνει επιθέσεις όπως: UDP flood, ICMP flood και άλλες. Ο στόχος της επίθεσης είναι ο κορεσμός του εύρους ζώνης του επιτιθέμενου -bandwidth- πόρου.

- Επιθέσεις βάσει πρωτοκόλλων. Περιλαμβάνει επιθέσεις: SYN flood, Ping of Death, Smurf DDoS, επιθέσεις κατακερματισμένων πακέτων και άλλες. Αυτός ο τύπος επίθεσης, καταναλώνει πόρους διακομιστών ή πόρους ενδιάμεσου εξοπλισμού επικοινωνίας (τείχη προστασίας και αντισταθμιστές φορτίου -load balancers-).

- Επιθέσεις στο επίπεδο εφαρμογής. Περιλαμβάνει GET/POST flood, επιθέσεις με στόχο τρωτά σημεία διακομιστών Apache, Windows ή OpenBSD και άλλους. Στις επιθέσεις αυτές, αποστέλλονται φαινομενικά νόμιμα αιτήματα περιεχομένου, με στόχο την κατάρρευσή τους προς επίθεση διακομιστή.

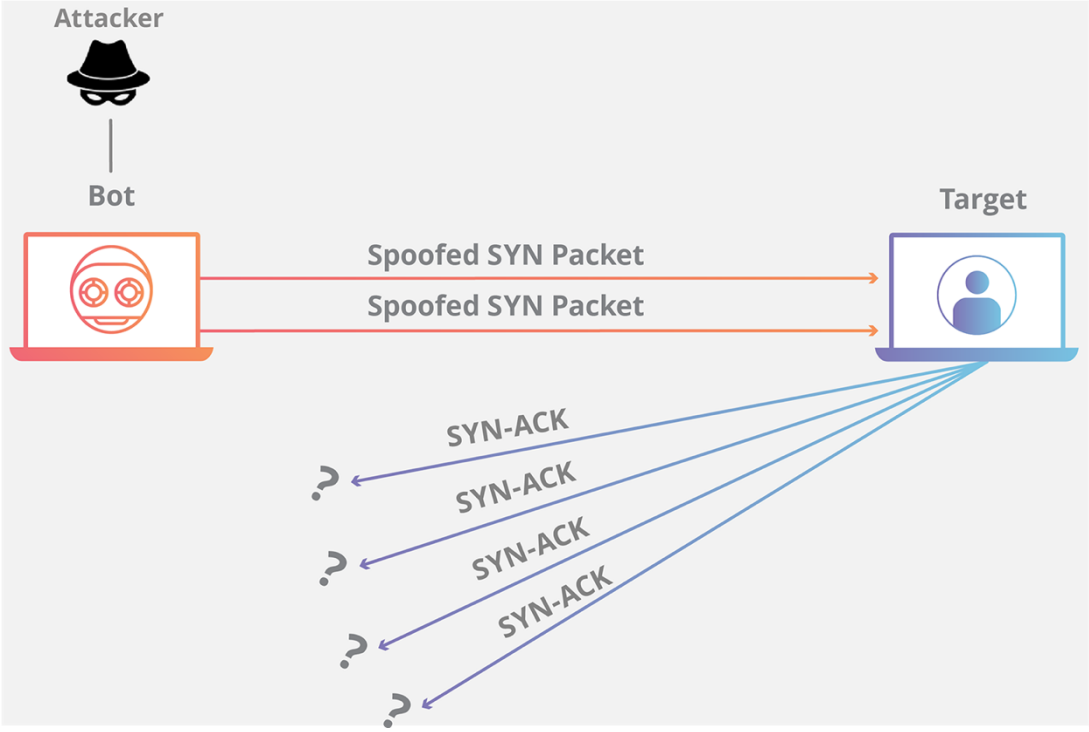
3.2.5 Συνηθέστεροι Τύποι Επιθέσεων

Ο δημοφιλέστερος τύπος επίθεσης, είναι ο HTTP-flood. Ο επιτιθέμενος με αυτήν την επίθεση αποστέλλει έναν μεγάλο αριθμό "υγιών" πακέτων HTTP στο υπό επίθεση σύστημα, με αποτέλεσμα την απόφραξη του καναλιού επικοινωνίας (Σχήμα 3.7 σελίδα 26).



Σχήμα 3.7: HTTP flood attack.

Ένας άλλος δημοφιλής τύπος επίθεσης είναι ο SYN-flood. Αυτός ο τύπος επίθεσης, εκμεταλλεύεται τα χαρακτηριστικά της τριμερούς χειραψίας -three-way handshake. Ο επιτιθέμενος, αποστέλλει έναν καταιγιστικό αριθμό πακέτων SYN στο δυνητικό υπολογιστή/θύμα. Το επιτιθέμενο σύστημα, θεωρώντας ότι τα παραπάνω πακέτα προέρχονται από κανονικό χρήστη, απαντά με (SYN-ACK) πακέτα, σύμφωνα με την διαδικασία της τριμερούς χειραψίας. Όμως, ο επιτιθέμενος δεν αποστέλλει ACK πακέτα για την ολοκλήρωση της "χειραψίας", με αποτέλεσμα την ατελείωτη αναμονή του υπολογιστή θύματος. Αυτή η αναμονή ολοκλήρωσης των ημιτελών συνδέσεων, απαιτεί υπολογιστικούς πόρους. Έτσι, ο υπολογιστής θύμα μετά από έναν αριθμό ατελών συνδέσεων, ξεπερνά το απαιτούμενο λειτουργικό όριο υπολογιστικών πόρων, και καθίσταται μη λειτουργικός (Σχήμα 3.8 σελίδα 27).



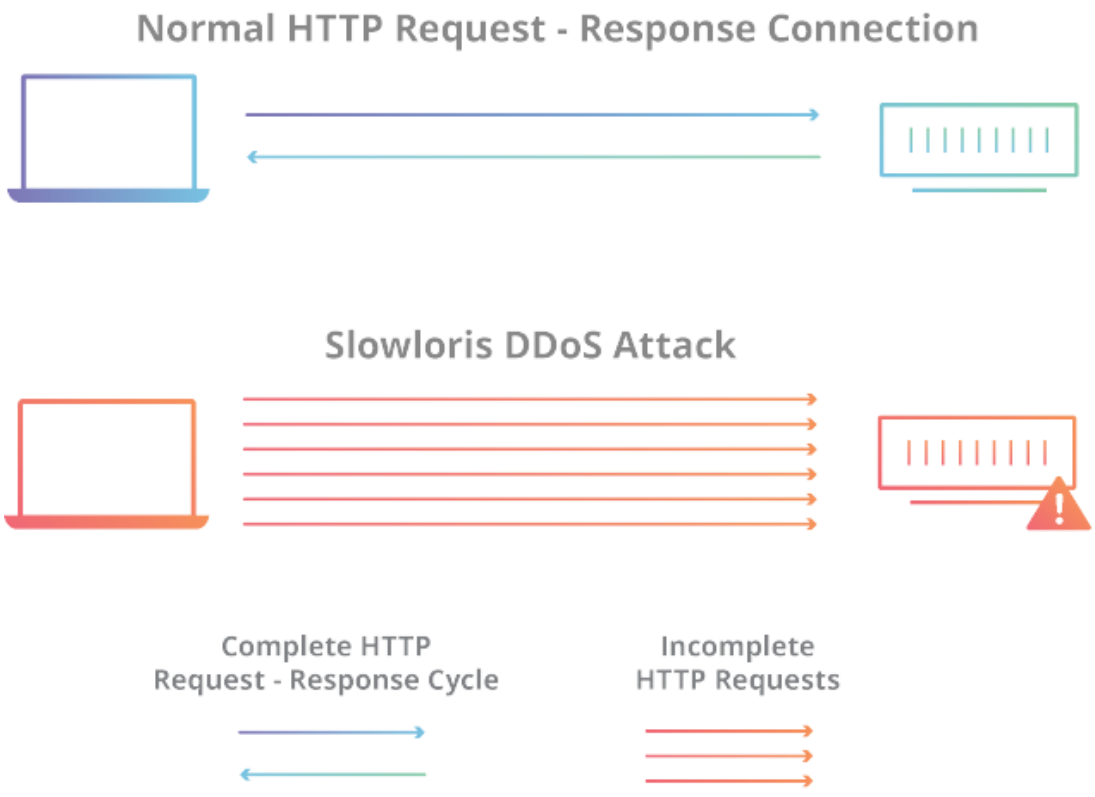
Σχήμα 3.8: SYN flood attack.

Στην επίθεση UDP flood, ο στόχος είναι η "υπερχείλιση" τυχαίων θυρών του συστήματος στόχου με πακέτα UDP. Αυτή η "υπερχείλιση", αναγκάζει το σύστημα στόχο σε επανειλημμένο έλεγχο των εφαρμογών, που "ακούν" στις υπό επίθεση θύρες. Στην περίπτωση που δεν υπάρχει κάποια εφαρμογή που να "ακούει" στις συγκεκριμένες θύρες, το σύστημα αποστέλλει πακέτο ICMP -Destination Unreachable. Αυτή η διαδικασία, έχει ως αποτέλεσμα την υπερβολική χρήση των πόρων του, που τελικά οδηγεί στην ανικανότητα εξυπηρέτησης του συστήματος.

Παρόμοια με την παραπάνω επίθεση είναι η ICPM flood. Κατά την επίθεση αυτή, αποστέλλονται πακέτα ICPM Echo Request με γρήγορο ρυθμό στον στόχο, χωρίς την αναμονή απάντησης. Όπως, γίνεται κατανοητό, το ICPM flood, καταναλώνει την χωρητικότητα του καναλιού επικοινωνίας (bandwidth), συνεπαγόμενη την επιβράδυνση της επίδοσης του συστήματος.

Το Ping of Death [62] είναι μια επίθεση, που εκμεταλλεύεται το ότι πολύ τύποι υπολογιστών, δεν μπορούν να χειριστούν πακέτα ping μεγαλύτερα από 65535 bytes. Μια επίθεση Ping of Death, περιλαμβάνει την αποστολή μεγάλων ping πακέτων στο σύστημα θύμα, μέχρι να τεθεί μη λειτουργικός.

Η επίθεση Slowloris [53], είναι μια επίθεση που πραγματοποιείται από έναν διακομιστή σε έναν άλλο, με σκοπό να τον καταστήσει μη λειτουργικό. Αυτό επιτυγχάνεται, με την δημιουργία μεγάλου αριθμού ημιτελών συνδέσεων, οι οποίες κρατούνται "ανοικτές" για όσο το δυνατόν περισσότερο χρόνο. Το σύστημα θύμα, διατηρεί τις συνδέσεις αυτές ανοικτές, και οδηγεί στην μη διαθεσιμότητα νέων συνδέσεων για νέους χρήστες (Σχήμα 3.9 σελίδα 28).



Σχήμα 3.9: Slowloris attack.

3.3 Τεχνητή Νοημοσύνη Και Μηχανική Μάθηση

Τι είναι τεχνητή νοημοσύνη; Παρατηρούμε διαφορετικές απαντήσεις-ορισμούς σε αυτό το ερώτημα, από πολλούς ερευνητές τα τελευταία χρόνια. Τα πρώτα προσεγγιστικά βήματα προς την τεχνητή νοημοσύνη, ξεκινούν από την Ελληνική αρχαιότητα με τον Αριστοτέλη (384-322 π.Χ.) στους "Συλλογισμούς", όπου περιέγραψε, το πώς σωστές υποθέσεις, οδηγούν πάντα σε σωστά συμπεράσματα.

Ως ορισμός Τεχνητή Νοημοσύνη (Artificial Intelligence), εμφανίστηκε για πρώτη φορά το 1956 [39], σε ερευνητικό συνέδριο για την μελέτη δυνατότητας χρήσης υπολογιστών για την μελέτη της ανθρώπινης νοημοσύνης [54]. Κατά τον Henri Bergson 1859-1941, AI είναι η "δυνατότητα κατασκευής τεχνητών αντικειμένων-εργαλείων που να κατασκευάζουν άλλα εργαλεία". Ο Patric Winston, καθηγητής του MIT και διευθυντής του εργαστηρίου ΤΝ στο ίδιο πανεπιστήμιο, ορίζει ως AI την "μελέτη ιδεών, που θα επιτρέψουν στους υπολογιστές να κάνουν πράγματα που κάνουν οι άνθρωποι με την ευφυΐα τους. Ο κεντρικός στόχος του AI, είναι να κάνει τους υπολογιστές πιο χρήσιμους, και να κατανοηθούν οι αρχές που καθιστούν την μηχανική ευφυΐα "δυνατή" [4].

Υπάρχουν λοιπόν πολλοί τρόποι για την προσομοίωση της ανθρώπινης νοημοσύνης. Η ΤΝ, μπορεί να είναι μια επιμελημένη σειρά if-then δηλώσεων σε ένα πρόγραμμα, ή μπορεί να είναι ένα πολύπλοκο στατιστικό μοντέλο, με προγραμματισμένες τις περιπτώσεις ενδιαφέροντος. Στις δύο παραπάνω προσεγγίσεις ΤΝ, επί της ουσίας δεν είναι τίποτα άλλο, από μια σειριακή δήλωση κανόνων, προγραμματισμένη από έναν άνθρωπο. Αυτές οι "μηχανές" συχνά αποκαλούνται: μηχανές κανόνων, έμπειρα συστήματα, συμβολική ΤΝ κ.α. [25].

Το ερώτημα που τίθεται: Οι προαναφερθείσες ΤΝ προσεγγίσεις, ενσαρκώνουν αυτό που οι Henri Bergson, Patric Winston και πολλοί άλλοι ερευνητές έχουν ορίσει ως ΤΝ;

3.3.1 Μηχανική Μάθηση

Η νοημοσύνη που μιμούνται οι μηχανές κανόνων, ομοιάζει με αυτήν ενός αυτόματου πωλητή αναψυκτικών, που υπολογίζει το υπόλοιπο των χρημάτων που πρέπει να επιστρέψει, στην περίπτωση που λάβει περισσότερα χρήματα από την αξία του αναψυκτικού. Οι μηχανές κανόνων, έμπειρα συστήματα και συμβολική ΤΝ, ενώ εντάσσονται στον ευρύτερο τομέα της ΤΝ, δεν θεωρούνται τεχνικές μηχανικής μάθησης.

Η μηχανική μάθηση (Machine Learning - ML) είναι κλάδος της ΤΝ. Όμως, αυτό που την διαφοροποιεί από τις άλλες τεχνικές, είναι η δυνατότητα να αυτορυθμίζεται/τροποποιείται, όταν εκτίθεται σε περισσότερα δεδομένα [38]. Ο τομέας της μηχανικής μάθησης λοιπόν, ερευνά και μελετά, την κατασκευή αλγορίθμων/μηχανών, που μπορούν να "μαθαίνουν" μέσω δεδομένων, και να κάνουν προβλέψεις επί νέων, πρωτόγνωρων δεδομένων. Ο σκοπός είναι, η μηχανή να προβλέψει ή να λάβει μια απόφαση, στηριζόμενη σε δεδομένα, χωρίς να ακολουθήσει προγραμματισμένες οδηγίες.

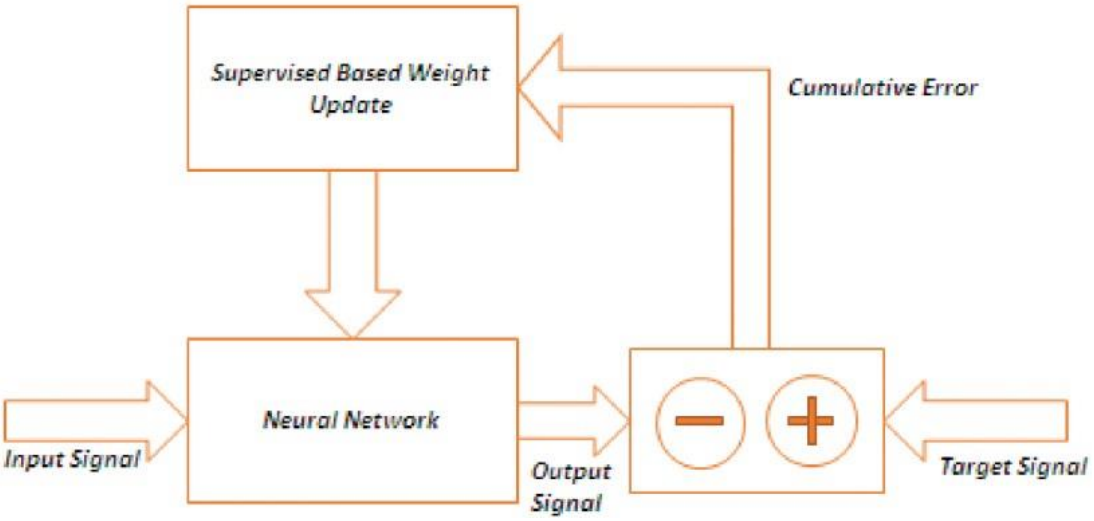
Το μεγαλύτερο ίσως κίνητρο για την εξέλιξη του ML, είναι ο ολοένα αυξανόμενος όγκος δεδομένων, και η ανάγκη εξόρυξης νέας "κρυφής γνώσης" από αυτά. Οι συμβατικές μέθοδοι ανάλυσης δεδομένων, περιορίζονται στην λογική ταξινόμηση με στατιστικούς κανόνες, που δεν προσφέρουν πολλά στην δημιουργία νέας γνώσης και εμπειρίας. Μοχλοί εξέλιξης της μηχανικής μάθησης, είναι η ανάπτυξη νέας υπολογιστικής τεχνολογίας (ισχυρότεροι επεξεργαστές, γρηγορότερες μνήμες RAM κ.α.), και το ελκυστικό κόστος των νέων αυτών τεχνολογιών [48].

3.3.2 Είδη Μηχανικής Μάθησης

Η μηχανική μάθηση περιλαμβάνει ένα ευρύ φάσμα τεχνικών, εργαλείων μάθησης, και θεωριών. Η επίλυση των προβλημάτων μέσω ML, απαιτεί αρκετό πειραματισμό, και για αυτό συχνά οι ερευνητές την θεωρούν ως ένα είδος τέχνης.

Ο τομέας της μηχανικής μάθησης, μπορεί να κατηγοριοποιηθεί στις παρακάτω κατηγορίες, ανάλογες με τους τρόπους που μαθαίνει ο άνθρωπος:

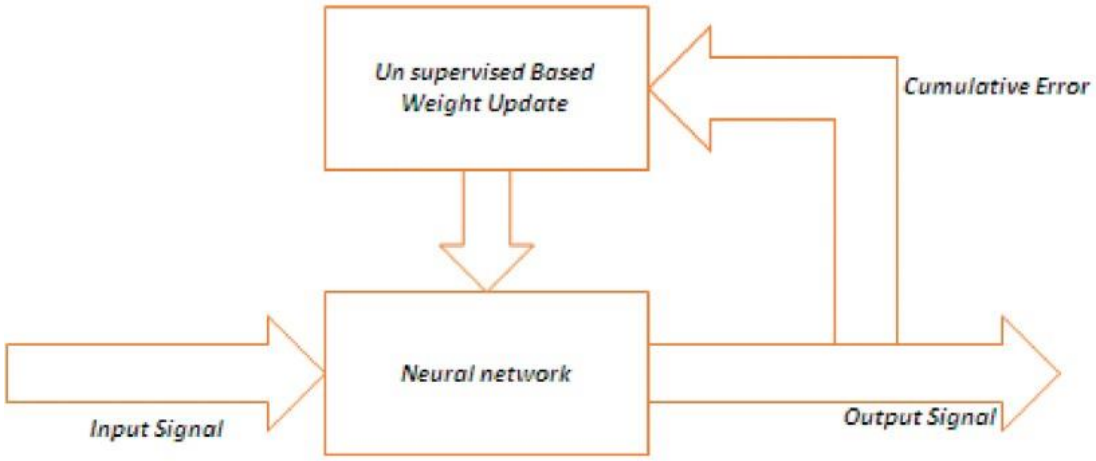
- Επιβλεπόμενη Μάθηση (Supervised Learning) [51]. Σε αυτήν την προσέγγιση, ο αλγόριθμος εκμάθησης τροφοδοτείται με δεδομένα εισόδου (Χ), που έχουν ήδη σωστή έξοδο (Υ). Το αποτέλεσμα του αλγορίθμου, είναι μια συνάρτηση, που συσχετίζει με σωστό τρόπο τα (Χ) και (Υ), με απώτερο σκοπό, την εξεύρεση μιας βέλτιστης γενικής συνάρτησης για εισόδους (Χ) με άγνωστες εξόδους (Υ). Η επιτυχία της μεθόδου, στηρίζεται στην τροφοδοσία σωστά συσχετισμένων εισόδων-εξόδων. Η τεχνική Supervised Learning χρησιμοποιείται για προβλήματα ταξινόμησης, διερμηνείας και πρόγνωσης (Σχήμα 3.10 σελίδα 31).



Σχήμα 3.10: Supervised Learning.

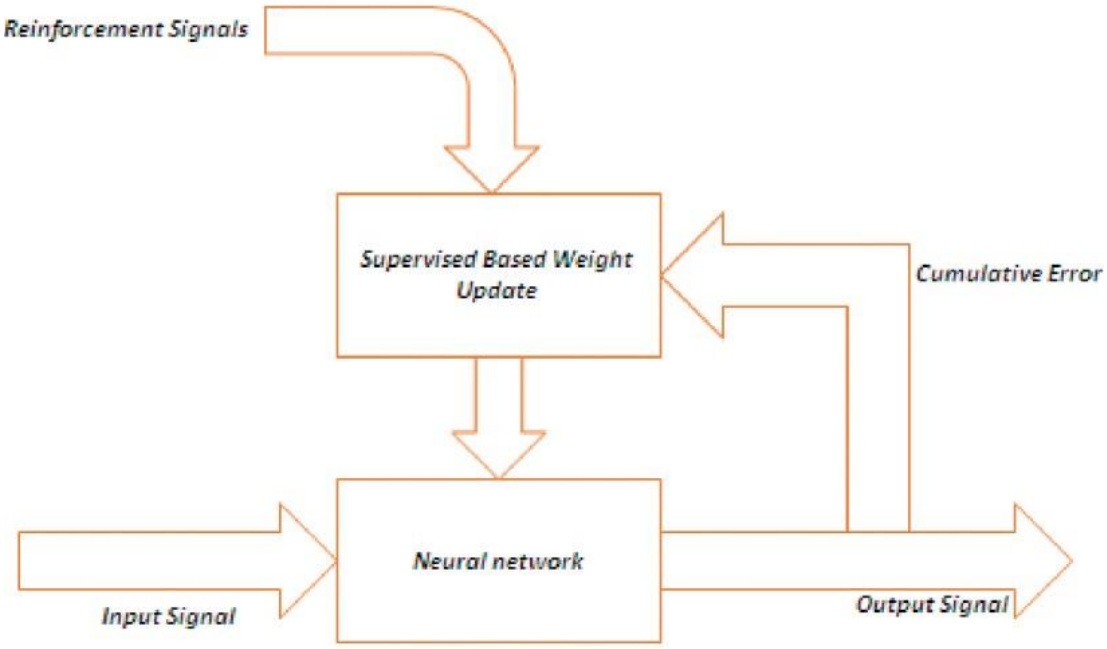
- Μη Επιβλεπόμενη Μάθηση (Unsupervised Learning) [14]. Ο αλγόριθμος εκμάθησης, κατασκευάζει ένα μοντέλο-συνάρτηση, η οποία περιγράφει τον συσχετισμό των εισόδων (Χ) και των εξόδων (Υ) με την μορφή παρατηρήσεων, χωρίς να γνωρίζει τις επιθυμητές εξόδους-αποτελέσματα. Η διαφοροποίηση με την προηγούμενη προσέγγιση, έγκειται στο ότι δεν υπάρχει σήμα σφάλματος έτσι ώστε ο

αλγόριθμος να προσαρμοστεί στο επιθυμητό αποτέλεσμα/προηγούμενη γνώση. Ουσιαστικά, ο αλγόριθμος αναζήτα μοτίβα σωστών παρατηρήσεων, μέσα από τα δεδομένα τροφοδοσίας. Τα προβλήματα για τα οποία είναι κατάλληλη (η Μη Επιβλεπόμενη Μάθηση), είναι η ανάλυση συσχετισμών και προβλήματα ομαδοποίησης (Σχήμα 3.11 σελίδα 32).



Σχήμα 3.11: Unsupervised Learning.

– Στην Ενισχυτική Μάθηση (Reinforcement Learning) [3], ο αλγόριθμος εκπαιδεύεται μέσα από μια σειρά ενεργειών, με την αλληλεπίδρασή του με το περιβάλλον. Έτσι, αντί ο αλγόριθμος να τροφοδοτείται a priori με σωστές εισόδους-εξόδους, η Ενισχυτική Μάθηση, παρέχει μία μέθοδο μέτρησης της απόδοσης του σωστού ή λάθους αποτελέσματος, και βάσει αυτής, προσαρμόζει τον αλγόριθμο μάθησης. Η μηχανή δοκιμάζει διαφόρους τρόπους για την επίλυση ενός προβλήματος, και στην περίπτωση επιτυχίας "επιβραβεύεται" με ένα σήμα. Αυτός ο τρόπος επίλυσης, μαθαίνεται και εφαρμόζεται, εάν η μηχανή συναντήσει εφάμιλλο πρόβλημα. Αυτός ο τρόπος μάθησης είναι κατάλληλος για προβλήματα που σχετίζονται με έλεγχο κίνησης οχημάτων, ρομπότ κ.α. (Σχήμα 3.12 σελίδα 33).



Σχήμα 3.12: Reinforcement Learning.

3.3.3 Αλγόριθμοι Ταξινόμησης

Οι αλγόριθμοι ταξινόμησης, ανήκουν στην κατηγορία μη επιβλεπόμενης μηχανικής μάθησης. Αύτη, είναι η επιλεχθείσα κατηγορία μηχανικής μάθησης του πειράματος της παρούσας διατριβής. Οι αλγόριθμοι αυτοί χρησιμοποιούνται για την ταξινόμηση δεδομένων, βασιζόμενοι σε παρελθοντικές παρατηρήσεις. Τα δεδομένα που απαιτούνται για την εκπαίδευση, αποτελούνται από ένα "σετ παρατηρήσεων εκπαίδευσης", με συσχετισμένες εισόδους (features) και εξόδους (που αντιπροσωπεύουν το επιθυμητό αποτέλεσμα της αντίστοιχης εισόδου). Η ολοκληρωμένη εκπαίδευση έχει ως εξής:

- Πριν ξεκινήσει η τροφοδοσία του αλγορίθμου εκμάθησης, γίνεται επεξεργασία του σετ δεδομένων εκπαίδευσης (feature extraction) [52], με στόχο την τροφοδοσία του αλγορίθμου με δεδομένα σχετικά του τελικού αποτελέσματος. Κατά το στάδιο της εκπαίδευσης, ο αλγόριθμος προσπαθεί να εντοπίσει μοτίβα και συσχετισμούς, μεταξύ των δεδομένων εισόδου και εξόδου. Το αποτέλεσμα της εκπαιδευτικής διαδικασίας,

είναι ένα γενικευμένο μοντέλο συσχετισμού εισόδων-εξόδων, το οποίο μπορεί να προβλέψει την έξοδο (αποτέλεσμα/κλάση) νέων μελλοντικών εισόδων.

- Για το εκπαιδευόμενο μοντέλο, θα πρέπει να αξιολογείται η επίδοση των προβλέψεων του. Η διαδικασία αξιολόγησης περιλαμβάνει, ένα σετ δεδομένων επαλήθευσης (validation dataset), πάνω στο οποίο καλείται να εκτελέσει σωστές προβλέψεις. Το μοντέλο λοιπόν, αυτορυθμίζεται βάσει των αποτελεσμάτων της επαλήθευσης, έτσι ώστε να επιτευχθεί μέγιστη ακρίβεια και ελάχιστο λάθος στις μελλοντικές προβλέψεις του.

- Η τελική επίδοση του μοντέλου, αξιολογείται με ένα σετ δεδομένων δοκιμής, ή test dataset. Το test dataset, είναι ένα δείγμα νέων/αγνώστων δεδομένων το οποίο δεν σχετίζεται καθόλου με το validation dataset.

- Ο συντονισμός του μοντέλου, ή hyper-parameter tuning, είναι η διαδικασία βελτιστοποίησης του μοντέλου, μέσω της αλλαγής των τιμών των παραμέτρων του αλγορίθμου εκμάθησης. Οι παράμετροι αυτές, δεν είναι δυνατόν να "μαθευτούν" κατά το εκπαιδευτικό στάδιο του μοντέλου. Η εξεύρεση των βέλτιστων παραμέτρων, αφενός μεν στηρίζεται σε τεχνικές όπως randomized search ή grid search, αφετέρου δε, επαφίεται στην εμπειρική επιλογή τιμών παραμέτρων από τον ερευνητή.

Μερικοί αλγόριθμοι ταξινόμησης είναι οι:

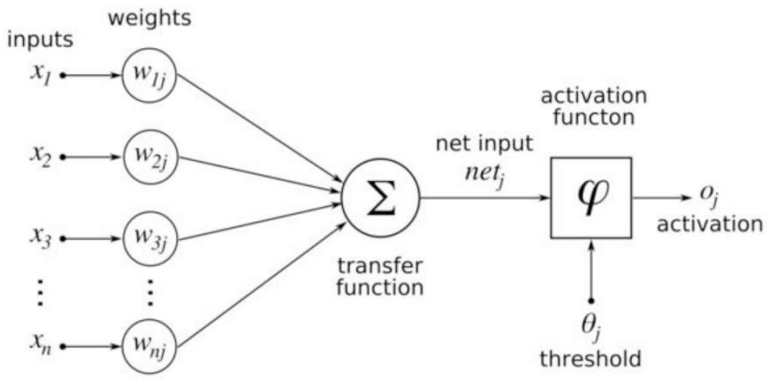
- Logistic Regression
- Random Forest
- k-Nearest Neighbors
- Neural Networks

- Gradient Boosting
- Decision Trees
- Support Vector Machines
- Naive Bayes

Η κατηγορία εκμάθησης που θα εστιάσουμε, είναι αυτή των νευρωνικών δικτύων, και πιο συγκεκριμένα των Βαθιών Νευρωνικών Δικτυών -Deep Neural Networks.

3.3.4 Βαθιά Νευρωνικά Δίκτυα

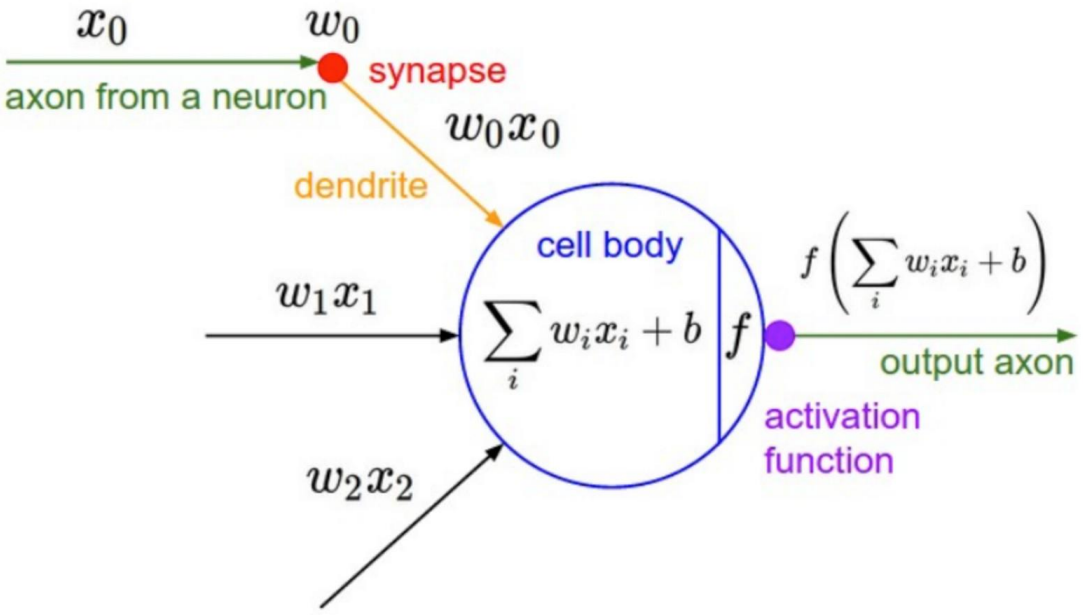
Η ανάπτυξη των βαθιών νευρωνικών δικτυών, κατέστη δυνατή τα πρόσφατα χρόνια, τόσο με την εξέλιξη των υπολογιστών πόρων (CPU, GPU) και αποθήκευσης/διαχείρισης δεδομένων, όσο και με την ανάπτυξη του τομέα της υπολογιστικής νοημοσύνης. Ο τεχνητός νευρώνας (Σχήμα 3.13 σελίδα 35), έχει πολλές ομοιότητες (Σχήμα 3.14 σελίδα 36) με τον βιολογικό νευρώνα (Σχήμα 3.15 σελίδα 37).



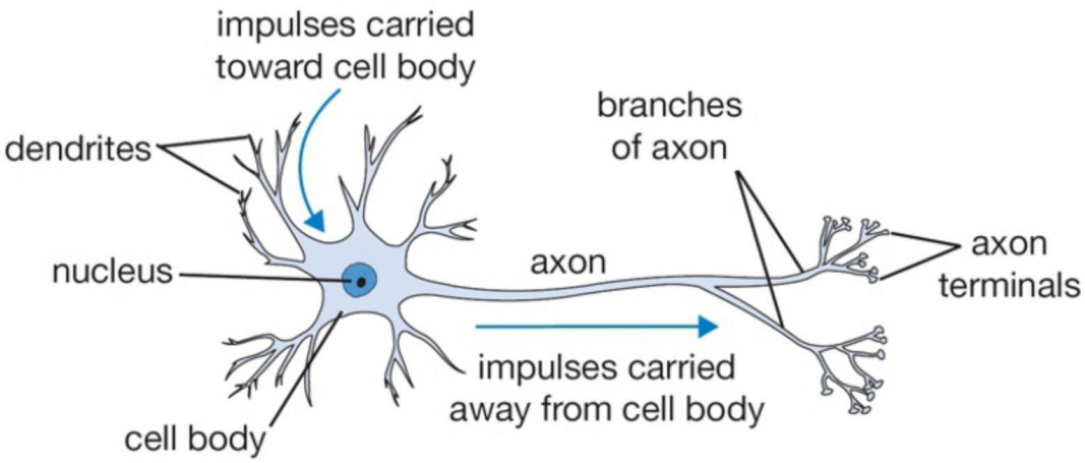
Σχήμα 3.13: Τεχνητός νευρώνας 1.

Κάθε τεχνητός νευρώνας, δέχεται αριθμητικά δεδομένα (είσοδοι), είτε από άλλους νευρώνες, είτε από το περιβάλλον, εφαρμόζει έναν υπολογισμό επί των εισόδων και παράγει ένα αποτέλεσμα (έξοδο). Το αποτέλεσμα αυτό, είτε προωθείται ως είσοδος σε άλλους νευρώνες, είτε είναι τελική έξοδος και κατευθύνεται στο περιβάλλον.

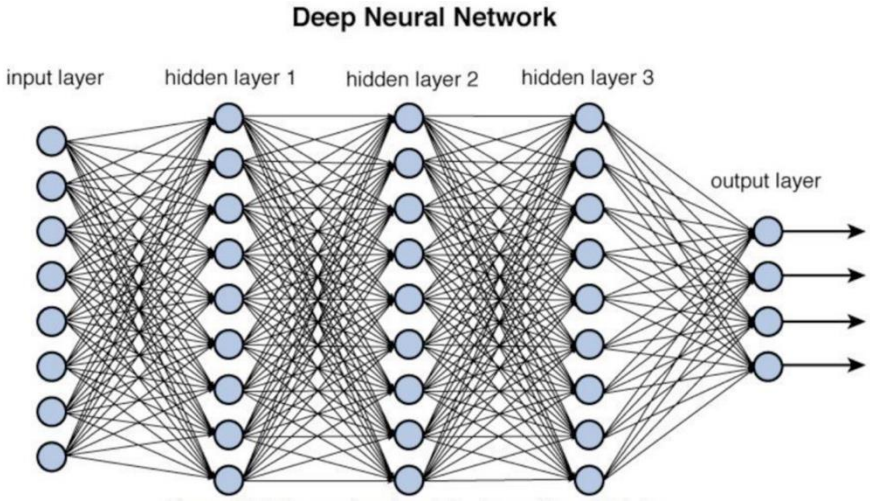
Τα βαθιά νευρωνικά δίκτυα, προσομοιάζουν την δομή του βιολογικού εγκεφάλου. Αποτελούνται από μεγάλο αριθμό διασυνδεδεμένων υπολογιστικών μονάδων/νευρώνες (Σχήμα 3.16 σελίδα 37), που έχουν την δυνατότητα να "αυτό-διδάσκονται", με την βοήθεια συναρτήσεων υπολογισμού συναπτικών βαρών. Το αποτέλεσμα είναι, η σταδιακή βελτίωση της μαθησιακής ικανότητας του δικτύου στην επίλυση προβλημάτων, χωρίς την παρέμβαση τρίτου, όπως παρατηρούμε στην περίπτωση των μηχανών κανόνων.



Σχήμα 3.14: Τεχνητός νευρώνας 2.



Σχήμα 3.15: Βιολογικός νευρώνας.



Σχήμα 3.16: Deep Neural Network.

3.3.5 Αξιολόγηση Μοντέλων Ταξινόμησης

Η κατασκευή, η βελτιστοποίηση και ο συντονισμός ενός νευρωνικού δικτύου, είναι αναπόσπαστα μέρη του κύκλου ζωής του. Παρόλα αυτά, η ευστοχία πρόβλεψης επί νέων άγνωστων δεδομένων, είναι η απόλυτη και η πιο σημαντική μέτρηση απόδοσης του. Η μέτρηση απόδοσης, επιτελείται σε ένα σετ δεδομένων, μη σχετικό με αυτό που χρησιμοποιήθηκε κατά την φάση εκπαίδευσης του μοντέλου. Το συγκεκριμένο σετ, αποτελείται από σωστά συσχετισμένες εισόδους-εξόδους, και τροφοδοτείται στο ήδη εκπαιδευμένο μοντέλο, με στόχο την παρατήρηση/μέτρηση της απόδοσης του.

Οι πιο σημαντικοί δείκτες μέτρησης απόδοσης είναι:

1) Το Confusion matrix [5], απεικονίζει σε μορφή πίνακα την απόδοση του μοντέλου. Οι στήλες στο Confusion matrix, αντιπροσωπεύουν περιπτώσεις βασιζόμενες σε προβλέψεις (Predicted), ενώ κάθε γραμμή του πίνακα απεικονίζει περιπτώσεις, βάση της πραγματικής (Actual) κλάσης, στις οποίες ανήκουν (Πίνακας 3.1 σελίδα 38).

	P (Predicted)	N (Predicted)
P (Actual)	TP True Positive	FN False Negative
N (Actual)	FP False Positive	TN True Negative

Πίνακας 3.1: Confusion Matrix δύο κλάσεων.

Οι ετικέτες του πίνακα υποδηλώνουν τα εξής:

- True Positive (TP): υποδηλώνει τον αριθμό των σωστών προβλέψεων για την θετική κλάση.

- False Negative (FN): υποδηλώνει τον αριθμό των περιπτώσεων αυτής της κλάσης, που προβλέφθηκαν λανθασμένα ως η αρνητική κλάση.

- False Positive (FP): υποδηλώνει τον αριθμό των περιπτώσεων, που προβλέφθηκαν λανθασμένα ως η θετική κλάση.

- True Negative (TN): υποδηλώνει τον αριθμό των περιπτώσεων, που σωστά προβλέφθηκαν ως η αρνητική κλάση.

2) Η μέτρηση Accuracy [29], είναι η συνολική ακρίβεια του μοντέλου (ποσοστό των σωστών προβλέψεων), η οποία αποδίδεται με την εξίσωση:

$$Accuracy = \frac{TP + TN}{TP + FP + FN + TN}$$

Στον αριθμητή, έχουμε το σύνολο των σωστών προβλέψεων, και στον παρονομαστή, το σύνολο όλων των αποτελεσμάτων πρόβλεψης του μοντέλου.

3) Η μέτρηση Precision, δείχνει την θετική προβλεπόμενη τιμή του μοντέλου ταξινόμησης, δηλαδή το ποσοστό των σωστών προβλέψεων. Περιγράφεται από την παρακάτω εξίσωση:

$$Precision = \frac{TP}{TP + FP}$$

Στον αριθμητή, έχουμε τις σωστές προβλέψεις για την θετική κλάση, και στον παρονομαστή το σύνολο των προβλέψεων για την θετική κλάση, συμπεριλαμβανόμενες και τις λάθος.

4) Το Recall, δείχνει τον αριθμό σωστών προβλέψεων για την θετική κλάση, και περιγράφεται με την εξίσωση:

$$Recall = \frac{TP}{TP + FN}$$

Στον αριθμητή, έχουμε το σύνολο των σωστών προβλέψεων, και στον παρονομαστή, το σύνολο των σωστών και άστοχων προβλέψεων για την θετική κλάση.

5) Το F1 score, με το οποίο υπολογίζεται ο αρμονικός μέσος όρος του precision και του recall. Η εξίσωση είναι:

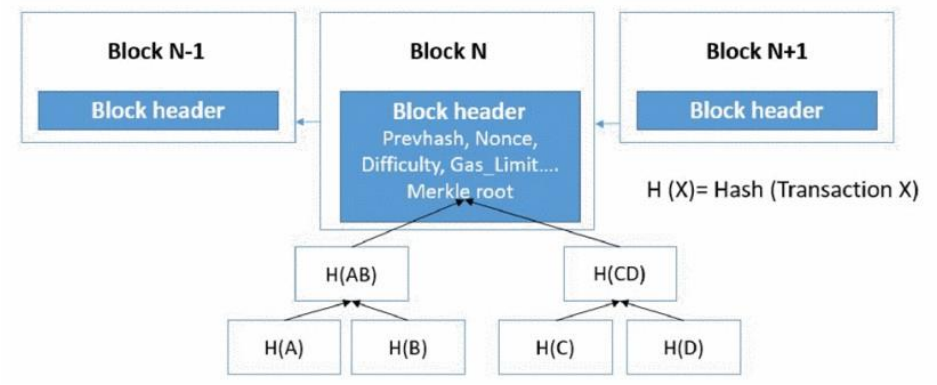
$$F_1 = \frac{2TP}{2TP + FP + FN}$$

3.4 Τεχνολογία Blockchain

Στο πείραμα της παρούσας διατριβής, γίνεται χρήση της τεχνολογίας blockchain ως μέσο καταγραφής συμβάντων ασφάλειας στο δίκτυο IoT. Τι είναι το blockchain;

Το blockchain είναι ένα αρχείο ψηφιακών συναλλαγών. Το όνομα του προέρχεται από την δομή του. Μεμονωμένα αρχεία/συναλλαγές/εγγραφές που ονομάζονται μπλοκ ή κόμβοι, συνδέονται μεταξύ τους σε μια ενιαία δομή (λίστα) η οποία ονομάζεται αλυσίδα. Μια πολύ γνωστή εφαρμογή blockchain, είναι τα κρυπτονομίσματα, οπού χρησιμοποιείται για την καταγραφή των συναλλαγών (Σχήμα 3.17 σελίδα 41).

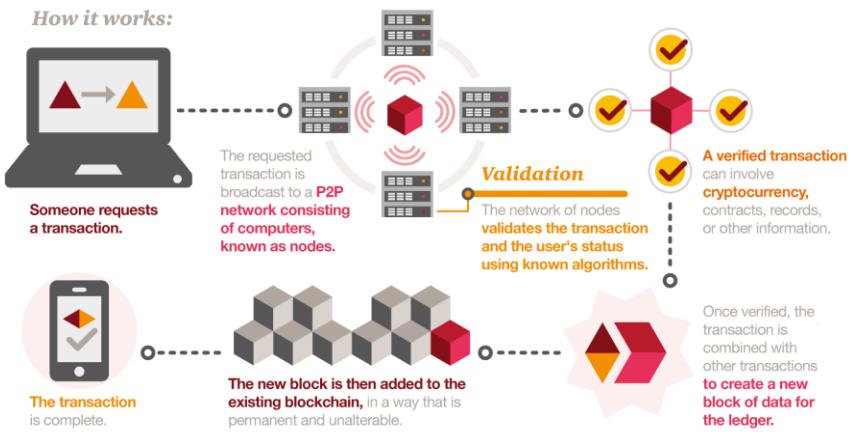
Κάθε νέα συναλλαγή που καταγράφεται/προστίθεται στο blockchain, πρέπει να επαληθευτεί πριν οριστικοποιηθεί. Η επαλήθευση πραγματοποιείται μέσω της συναίνεσης μεταξύ των κόμβων. Οι ανεξάρτητοι αυτοί κόμβοι, σχηματίζουν ένα αποκεντρωμένο δίκτυο, όπου



Σχήμα 3.17: Blockchain blocks.

συνεργικά επικυρώνουν μια νέα συναλλαγή ως έγκυρη. Αυτή η αποκεντρωμένη δικτυακή δομή, διασφαλίζει ότι κανένα ανεξάρτητο σύστημα ή κόμβος, δεν μπορεί να προσθέσει αυθαίρετα νέες συναλλαγές.

Ειδικότερα, όταν μια νέα συναλλαγή προστίθεται, αυτή συνδέεται με την προηγούμενη με μια "κρυπτογραφική σύνοψη" (cryptographic hash), η οποία παράγεται από τα περιεχόμενα της προηγούμενης μπλοκ-συναλλαγής. Διασφαλίζεται έτσι, η "αδιάρρηκτη" φύση της αλυσίδας, καθώς και η μόνιμη εγγραφή της νέας συναλλαγής (Σχήμα 3.18 σελίδα 42).



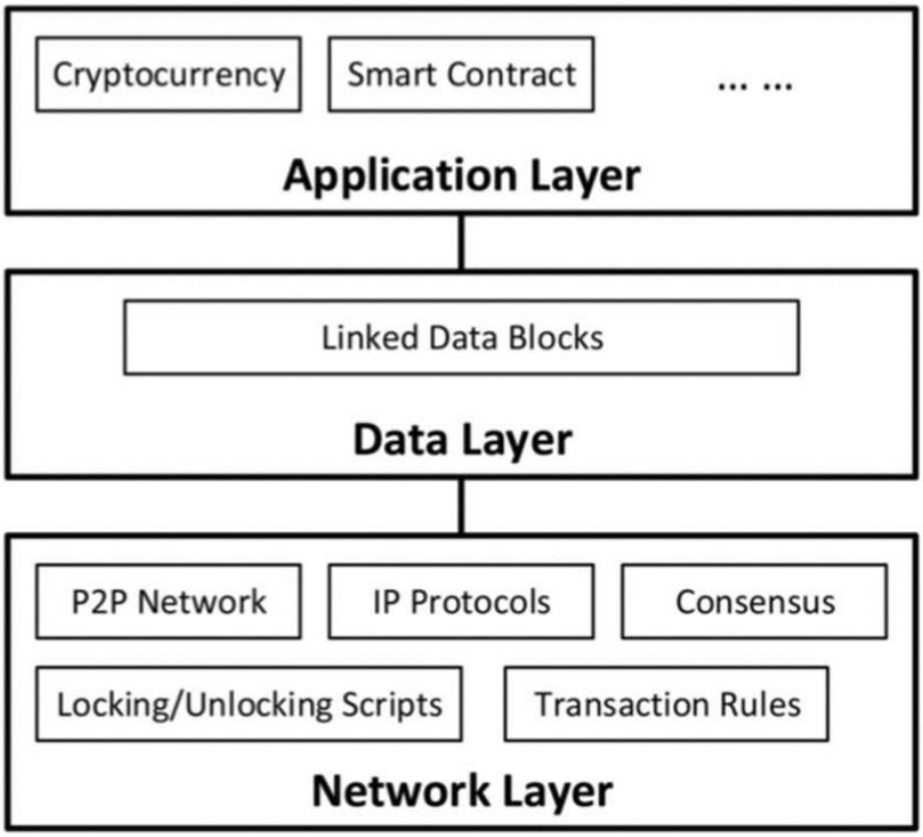
Σχήμα 3.18: How blockchain works.

Σε ένα δίκτυο blockchain, διακρίνονται τα έξης επίπεδα [2] (Σχήμα 3.19 σελίδα 43):

- Το επίπεδο δικτύου Network Layer, όπου το blockchain συνδέεται με τους χρήστες και το περιβάλλον. Σε αυτό το επίπεδο, πραγματοποιείται η επικύρωση μέσω συναίνεσης νέων συναλλαγών.

- Το επίπεδο δεδομένων Data Layer. Εδώ, καθορίζονται οι αλγόριθμοί και γενικότερα οι μηχανισμοί, που επεξεργάζονται τα δεδομένα του δικτύου blockchain.

- Το επίπεδο εφαρμογής Application Layer. Σε αυτό, υπάγονται οι διάφορες εφαρμογές που δύναται να χρησιμοποιήσουν το blockchain, όπως τα κρυπτονομίσματα.



Σχήμα 3.19: Blockchain discrete levels.

3.4.1 Δημόσια Και Ιδιωτικά Blockchain

Τα δίκτυα blockchain, μπορούν να διακριθούν σε δημόσια και ιδιωτικά [30]. Οι δύο αυτές κατηγορίες, μοιράζονται κοινά χαρακτηριστικά, όπως:

- Η δικτυακή δομή τους είναι αποκεντρωμένη, όπου κάθε κόμβος διατηρεί αντίγραφο όλων των συναλλαγών του δικτύου.

- Ο συγχρονισμός του αντίγραφου συναλλαγών, επιτυγχάνεται με την διαδικασία της συναίνεσης (consensus).

- Διαθέτουν μηχανισμό ορθότητας συναλλαγών.

Η διαφορά μεταξύ των δημόσιων και ιδιωτικών blockchain, έγκειται στο ποιος μπορεί να συμμετάσχει. Στο δημόσιο δίκτυο, οποιοσδήποτε μπορεί να συμμετάσχει, ήτοι, να διαβάσει και να προσθέσει νέες συναλλαγές. Αντίθετα, στο ιδιωτικό, υπάρχει περιορισμός, στο ποιος μπορεί να συμμετάσχει, και στην πρόσβαση των συναλλαγών.

Η δημιουργία διαφορετικών τύπων, προήλθε από την ανάγκη αντιμετώπισης πρακτικών προβλημάτων ενσωμάτωσης του blockchain, σε σχέση με το ποια οντότητα μπορεί να έχει πρόσβαση σε αυτό. Σε εφαρμογές λ.χ. κρυπτονομίσματα, η χρήση δημόσιου blockchain θεωρείται κατάλληλη, όπου οι κύριοι στόχοι, είναι η ανωνυμία της συμμετέχουσας οντότητας, και η διαφάνεια των συναλλαγών. Η χρήση ιδιωτικού δικτύου, κρίνεται καταλληλότερη σε εφαρμογές εθνικής ασφάλειας, ασφάλειας και επαλήθευσης εταιρικών συναλλαγών, κ.α. όπου θα πρέπει να είναι γνωστό το ποιος συμμετέχει στο δίκτυο, και τι μπορεί να κάνει σε αυτό.

3.4.2 Οφέλη Blockchain Στο IoT

Το blockchain θεωρείται εγγενώς (κρυπτογραφικά) ασφαλές κατανεμημένο δίκτυο, που επιτρέπει την ασφαλή μεταφορά δεδομένων μέσα σε αυτό. Η κατανεμημένη δομή και η "φυσική" ασφάλεια που προσφέρει, είναι χαρακτηριστικά που ένα δίκτυο IoT μπορεί να επωφεληθεί.

Παραιτείται ότι τα IoT δίκτυα, βασίζονται σε μια κεντρική αρχιτεκτονική (centralized architecture). Αυτό πρακτικά σημαίνει ότι, ένα αντικείμενο IoT στέλνει τα δεδομένα που συλλέγει στο νέφος (cloud) όπου επεξεργάζονται, και είτε προωθούνται σε άλλες συσκευές/υπολογιστές/υπηρεσίες, είτε αποστέλλονται πίσω στο IoT αντικείμενο. Το ζήτημα που ανακύπτει με αύτη την αρχιτεκτονική, είναι περιορισμένη δυνατότητα επεκτασιμότητας, που έχει ως αποτέλεσμα, την καθυστερημένη επικοινωνία μεταξύ των συσκευών, με ενδεχόμενη αύξηση του κόστους λειτουργίας. Το πρόβλημα αυτό, προβλέπεται να γίνει εντονότερο στο άμεσο μέλλον, όπου προβλέψεις δείχνουν τον αριθμό τον IoT συσκευών να ξεπερνάει τα 50 δισεκατομμύρια το 2020 [59].

Ένα άλλο ζήτημα που μπορεί να προκύψει από την κεντρική αρχιτεκτονική, είναι η διαθεσιμότητα του συστήματος. Σε ένα δίκτυο κεντρικής αρχιτεκτονικής, ο κίνδυνος "αποτυχίας μοναδικού σημείου" (single point of failure) είναι υπαρκτός. Αντίθετα, σε ένα αποκεντρωμένο σύστημα blockchain, είναι αδύνατη η ταυτόχρονη αποτυχία όλων των κόμβων.

Η προσφερόμενη από την τεχνολογία blockchain δυνατότητα έξυπνων συμβολαίων-smart contracts [22], επιτρέπει στις IoT συσκευές να λειτουργούν με ασφάλεια και αυτονομία. Επιπλέον, τα "έξυπνα συμβόλαια" επιτρέπουν αυτοματοποίηση εργασιών, και μείωση του κόστους λειτουργείας.

Ο ιδανικότερος τύπος blockchain για εφαρμογές ασφάλειας που εμπλέκουν IoT, είναι ο ιδιωτικός [13] [47]. Στα ιδιωτικά blockchain δίκτυα, οι συναλλαγές επιτελούνται πιο γρήγορα σε σύγκριση με τα δημόσια, λόγω του ότι δεν διαθέτουν μεγάλο αριθμό κόμβων, καθώς και της απουσίας Proof of Work (PoW) ή Proof of Stake (PoS) [61]. Τέλος, λόγω των ευάριθμων κόμβων, τα ιδιωτικά δίκτυα έχουν αυξημένη δυνατότητα επεκτασιμότητας, ιδιότητα χρήσιμη με την αναμενόμενη αύξηση του αριθμού των IoT συσκευών.

Κεφάλαιο 4
Πειραματικός Σχεδιασμός

Ο στόχος του πειράματος, είναι η κατασκευή ενός αυτόνομου ελεγχόμενου συστήματος δοκιμής απειλών, σε IoT δίκτυα. Τα καινοτόμα στοιχεία του συστήματος είναι α) ο σχεδιασμός αποκλειστικά με λογισμικό ανοικτού κώδικα β) η εύκολη παραμετροποίηση γ) η ανάλυση της δικτυακής κίνησης σε πραγματικό χρόνο και δ) η σύλληψη κακόβουλης δικτυακής κίνησης από απειλή, που το σύστημα ανίχνευσης απειλών δεν έχει εκπαιδευτεί να ανιχνεύει.

4.1 Τμήματα Του Πειράματος

Η δόμηση του συστήματος πραγματοποιήθηκε σε υπολογιστικό σύστημα, όπως περιγράφεται στον Πίνακα 4.1 σελίδα 46.

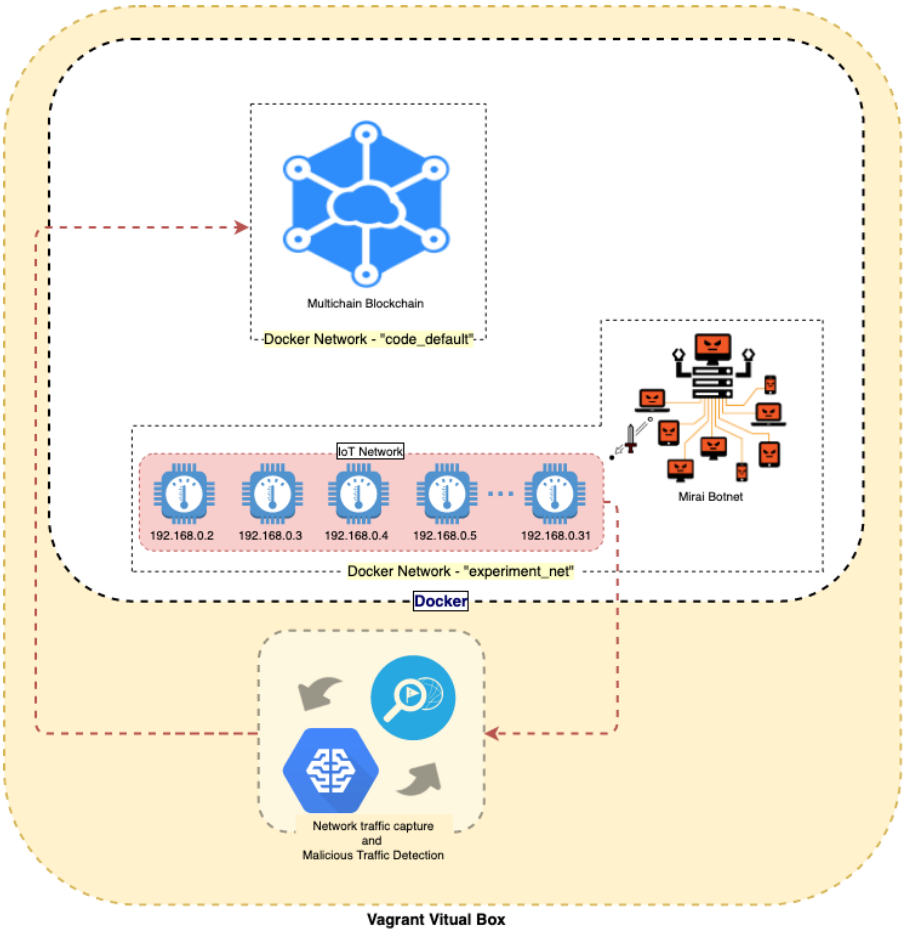
Model Name	MacBook Pro (Retina, 15-inch, Mid 2015)
Processor Name	Intel Core i7
Processor Speed	2.5 GHz
Number of Processors	1
Total Number of Cores	4
L2 Cache (per Core)	256 KB
L3 Cache	6 MB
Memory	16 GB 1600 MHz DDR3
Graphics	AMD Radeon R9 M370X 2048 MB Intel Iris Pro 1536 MB

Πίνακας 4.1: Host system specifications.

Ένα από τα βασικά χαρακτηριστικά του συστήματος, είναι η "φορητότητα" του (portability). Αυτή, επιτυγχάνεται με την χρήση τεχνολογίας εικονικής υπολογιστικής, και πιο συγκεκριμένα της τεχνολογίας Vagrant [37]. Επίσης η φορητότητα, ευνοεί την

αναπαραξιμότητα του πειράματος, σε έτερα υπολογιστικά συστήματα διαφορετικής αρχιτεκτονικής. Επιπλέον, οι καλές ερευνητικές πρακτικές, καταδεικνύουν τον πειραματισμό με κακόβουλο λογισμικό σε απομονωμένο και ελεγχόμενο περιβάλλον, όπου προσφέρεται με την παραπάνω τεχνολογία.

Η αρχιτεκτονική του πειραματικού συστήματος είναι "σπονδυλωτή" -modular architecture. Η προσέγγιση αυτή, προσφέρει μεγίστη παραμετροποίηση λ.χ. δοκιμή άλλων τύπων botnet, και δυνατότητα για μελλοντική βελτίωση των επιμέρους τμημάτων του συστήματος, χωρίς να επηρεάζεται η λειτουργικότητα των υπόλοιπων μερών. Η διαγραμματική σύνοψη του συστήματος, και η σχέση των επιμέρους τμημάτων, απεικονίζεται στο (Σχήμα 4.1 σελίδα 47). Τα μέρη του συστήματος περιγράφονται παρακάτω.



Σχήμα 4.1: Διαγραμματική σύνοψη του συστήματος.

4.2 Δίκτυο IoT Αντικειμένων

Το υπό εξέταση αντικείμενο του πειράματος, είναι η ασφάλεια ενός δικτύου IoT. Για την κατασκευή του δικτύου εντός του εικονικού περιβάλλοντος Vagrant, εγκαταστάθηκε η τεχνολογία Docker [21]. Η χρήση Docker container ενδείκνυται για προσομοίωση IoT, καθώς παρατηρούμε ότι οι μεγαλύτερες εταιρείες παροχής νεφοϋπολογιστικής υποδομής, πλέον παρέχουν υπηρεσίες εξομοίωσης IoT υποδομής με χρήση container, λ.χ. AWS IoT Device Simulator [5].

Με την βοήθεια του Docker, δημιουργήθηκαν αυτοδύναμες υπολογιστικές μονάδες containers, οι οποίες προσομοιώνουν τα IoT αντικείμενα, και συγκεκριμένα συσκευές "απομακρυσμένων" θερμομέτρων. Πρέπει να σημειωθεί, ότι δεν πραγματοποιήθηκε ολοκληρωτική εξομοίωση των αντικειμένων, ήτοι δεν εγκαταστάθηκε λογισμικό firmware θερμόμετρου. Σε κάθε συσκευή εγκαθίσταται το ελάχιστο απαραίτητο λογισμικό, που την καθιστά λειτουργική και κατάλληλη για τον ερευνητικό σκοπό. Οι εντολές δημιουργίας (build commands) του κάθε αντικείμενου, παρατίθενται στο αρχείο Dockerfile [6]. Κάθε IoT συσκευή, μπορεί να εκθέσει την τρέχουσα θερμοκρασίας μέσω μιας διεύθυνσης IP ή κανονικής διεύθυνσης domain name λ.χ. " curl remote−thermometer−0" ή "curl 192.168.0.2".

Συνοπτικά, τα κύρια μέρη/χαρακτηρίστηκα του αντικειμένου είναι:

- Εφαρμογή Python Flask [44] για την διάθεση των δεδομένων θερμοκρασίας στην πόρτα 80.

- Πρόγραμμα εξομοίωσης θερμοκρασιακών δεδομένων [7].

[5] https://aws.amazon.com/solutions/iot-device-simulator/
[6] https://github.com/anarchos78/iot-blockchain-ml-botnet-experiment/blob/master/project-files/docker_files/iot/Dockerfile
[7] https://github.com/anarchos78/iot-blockchain-ml-botnet-experiment/blob/master/project-files/docker_files/iot/app/helpers.py

- Πρόσβαση SSH στην πόρτα 22.

- Πρόσβαση telnet στην πόρτα 23.

Για την επιτυχημένη προσομοίωση επίθεσης στο δίκτυο IoT από το Mirai botnet, ένας συγκεκριμένος αριθμός συσκευών, έχει σκοπίμως αδύναμα διαπιστευτήρια telnet -login: root και password: root. Ο αριθμός αυτός καθορίζεται δυναμικά, με βάσει τον συνολικό αριθμό των IoT.

Όλες οι συσκευές συνδέονται σε ένα δίκτυο, με το όνομα "experiment_net". Το δίκτυο αυτό, δημιουργήθηκε από το λογισμικό Docker και είναι τύπου bridge [8].

Παρατίθεται ο πίνακας με το όνομα κάθε συσκευής, την IP διεύθυνση και το κανονικό όνομα - Domain Name (Πίνακας 4.2 σελίδα 49).

Όνομα IoT	IP διεύθυνση	Κανονικό όνομα -Domain Name
remote-thermometer-0	192.168.0.2	remote-thermometer-0
remote-thermometer-0	192.168.0.3	remote-thermometer-1
remote-thermometer-0	192.168.0.4	remote-thermometer-2
remote-thermometer-0	192.168.0.5	remote-thermometer-3
remote-thermometer-0	192.168.0.6	remote-thermometer-4
remote-thermometer-0	192.168.0.7	remote-thermometer-5
remote-thermometer-0	192.168.0.8	remote-thermometer-6
remote-thermometer-0	192.168.0.9	remote-thermometer-7
remote-thermometer-0	192.168.0.10	remote-thermometer-8
remote-thermometer-0	192.168.0.11	remote-thermometer-9
remote-thermometer-0	192.168.0.12	remote-thermometer-10
remote-thermometer-0	192.168.0.13	remote-thermometer-11
remote-thermometer-0	192.168.0.14	remote-thermometer-12
remote-thermometer-0	192.168.0.15	remote-thermometer-13
remote-thermometer-0	192.168.0.16	remote-thermometer-14
remote-thermometer-0	192.168.0.17	remote-thermometer-15
remote-thermometer-0	192.168.0.18	remote-thermometer-16
remote-thermometer-0	192.168.0.19	remote-thermometer-17
remote-thermometer-0	192.168.0.20	remote-thermometer-18

[8] https://docs.docker.com/network/bridge/

remote-thermometer-0	192.168.0.21	remote-thermometer-19
remote-thermometer-0	192.168.0.22	remote-thermometer-20
remote-thermometer-0	192.168.0.23	remote-thermometer-21
remote-thermometer-0	192.168.0.24	remote-thermometer-22
remote-thermometer-0	192.168.0.25	remote-thermometer-23
remote-thermometer-0	192.168.0.26	remote-thermometer-24
remote-thermometer-0	192.168.0.27	remote-thermometer-25
remote-thermometer-0	192.168.0.28	remote-thermometer-26
remote-thermometer-0	192.168.0.29	remote-thermometer-27
remote-thermometer-0	192.168.0.30	remote-thermometer-28
remote-thermometer-0	192.168.0.31	remote-thermometer-29

Πίνακας 4.2: Πίνακας IoT.

4.3 Mirai Botnet

Για την επίθεση χρησιμοποιήθηκε το Mirai botnet. Η δημιουργία του botnet, βασίστηκε στις οδηγίες ευρισκόμενες στο github [9]. Για την σωστή ενσωμάτωση του κακόβουλου κώδικα στον πειραματικό σχεδιασμό, τα απαιτούμενα μέρη του μετατράπηκαν σε Docker containers. Οι εντολές δημιουργίας του botnet, παρατίθενται στα αρχεία: α) Εντολές δημιουργίας bot -Dockerfile [10] και β) Εντολές δημιουργίας cnc -Dockerfile [11]. Το bot και το cnc, συνδέονται στο docker δίκτυο "experiment_net".

4.4 Το Νευρωνικό Δίκτυο

Το κεντρικό τμήμα του συστήματος ανίχνευσης botnet του πειράματος, βασίζεται στην τεχνολογία νευρωνικών δικτύων, και πιο συγκεκριμένα στα ANN [20]. Η επιλογή της προαναφερθείσας τεχνολογίας, στηρίζεται στο γεγονός ότι το τοπίο διαδικτυακών απειλών, είναι δυναμικό και απρόβλεπτο. Παράλληλα με την αύξηση της χρήσης δικτύων, εξελίσσονται και οι σχετικές με αυτά απειλές. Παρατηρούμε την εμφάνιση νέων τύπων απειλών/εισβολών,

[9] https://github.com/jgamblin/Mirai-Source-Code
[10] https://github.com/anarchos78/iot-blockchain-ml-botnet-experiment/blob/master/project-files/docker_files/mirai/bot/Dockerfile
[11] https://github.com/anarchos78/iot-blockchain-ml-botnet-experiment/blob/master/project-files/docker_files/mirai/cnc/Dockerfile

που τα "παραδοσιακά" IDS και IPS [26] δεν μπορούν να εντοπίσουν. Τα συστήματα αυτά, περιορίζονται στην στατική ανάλυση πακέτων, δηλαδή αναλύουν την δικτυακή κίνηση με τα ψηφιακά αποτυπώματα γνωστών απειλών. Γίνεται κατανοητό, ότι είναι αποδοτικά με τις ήδη γνωστές απειλές, αλλά με τις άγνωστες/πρωτόγνωρες, το ποσοστό αποτυχίας ανίχνευσης είναι μεγάλο.

Σε αντίθεση με τα "παραδοσιακά" IDS και IPS, τα συστήματα εντοπισμού απειλών που βασίζονται στην δυναμική ανίχνευση ανωμαλιών δικτυακής κίνησης, φαίνεται να είναι πλέον αποδοτικά για άγνωστες απειλές. Τα ANNs, είναι το μέσο επιλογής για την μοντελοποίηση δυναμικής συμπεριφοράς απειλών. Τα νευρωνικά δίκτυα, προσφέρουν την δυνατότητα εύρεσης βέλτιστου μοντέλου ενός συστήματος, με την βοήθεια πρότερης γνώσης για το καθαυτό σύστημα.

Για την δημιουργία του μοντέλου εντοπισμού ανωμαλιών/απειλών από botnet, ακολουθηθήκαν τα παρακάτω βήματα:

1) Επιλογή δεδομένων εκπαίδευσης του δικτύου. Η επιθυμητή απόδοση του τελικού μοντέλου, είναι η επιτυχής ανίχνευση απειλής για την οποία δεν έχει εκπαιδευτεί. Για να επιτευχθεί ο παραπάνω στόχος, τα δεδομένα εκπαίδευσης θα πρέπει να πληρούν τα εξής κριτήρια:

    - Να περιέχουν ικανοποιητικό αριθμό δικτυακής κίνησης botnet. Ο μικρός αριθμός botnet, δεν μπορεί να διασφαλίσει την ποικιλία που απαιτείται κατά την εκπαίδευση, με συνέπεια την φτωχή απόδοση ανίχνευσης.

    - Να είναι "ρεαλιστικά". Η κακόβουλη δικτυακή κίνηση, θα πρέπει να αντικατοπτρίζει την πραγματική συμπεριφορά ενός botnet. Η δικτυακή κίνηση παραχθείσα σε ελεγχόμενο περιβάλλον, δεν μπορεί απεικονίσει την πραγματική λειτουργία του κακόβουλου λογισμικού, καθώς είναι αποτέλεσμά χρονικά βεβιασμένων προσεγγίσεων, που δεν δίνουν τον απαιτούμενο χρόνο στο κακόβουλο λογισμικό, να εκδηλώσει όλη την λειτουργικότητα του.

• Τα δεδομένα θα πρέπει να περιέχουν, όχι μόνο κακόβουλη δικτυακή κίνηση, αλλά και επιθυμητή/καλόβουλη κίνηση. Αυτός ο συνδυασμός, προσομοιώνει την πραγματική δικτυακή κίνηση, που θα αντιμετωπίσει το μοντέλο ανίχνευσης.

Το σετ εκπαιδευτικών δεδομένων που κρίθηκε κατάλληλο για το ANN, είναι το Botnet dataset [12] [6] από το "Canadian Institute for Cybersecurity" (Πίνακας 4.3 σελίδα 52).

Botnet name	Type	Portion of flows in dataset
Neris	IRC	21159 (12%)
Rbot	IRC	39316 (22%)
Virut	HTTP	1638 (0.94%)
NSIS	P2P	4336 (2.48%)
SMTP	P2P	11296 (6.48%)
Zeus	P2P	31 (0.01%)
Zeus control (C & C)	P2P	20 (0.01%)

Πίνακας 4.3: Distribution of botnet types in the training dataset.

2) Προετοιμασία δεδομένων για την εκπαίδευση του νευρωνικού δικτύου. Για την τροφοδότηση του ANN, πραγματοποιήθηκε προετοιμασία των δεδομένων η οποία περιέλαβε:

- Την εξαγωγή Bidirectional Flows (biflow) από το Botnet dataset -αρχείο τύπου pcap. Το textlatinbiflow, είναι μια αμφίδρομη δομή ροής δικτυακής κυκλοφορίας. Κάθε ροή δείχνει: α) την προς τα εμπρός (outbound traffic) επικοινωνία (αποστολή πακέτο δεδομένων) της πηγής με τον προορισμό και β) την αντίστροφη (inbound traffic) επικοινωνία από τον προορισμό προς την πηγή. Η biflow δομή, αποδεικνύεται ιδιαίτερα αποδοτική για την εκπαίδευση ANN [9]. Το λογισμικό CICFLOWMETER [13] χρησιμοποιήθηκε για την εξαγωγή των χαρακτηριστικών [14] (features) εκπαίδευσης του μοντέλου [18] [35], σε αρχείο τύπου csv.
- Την κανονικοποίηση των δεδομένων. Για την σωστή τροφοδοσία του

[12] https://www.unb.ca/cic/datasets/botnet.html
[13] https://github.com/ISCX/CICFlowMeter
[14] http://www.netflowmeter.ca/netflowmeter.html

ANN τα δεδομένα πρέπει να είναι:

- αριθμητικά, λόγω του ότι όλα τα στοιχεία στο σετ τροφοδοσίας δεν είναι αριθμητικά,
- να εντάσσονται σε μια συγκεκριμένη κλίμακα (0-1) έτσι ώστε να είναι συγκρίσιμα.

Επίσης, η κανονικοποίηση συμβάλλει στη μείωση του χρόνου εκπαίδευσης.

- Την διάκριση και τιτλοφόρηση (labeling) των biflow σε κακόβουλα και καλόβουλα.
- Την εγγραφή και αποθήκευση [15] των επεξεργασμένων δεδομένων σε κατάλληλη μορφή (NumPy array [16])

Ο σχετικός με την προετοιμασία πηγαίος κώδικας βρίσκεται στο process_dataset.py[17].

3) Κατασκευή του ANN. Για την σύνθεση του δικτύου χρησιμοποιήθηκε το TensorFlow[18] και το Keras [19]. Οι δύο αυτές βιβλιοθήκες ανοικτού λογισμικού, καθιστούν τον πειραματισμό με νευρωνικά δίκτυα προσιτό, καθώς δεν απαιτούν υψηλού επιπέδου γνώση της λειτουργίας, και της θεωρίας της μηχανικής μάθησης για την κατασκευή ενός δικτύου [28] [23]. Η δομή του ANN (Σχήμα 4.2 σελίδα 54) αποτελείται από:

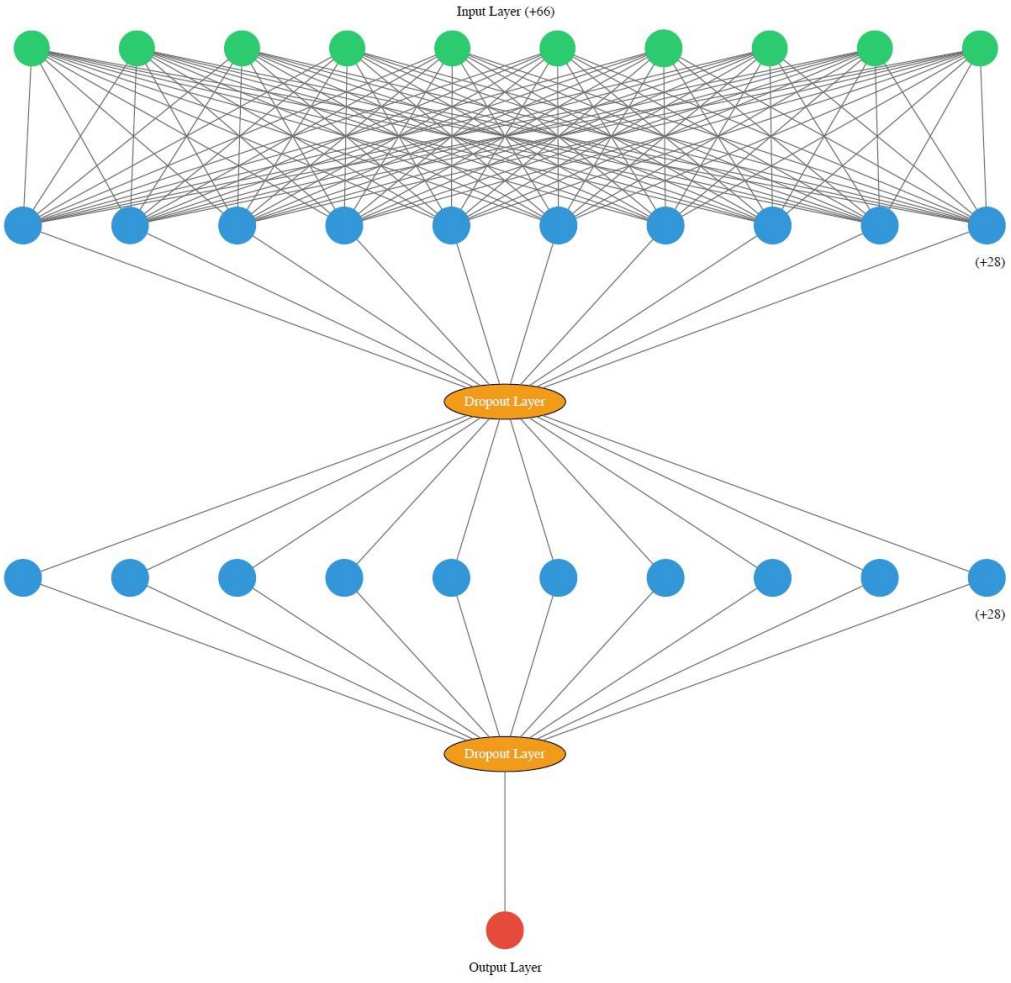
- εβδομήντα έξι (76) νευρώνες εισόδου (input layer),
- τριάντα οκτώ (38) υπολογιστικούς νευρώνες (hidden layer),
- επίπεδο απενεργοποίησης μέρους -20%- νευρώνων (dropout layer) [55],

[15] https://github.com/anarchos78/iot-blockchain-ml-botnet-experiment/tree/master/project-files/create_prediction_model/dumps
[16] https://docs.scipy.org/doc/numpy/reference/generated/numpy.array.html
[17] https://github.com/anarchos78/iot-blockchain-ml-botnet-experiment/blob/master/project-files/create_prediction_model/process_dataset.py
[18] https://github.com/tensorflow/tensorflow
[19] https://github.com/keras-team/keras

- τριάντα οκτώ (38) υπολογιστικούς νευρώνες (hidden layer),

- επίπεδο απενεργοποίησης μέρους -20%- νευρώνων (dropout layer),

- ένα (1) νευρώνα εξόδου (καθορισμός κλάσης του biflow σε καλόβουλο ή κακόβουλο)

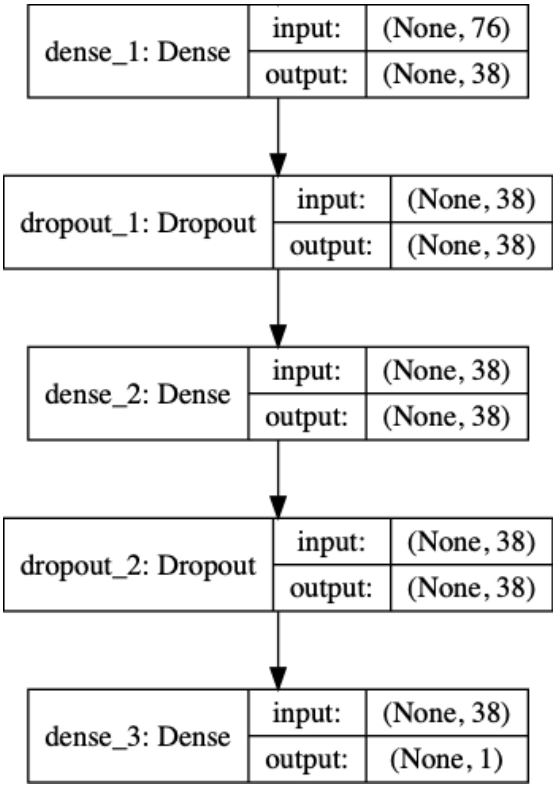


Σχήμα 4.2: Δομή του ANN.

Τα χαρακτηριστικά του νευρωνικού δικτύου συνοψίζονται στον Πίνακα 4.4 σελίδα 55 και στο (Σχήμα 4.3 σελίδα 55).

Layer (type)	Output Shape	Parameters (weights) #
dense_1 (Dense)	(None, 38)	2926
dropout_1 (Dropout)	(None, 38)	0
dense_2 (Dense)	(None, 38)	1482
dropout_2 (Dropout)	(None, 38)	0
dense_3 (Dense)	(None, 1)	39
Total params: 4447		
Trainable params: 4447		
Non-trainable params: 0		

Πίνακας 4.4: Output shape and number of weights in each layer.



Σχήμα 4.3: Plot of neural network model graph.

Για την εξεύρεση των καλύτερων παραμέτρων του ANN, χρησιμοποιήθηκε η κλάση RandomizedSearchCV[20] της βιβλιοθήκης λογισμικού Scikit. Με την κλάση αυτή, δοκιμαστήκαν όλοι οι παρακάτω πιθανοί συνδυασμοί παραμέτρων:

[20] https://scikit-learn.org/stable/modules/generated/sklearn.model_selection.RandomizedSearchCV.html

```
{
    'batch_size': [32, 64, 128, 256, 512],
    'epochs': [256, 512],
    'optimizer': ['adam', 'rmsprop'],
    'activation': ['relu', 'linear'],
    'dropout': [0.2, 0.25, 0.3]
}
```

Ο βέλτιστος συνδυασμός παραμέτρων για το νευρωνικό δίκτυο του πειράματος είναι:

```
{
    'batch_size': 128,
    'epochs': 512,
    'optimizer': 'rmsprop',
    'activation': 'relu',
    'dropout': 0.2
}
```

Ο σχετικός πηγαίος κώδικας βρίσκεται στο optimize_ann.py [21] και final_model_training.py [22].

4) Αξιολόγηση του τελικού μοντέλου. Η απόδοση του τελικού μοντέλου είναι ικανοποιητική, βάσει δοκιμών σε τμήμα -33%- του σετ δεδομένων εκπαίδευσης. Ο Πίνακας 4.5 σελίδα 56, δείχνει τον πίνακα σύγχυσης (confusion matrix) των προβλέψεων του μοντέλου επί των δεδομένων εκπαίδευσης.

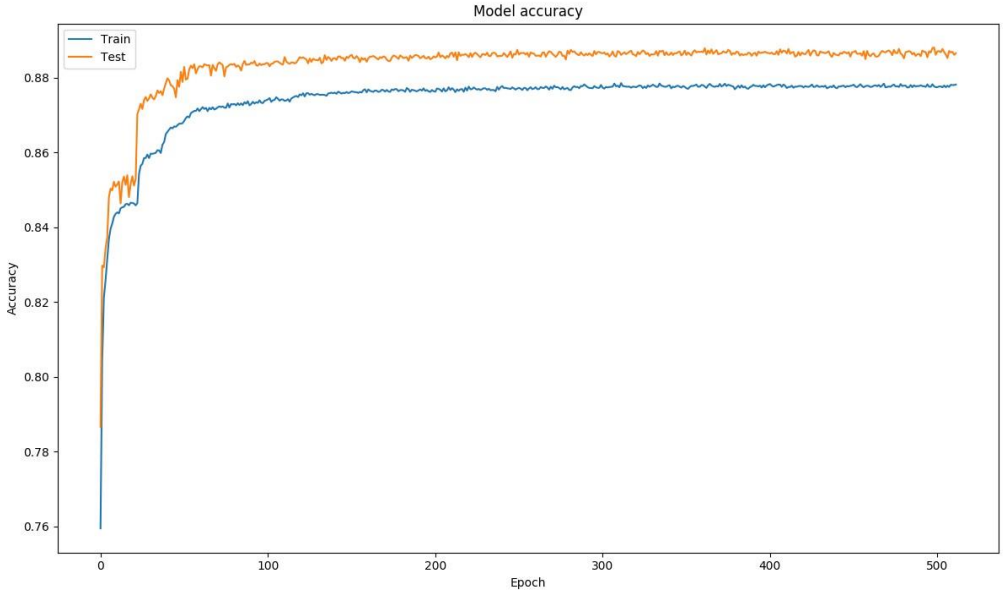
24513	1862
6412	38445

Πίνακας 4.5: Confusion Matrix.

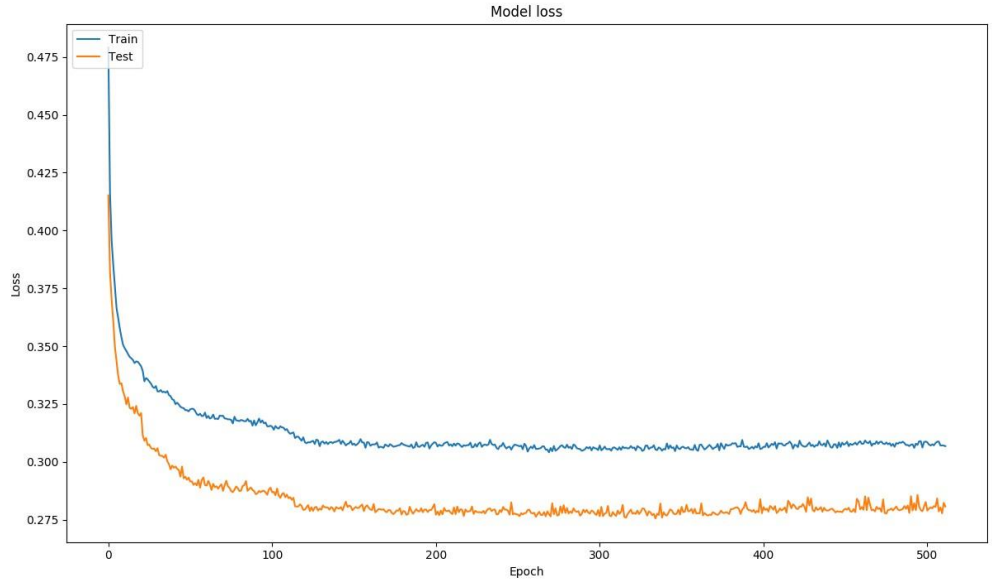
Ο δείκτης ακριβείας -accuracy- του μοντέλου είναι 88,38%, και ο δείκτης απώλειας -loss- 28,18%. Στο (Σχήμα 4.4 σελίδα 57), φαίνεται η βελτίωση του δείκτη ακριβείας, σε

[21] https://github.com/anarchos78/iot-blockchain-ml-botnet-experiment/blob/master/project-files/create_prediction_model/optimize_ann.py
[22] https://github.com/anarchos78/iot-blockchain-ml-botnet-experiment/blob/master/project-files/create_prediction_model/final_model_training.py

σχέση με τους κύκλους μάθησης (epochs), και στο (Σχήμα 4.5 σελίδα 57), φαίνεται η μείωση του δείκτη απώλειας, στην ανάλογη σχέση του με τους κύκλους μάθησης.



Σχήμα 4.4: Model accuracy over epochs.



Σχήμα 4.5: Model loss over epochs.

4.5 Το Δίκτυο Blockchain

Μία από τις βασικές προκλήσεις του IoT είναι η ασφάλεια. Τα εγγενή χαρακτηριστικά ασφάλειας, καθώς και η μη κεντρική αρχιτεκτονική του blockchain, οδήγησαν στην συμπερίληψη του στο πειραματικό σύστημα. Το blockchain είναι υπεύθυνο, για την καταγραφή συμβάντων σχετικών με την ασφάλεια του IoT δικτύου, καθώς επίσης και για την ενημέρωση του διαχειριστή, για την περίπτωση έκθεσης IoT αντικειμένων σε απειλή. Η συνδυαστική χρήση blockchain και τεχνολογίας IoT, φαίνεται να παρουσιάζει πολυεπίπεδο ενδιαφέρον [50]. Για το σκοπό του πειράματος, χρησιμοποιήθηκε το multichain[23][24] ως blockchain τεχνολογία. Η προαναφερθείσα τεχνολογία, προσφέρει δυνατότητα γρήγορης δημιουργίας ιδιωτικού δικτύου blockchain, και εύκολης ενσωμάτωσης του, σε ήδη υπάρχοντα οικοσυστήματα λογισμικού. Η ενσωμάτωση του Multichain στο πείραμα, πραγματοποιήθηκε με την μετατροπή του σε Docker containers. Οι εντολές δημιουργίας του botnet, παρατίθενται στα αρχεία: α) multichain master node-Dockerfile [25] και β) multichain slave node-Dockerfile [26].

Συγκεκριμένα στο blockchain, καταγράφεται το "επίπεδο εμπιστοσύνης" (trust level) για κάθε IoT αντικείμενο ξεχωριστά. Τα διαθέσιμα επίπεδα εμπιστοσύνης είναι: low, normal και high. Κατά την αρχικοποίηση του πειράματος, το trust level για όλα τα αντικείμενα θεωρείται "high". Στην περίπτωση ανίχνευσης απειλής από το σύστημα ανάλυσης δικτυακής κίνησης, το trust level καταγράφεται στο blockchain ως "low". Η καταγραφή "low" ενεργοποιεί την εκτέλεση βοηθητικού προγράμματος multichain.py [27], το οποίο καταγράφει το γεγονός στο αρχείο "iot-trust-level.log" για την ενημέρωση του διαχειριστή του συστήματος. Η χρήση blockchain στο σύστημα, απέδειξε ότι:

1) Συμβάλει στην ενίσχυση της αξιοπιστίας και της ανιχνευσιμότητας περιστατικών ασφάλειας εντός του IoT δικτύου. Καμία οντότητα δεν μπορεί να τροποποιήσει τις εγγραφές στο blockchain του συστήματος, με σκοπό την απόκρυψη ιχνών κακόβουλων ενεργειών.

[23] https://www.multichain.com/
[24] https://www.multichain.com/download/MultiChain-White-Paper.pdf
[25] https://github.com/anarchos78/iot-blockchain-ml-botnet-experiment/blob/master/project-files/docker_files/kunstmaan-master-multichain/Dockerfile
[26] https://github.com/anarchos78/iot-blockchain-ml-botnet-experiment/blob/master/project-files/docker_files/kunstmaan-node-multichain/Dockerfile
[27] https://github.com/anarchos78/iot-blockchain-ml-botnet-experiment/blob/master/project-files/multichain_notification/multichain.py

2) Με την χρήση του blockchain smart contact χαρακτηριστικού, ο διαχειριστής του συστήματος ενημερώνεται για τα περιστατικά ασφάλειας του δικτύου IoT, στον σωστό χρόνο και με την σωστή/φύσει αδιάβλητη πληροφορία. Δυνητικά, το smart contract μπορεί να βοηθήσει στην πρόληψη εξάπλωσης απειλής, απενεργοποιώντας αυτόματα την εκτεθειμένη IoT συσκευή.

3) Η αποκεντρωμένη φύση του blockchain, αποτρέπει την αποτυχία "ενός σημείου" του συστήματος ενημέρωσης.

4) Μπορεί να επεκταθεί ευκολά και με χαμηλό κόστος, εν συγκρίσει με μια κεντρική υποδομή.

4.6 Βοηθητικό Λογισμικό

Παρακάτω, παρατίθεται το βοηθητικό λογισμικό του πειράματος, καθώς και μια σύντομη περιγραφή:

- Vagrantfile [28], είναι υπεύθυνο για την ενορχήστρωση και την αρχικοποίηση του πειράματος. Στο εν λόγω αρχείο, καθορίζονται όλες οι παράμετροι του συστήματος, μέσω μεταβλητών. Οι σημαντικότερες μεταβλητές είναι:

    - IOT_OBJECTS: καθορίζει τον αριθμό των IoT αντικείμενων του πειράματος.

    - SNIFF_TIMEOUT: καθορίζει το χρονικό διαστήματα ανάλυσης της κίνησης στο δίκτυο IoT, σε δευτερόλεπτα.

    - RETARIN_MODEL: η μεταβλητή αυτή καθορίζει, την επαναδημιουργία του μοντέλου κατά την αρχικοποίηση. Η τιμή 0 συμβολίζει "ΟΧΙ", και η τιμή 1, "ΝΑΙ". Η χρήση της μεταβλητής είναι απαραίτητη, στην περίπτωση αλλαγής των μεταβλητών του μοντέλου εντοπισμού απειλών.

    - FIND_OPTIMUM_ANN_PARAMETERS: αυτή η μεταβλητή χρησιμοποιείται σε συναρμογή με την προηγούμενη, και καθορίζει, αν κατά την αρχικοποίηση του

[28] https://github.com/anarchos78/iot-blockchain-ml-botnet-experiment/blob/master/Vagrantfile

συστήματος, θα πρέπει να βρεθούν οι βέλτιστες παράμετροι, του υπό εκπαίδευση μοντέλου.

- DOCKER_NETWORK_SUBNET: καθορίζει των αριθμό των IoT αντικειμένων. Η προκαθορισμένη τιμή (192.168.0.0/16), δίνει την δυνατότητα για 65.536 IP διευθύνσεις.

- VIRTUALBOX_CPUS: ορίζει των αριθμό εικονικών πυρήνων επεξεργαστή για το εικονικό περιβάλλον του συστήματος.

- VIRTUALBOX_MEMORY: ορίζει την RAM του εικονικού περιβάλλοντος του συστήματος, σε MB. Οι μεταβλητές VIRTUALBOX_CPUS και VIRTUALBOX_MEMORY, καθορίζουν την απόδοση του συστήματος.

- start_experiment.sh [29], εκτελέσιμο αρχείο που ξεκινά το πείραμα μέσω του Vagrantfile. Το αρχείο αυτό, δίνει την δυνατότητα αρχικοποίησης του συστήματος, με τροποποιημένες τιμές μεταβλητών, εντός του εικονικού περιβάλλοντος. Θα πρέπει να προηγηθεί, καταστροφή - teardown- του συστήματος, με το αρχείο stop_experiment.sh.

- stop_experiment.sh [30], εκτελέσιμο αρχείο που σταματά το πείραμα, εντός του εικονικού περιβάλλοντος. Χρήσιμο στην περίπτωση επανεκκίνησης του πειράματος, με διαφορετικές από τις αρχικές παραμέτρους.

- create_docker_compose.py [31], πρόγραμμα δημιουργίας του αρχείου ενορχήστρωσης της υποδομής docker. Η υποδομή περιλαμβάνει: α) το δίκτυο " experiment_net", β) τα IoT αντικείμενα, γ) το mirai botnet, δ) το δίκτυο blockchain -multichain.

- iot_requester.py [32], πρόγραμμα παραγωγής θεμιτής δικτυακής κίνησης, εντός του δικτύου IoT.

[29] https://github.com/anarchos78/iot-blockchain-ml-botnet-experiment/blob/master/project-files/start_experiment.sh
[30] https://github.com/anarchos78/iot-blockchain-ml-botnet-experiment/blob/master/project-files/stop_experiment.sh
[31] https://github.com/anarchos78/iot-blockchain-ml-botnet-experiment/blob/master/project-files/create_docker_compose.py
[32] https://github.com/anarchos78/iot-blockchain-ml-botnet-experiment/blob/master/project-files/iot_requester.py

- iot_network_watcher.py [33], πρόγραμμα σύλληψης δικτυακής κίνησης στο δίκτυο IoT. Εκτελεί τις απαραίτητες εργασίες, για την σύλληψη και μετατροπή της δικτυακής κίνησης, σε ενδεδειγμένη για το μοντέλο ανάλυσης μορφή. Οι παραπάνω εργασίες εκτελούνται παράλληλα και ανά IoT συσκευή.

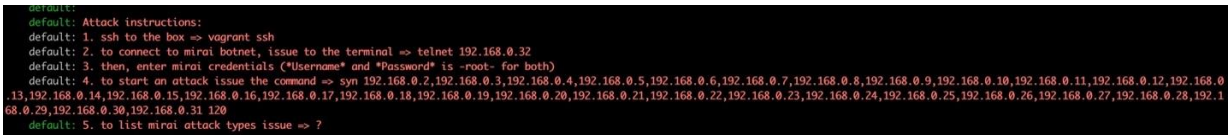
- detect_malicious_traffic.py [34], πρόγραμμα ανάλυσης της συλληφθείσας δικτυακής κίνησης. Στο παρόν αρχείο, πραγματοποιείται η διάκριση της κίνησης, σε καλόβουλη ή κακόβουλη. Σε περίπτωση εντοπισμού κακόβουλης κίνησης, καταγράφεται στο blockchain, "low" επίπεδο ασφάλειας, για το υπό εξέταση IoT αντικείμενο.

Ο πηγαίος κώδικας του πειράματος, είναι διαθέσιμος στο αποθετήριο κώδικα github [35].

[33] https://github.com/anarchos78/iot-blockchain-ml-botnet-experiment/blob/master/project-files/iot_network_watcher.py
[34] https://github.com/anarchos78/iot-blockchain-ml-botnet-experiment/blob/master/project-files/detect_malicious_traffic.py
[35] https://github.com/anarchos78/iot-blockchain-ml-botnet-experiment

Κεφάλαιο 5
Πειραματικά Αποτελέσματα

Για την αρχικοποίηση του πειράματος, από τον φάκελο του πηγαίου κώδικα iot-blockchain-ml-botnet-experiment [36] σε μια κονσόλα εκσφαλμάτωσης/γραμμή εντολών (terminal), η εντολή vagrant up, επιτελεί τις απαραίτητες διαδικασίες δημιουργίας και παραμετροποίησης, του εικονικού περιβάλλοντος του πειράματος. Η διαδικασίας είναι χρονοβόρα, και εξαρτάται από τον αριθμό αντικείμενων IoT. Ο αριθμός IoT αντικειμένων του παρόντος πειράματος, είναι 30. Μετά το πέρας δημιουργίας του πειραματικού περιβάλλοντος, στην γραμμή εντολών εμφανίζονται οδηγίες, για την διεξαγωγή επίθεσης στο δίκτυο IoT με το Mirai botnet (Σχήμα 5.1 σελίδα 62).



Σχήμα 5.1: Πέρας αρχικοποίησης και οδηγίες επίθεσης.

Για την έναρξη επίθεσης, είναι απαραίτητη η είσοδος στο εικονικό περιβάλλον με την εντολή vagrant ssh, και στην συνέχεια η είσοδος στο botnet με την εντολή telnet 192.168.0.32 (το Username και το Password είναι root) (Σχήμα 5.2 σελίδα 62).

Σχήμα 5.2: Είσοδος στο botnet.

[36] https://github.com/anarchos78/iot-blockchain-ml-botnet-experiment

Η εντολή "?", εκτυπώνει στην γραμμή εντολών, την λίστα με τους τύπους επιθέσεων του botnet (Σχήμα 5.3 σελίδα 63).

```
root@botnet# ?
Available attack list
greeth: GRE Ethernet flood
udp: UDP flood
dns: DNS resolver flood using the targets domain, input IP is ignored
syn: SYN flood
stomp: TCP stomp flood
greip: GRE IP flood
vse: Valve source engine specific flood
ack: ACK flood
udpplain: UDP flood with less options. optimized for higher PPS
http: HTTP flood

root@botnet#
```

Σχήμα 5.3: Τύποι επιθέσεων του Mirai botnet.

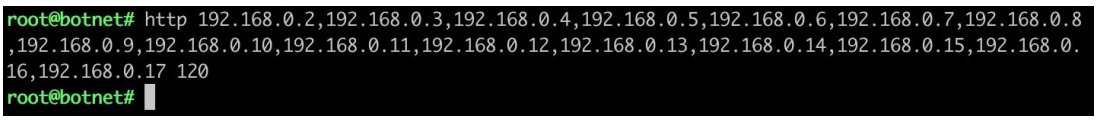
Για την διερεύνηση της απόδοσης του συστήματος, ακολουθήθηκαν τα παρακάτω βήματα:

1. Ολιγόλεπτη αναμονή πριν την επίθεση, για την σύλληψη καλόβουλης δικτυακής κυκλοφορίας.
2. Επίθεση τύπου ack για 120 δευτερόλεπτα στα IoT με IP: 192.168.0.2, 192.168.0.3, 192.168.0.4, 192.168.0.5, 192.168.0.6, 192.168.0.7, 192.168.0.8, 192.168.0.9, 192.168.0.10, 192.168.0.11, 192.168.0.12, 192.168.0.13, 192.168.0.14, 192.168.0.15, 192.168.0.16, 192.168.0.17, 192.168.0.18 και 192.168.0.19 (Σχήμα 5.4 σελίδα 63).

```
root@botnet# ack 192.168.0.2,192.168.0.3,192.168.0.4,192.168.0.5,192.168.0.6,192.168.0.7,192.168.0.8,
192.168.0.9,192.168.0.10,192.168.0.11,192.168.0.12,192.168.0.13,192.168.0.14,192.168.0.15,192.168.0.1
6,192.168.0.17,192.168.0.18,192.168.0.19 120
root@botnet#
```

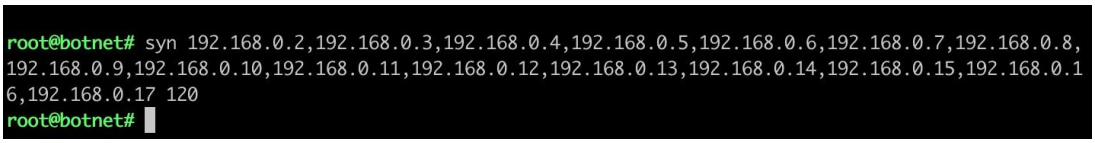
Σχήμα 5.4: Επίθεση ack.

3. Ολιγόλεπτη αναμονή πριν την επόμενη επίθεση.
4. Επίθεση τύπου http για 120 δευτερόλεπτα στα IoT με IP: 192.168.0.2, 192.168.0.3, 192.168.0.4, 192.168.0.5, 192.168.0.6, 192.168.0.7, 192.168.0.8, 192.168.0.9, 192.168.0.10, 192.168.0.11, 192.168.0.12, 192.168.0.13, 192.168.0.14, 192.168.0.15, 192.168.0.16, και 192.168.0.17 (Σχήμα 5.5 σελίδα 64).



Σχήμα 5.5: Επίθεση http.

5. Ολιγόλεπτη αναμονή πριν την επόμενη επίθεση.
6. Επίθεση τύπου syn για 120 δευτερόλεπτα στα IoT με IP: 192.168.0.2, 192.168.0.3, 192.168.0.4, 192.168.0.5, 192.168.0.6, 192.168.0.7, 192.168.0.8, 192.168.0.9, 192.168.0.10, 192.168.0.11, 192.168.0.12, 192.168.0.13, 192.168.0.14, 192.168.0.15, 192.168.0.16, και 192.168.0.17 (Σχήμα 5.6 σελίδα 64).



Σχήμα 5.6: Επίθεση syn.

7. Ολιγόλεπτη αναμονή πριν τον τερματισμό του πειράματος. για την σύλληψη καλόβουλης δικτυακής κυκλοφορίας.
8. Τερματισμός επίθεσης.

Το πείραμα εκτελέστηκε για 25 λεπτά και 7 δευτερόλεπτα, και αναλύθηκαν πάνω από 800.000 πακέτα στο χρονικό αυτό διάστημα.

Παρατίθεται η σύνοψη των αποτελεσμάτων:

- Για τα πρώτα 3 λεπτά και 53 δευτερόλεπτα του πειράματος, (2019-05-04 13:00:07 μέχρι 2019-05-04 13:03:59) δεν διενεργήθηκε καμία επίθεση. Στο διάστημα αυτό, καταγράφηκε "low trust level" για τα IoT "remote-thermometer-19", και "remote-thermometer-29". Καταγράφηκαν λανθασμένα περιστατικά για 2 από τα 30 IoT αντικείμενα.

- Τα επόμενα 2 λεπτά εκτελέστηκε επίθεση ack (2019-05-04 13:04:00 μέχρι 2019-05-04 13:05:59). Το σύστημα εντόπισε επιτυχώς, όλα τα περιστατικά σχετικά με τα IoT που δέχθηκαν επίθεση. Καταγράφηκαν λανθασμένα περιστατικά, για 11 από τα 30 IoT αντικείμενα.

- Για τα επόμενα 3 λεπτά δεν διενεργήθηκε καμία επίθεση (2019-05-04 13:06:00 μέχρι 2019-05-04 13:09:59). Καταγράφηκαν λανθασμένα περιστατικά, για 13 από τα 30 IoT αντικείμενα.

- Στα επόμενα 2 λεπτά εκτελέστηκε επίθεση http (2019-05-04 13:10:00 μέχρι 2019-05-04 13:11:59). Το σύστημα εντόπισε επιτυχώς, όλα τα περιστατικά σχετικά με τα IoT, που δέχθηκαν επίθεση και καταγράφηκαν λανθασμένα περιστατικά, για 6 από τα 30 IoT αντικείμενα.

- Για τα επόμενα 3 λεπτά, δεν διενεργήθηκε καμία επίθεση (2019-05-04 13:12:00 μέχρι 2019-05-04 13:15:59). Καταγράφηκαν λανθασμένα περιστατικά, για 11 από τα 30 IoT αντικείμενα.

- Στα επόμενα 2 λεπτά εκτελέστηκε επίθεση syn (2019-05-04 13:16:00 μέχρι 2019-05-04 13:17:59). Το σύστημα εντόπισε επιτυχώς, όλα τα περιστατικά σχετικά με τα IoT που δέχθηκαν επίθεση, και καταγράφηκαν λανθασμένα περιστατικά, για 7 από τα 30 IoT αντικείμενα.

- Μέχρι την λήξη του πειράματος, δεν εκτελέστηκε καμία επίθεση (2019-05-04 13:18:00 μέχρι 2019-05-04 13:25:14). Καταγράφηκαν λανθασμένα περιστατικά, για 16 από τα 30 IoT αντικείμενα.

Κεφάλαιο 6
Συμπεράσματα

Αρχικά πραγματοποιήθηκε ο καθορισμός του ερευνητικού πλαισίου, με την μελέτη σύγχρονης βιβλιογραφίας, σχετική με τις επιμέρους τεχνολογίες που εξετάζει η παρούσα έρευνα. Έπειτα, παρατέθηκε το γνωστικό πλαίσιο της διατριβής, στο οποίο αναλύθηκαν οι τεχνολογικές επιλογές του πειραματικού συστήματος. Στην συνέχεια, παρουσιάστηκε ο πειραματικός σχεδιασμός, στον οποίο δόθηκε έμφαση στην τεχνολογική περιγραφή. Τέλος, παρατίθενται η εκτέλεση του πειράματος, καθώς και τα πειραματικά αποτελέσματα.

Ο κύριος στόχος της έρευνας, ήταν η δημιουργία ενός αποδοτικού συστήματος, για την σύλληψη και διαχείριση δικτυακής κίνησης ενός δικτύου IoT, με σκοπό την πρόληψη και τον εντοπισμό επιθέσεων σε αυτό. Το σημαντικότερο χαρακτηριστικό του δημιουργηθέντος συστήματος, είναι η σπονδυλωτή δομή του. Η εύκολη τροποποίηση του, προσφέρει την δυνατότητα κατασκευής νέων πειραματικών συστημάτων, που μπορούν να αποτελέσουν βάση για μελλοντικές έρευνες. Έτσι, τα τέσσερα πρώτα ερευνητικά αντικείμενα (σελίδα 2) προσεγγίστηκαν επιτυχώς. Πιο αναλυτικά:

1) Επιτεύχθηκε η δημιουργία ενός πειραματικού περιβάλλοντος, για μελέτη επιθέσεων σε δίκτυο IoT.

2) Το δημιουργηθέν πειραματικό περιβάλλον, μπορεί εύκολα να επεκταθεί για μελλοντική έρευνα απειλών IoT.

3) Το σύστημα εντοπισμού, διαχείρισης και ανάλυσης δικτυακής κίνησης, είναι πραγματικού χρόνου.

4) Η τεχνολογία blockchain, αποδεικνύεται ότι μπορεί να συνδυαστεί με την τεχνολογία IoT, για την αποθήκευση δεδομένων μικρού όγκου.

Πρέπει να αναφερθεί, ότι η χρήση φυσικών IoT συσκευών για την δημιουργία του συστήματος, δεν ήταν δυνατή. Τα κύρια εμπόδια ήταν:

1) το υψηλό κόστος απόκτησης του απαραίτητου εξοπλισμού,

2) οι φυσικοί περιορισμοί, επί παραδείγματι, η αδυναμία τοποθέτησης IoT συσκευών σε απομακρυσμένα γεωγραφικά σημεία.

Τα παραπάνω εμπόδια, περιόρισαν το επίπεδο εξομοίωσης των IoT αντικειμένων, στην αναπαραγωγή της δικτυακής συμπεριφοράς τους. Έτσι, δεν αναπαράχθηκε το φυσικό επίπεδο (hardware) και το firmware των θερμοκρασιακών αισθητήρων. Δόθηκε βάρος, στην εξομοίωση του δικτυακού σχεδιασμού. Οι σχεδιαστικές αυτές επιλογές, δεν αλλοίωσαν την πραγματική φύση του IoT (αυτοδυναμία και ανεξαρτησία). Ο σκοπός των εξομοιωμένων συσκευών, ήταν η συλλογή θερμοκρασιακών δεδομένων, με σκοπό την προώθηση τους, για περεταίρω επεξεργασία.

Ένα σύστημα πραγματικού χρόνου, είναι ένα οποιοδήποτε σύστημα επεξεργασίας πληροφορίων, που ανταποκρίνεται σε εξωτερικά ερεθίσματα εισόδου, μέσα σε ένα καθορισμένο και πεπερασμένο χρονικό πλαίσιο. Η ορθότητα των αποτελεσμάτων του συστήματος, εξαρτάται όχι μόνο από το λογικό αποτέλεσμα επεξεργασίας, αλλά και από τον χρόνο παράδοσης. Επιπλέον, η αποτυχία παράδοσης του αποτελέσματος επεξεργασίας, από ένα σύστημα πραγματικού χρόνου, είναι το ίδιο ανεπιθύμητη, όσο και η παράδοση λάθος αποτελέσματος. Στο πλαίσιο του σχεδιασθέντος συστήματος, ο χρόνος ανάλυσης δικτυακής κίνησης είναι πραγματικός. Η ενημέρωση του διαχειριστή συστήματος, είναι 10 δευτερόλεπτα. Ο χρόνος αυτός μπορεί να ρυθμιστεί, με την μεταβλητή "SNIFF_TIMEOUT" [37], πριν την αρχικοποίηση του συστήματος. Επιπλέον, η ενημέρωση του διαχειριστή μπορεί να πραγματοποιηθεί με διάφορους τρόπους, λ.χ. με email ή/και SMS, τροποποιώντας το αρχείο multichain.py [38].

Λαμβάνοντας υπόψη την ραγδαία εξάπλωση της τεχνολογίας IoT, η διευθυνσιοδότηση IoT με IPv4 διευθύνσεις, δεν θα είναι δυνατή στο άμεσο μέλλον. Ο λόγος είναι ότι ο αριθμός IPv4 διευθύνσεων δεν είναι επαρκής (4.294.967.296), για την διασύνδεση, τόσο των υπαρχόντων όσο και των υπό δημιουργία IoT αντικείμενων. Ως μια λύση στον περιορισμένο αριθμό IP, είναι το νέο

[37] https://github.com/anarchos78/iot-blockchain-ml-botnet-experiment/blob/7e3a8b69eb93e558be960b75208d00ed1d31404d/Vagrantfile#L5
[38] https://github.com/anarchos78/iot-blockchain-ml-botnet-experiment/blob/master/project-files/multichain_notification/multichain.py

πρωτόκολλο IPv6, με 340.282.366.920.938.463.463.374.607.431.768.211.456 διευθύνσεις, αριθμός που κρίνεται επαρκής για αρκετά χρόνια. Άλλη λύση διευθυνσιοδότησης, είναι μέσω router/switch.

Τα IoT αντικείμενα του πειραματικού συστήματος, χρησιμοποιούν στατικές IPv4 διευθύνσεις. Εκ πρώτης όψεως, η χρήση IPv4, φαίνεται περιοριστική. Στον σχεδιασμό του συστήματος, ο μέγιστος προβλεπόμενος αριθμός στατικών IP διευθύνσεων, και κατά συνέπεια ο μέγιστος αριθμός IoT με στατική IP, είναι 65.536 (helpers.py [39]). Ο αριθμός των αντικειμένων, καθορίζεται κατά την αρχικοποίηση του πειράματος, μέσω της μεταβλητής "IOT_OBJECTS" [40]. Πρέπει να τονισθεί ότι η αρχικοποίηση του πειράματος με έναν μεγάλο αριθμό αντικειμένων, περιορίζεται από τους πεπερασμένους πόρους του host συστήματος.

Η χρήση μεγάλου αριθμού IoT συσκευών στο πλαίσιο του παρόντος σχεδιασμού, δεν είναι λογική, για τον λόγο ότι αναφερόμαστε σε ένα δίκτυο απομακρυσμένων θερμομέτρων στο Ηνωμένο Βασίλειο, όπου μερικές εκατοντάδες συσκευές, εξυπηρετούν άριστα τον σκοπό του συστήματος.

Στην περίπτωση που απαιτούντο ένας τεράστιος αριθμός IoT συσκευών, η προσέγγιση θα ήταν διαφορετική, συνυπολογίζοντας τις απαιτήσεις του πεδίου εφαρμογής. Για παράδειγμα, οι IoT συσκευές σε ένα σύστημα αυτοματισμού οικίας, δεν είναι απαραίτητο να διαθέτουν IP. Μπορούν να επικοινωνήσουν με άλλους τρόπους, όπως bluetooth ή RFID. Στην περίπτωση αναγκαστικής χρήσης IP, η διευθυνσιοδότηση μπορεί να πραγματοποιηθεί μέσω του router/switch. Το πειραματικό σύστημα, προσφέρει την δυνατότητα χρήσης του πρωτόκολλου IPv6 για την απόδοση διεύθυνσης, αλλά και την χρήση router για τον ίδιο σκοπό.

Συνοψίζοντας τα παραπάνω, ο σχεδιασμός του δικτύου IoT, ο σχεδιασμός του botnet, ο σχεδιασμός του συστήματος σύλληψης και ανάλυσης της δικτυακής κίνησης, αλλά και η συναρμογή όλων των παραπάνω, φαίνεται να αποτελούν μια στέρεα πειραματική βάση.

Η διάρκεια εκτέλεσης του πειράματος (25 λεπτά και 7 δευτερόλεπτα), μπορεί να γεννήσει ερωτήματα. Η απόφαση για την διάρκεια εκτέλεσης, βασίστηκε στο γεγονός, ότι για το εν λόγω χρονικό διάστημα, το σύστημα θα δέχονταν έναν καταιγισμό πακέτων (800.000 - 530 πακέτα

[39] https://github.com/anarchos78/iot-blockchain-ml-botnet-experiment/blob/master/project-files/utils/helpers.py
[40] https://github.com/anarchos78/iot-blockchain-ml-botnet-experiment/blob/7e3a8b69eb93e558be960b75208d00ed1d31404d/Vagrantfile#L4

ανά δευτερόλεπτο). Αυτός ο αριθμός πακέτων, αποδείχθηκε ικανοποιητικός για τον ερευνητικό σκοπό.

Σχετικά με το 5ο ερευνητικό αντικείμενο (σελίδα 2), παρατηρήθηκε αστοχία. Πρέπει να αναφερθεί ότι, η εξεύρεση αποδοτικού μοντέλου πρόβλεψης, ήταν ένα από τα πέντε ερευνητικά αντικείμενα της διατριβής, το οποίο δεν ήταν το κυριότερο. Η αστοχία ανάλυσης κακόβουλης κυκλοφορίας πραγματικού χρόνου, με την χρήση μοντέλου μηχανικής μάθησης, δεν μπορεί να αποδοθεί αποκλειστικά στο μοντέλο. Η εκπαίδευση του νευρωνικού δικτύου, παρήγαγε ένα μοντέλο με ικανοποιητικά χαρακτηριστικά. Όμως, στον πειραματικό σχεδιασμό, δεν ελήφθη υπόψη, ότι μεμονωμένες επιτυχείς προβλέψεις, δεν αποδεικνύουν αν το IoT αντικείμενο είναι ασφαλές ή όχι. Απλουστέρα, η κακόβουλη δικτυακή κίνηση, μπορεί να "κρυφτεί" σε ένα σύστημα, από το οποίο διέρχεται μεγάλη δικτυακή κίνηση, με συνέπεια τον μη εντοπισμό επίθεσης.

Πρέπει να τονισθεί ότι η δυσκολία της παρούσας ερευνητικής υπόθεσης, δεν έγκειται αποκλειστικά στην εξεύρεση του επιτυχέστερου μοντέλου πρόβλεψης. Σε ένα πραγματικό σύστημα, η παραγωγή δικτυακής κίνησης είναι τεράστια. Αυτό συνεπάγεται έναν δυσθεώρητο αριθμό πακέτων, από τον οποίο ένα μικρό ποσοστό είναι κακόβουλο, σε αναλογία με το συνολικό αριθμό.

6.1 Προτάσεις Και Μελλοντική Δουλειά

Κατά την πειραματική διαδικασία, παρατηρήθηκε υπερβολική χρήση πόρων συστήματος, με συνέπεια την μη σταθερή απόδοση του. Αυτό μπορεί να λυθεί, με την χρήση ισχυρότερου συστήματος, ή/και με την παροχή περισσότερων υπολογιστικών πόρων στο εικονικό περιβάλλον του πειράματος.

Το νευρωνικό δίκτυο χρησιμοποιεί το CICFLOWMETER [18] για την παραγωγή biflow, και την εξαγωγή των χαρακτηριστικών εκπαίδευσης του. Η επιλογή μικρότερου αριθμού χαρακτηριστικών από αυτού που χρησιμοποιήθηκε στο πείραμα, θα μπορούσε να μειώσει τον χρόνο εκπαίδευσης του ANN, αλλά και την ακρίβεια πρόβλεψης/κατηγοριοποίησης, της δικτυακής κυκλοφορίας του IoT δικτύου.

Άλλες βελτιώσεις:

- Συμπερίληψη MQTT [41] με αποτέλεσμα καλύτερη προσομοίωση ενός οικοσυστήματος IoT.

- Μετατροπή πραγματικού λογισμικού αισθητήρα θερμομέτρου σε Docker container.

- Μετατροπή του ANN σε Docker container.

- Μετατροπή των προγραμμάτων σύλληψης και ανάλυσης της δικτυακής κίνησης σε Docker container.

- Πραγματοποίηση επιθέσεων με διάφορα botnet.

- Δημιουργία συστήματος σύλληψης δικτυακής δραστηριότητας, εντός IoT δικτύου, πριν την εγκατάσταση και λειτουργία του συστήματος ανίχνευσης κακόβουλης κίνησης. Ο στόχος, είναι η συλλογή εκπαιδευτικού υλικού για το ANN, από το σύστημα που προορίζεται να προστατέψει. Πιθανότατα η τροφοδοσία του ANN με δεδομένα από το IoT δίκτυο καθαυτό, να παραγάγει ένα αποδοτικότερο μοντέλο, εν συγκρίσει με αυτό του παρόντος πειράματος.

[41] http://mqtt.org/

Βιβλιογραφία

[1] 35 Types of DDoS Attacks Explained. https://javapipe.com/blog/ddos- types/. Accessed: 2019-04-19.

[2] Q. E. Abbas and J. Sung-Bong. "A Survey of Blockchain and Its Applications". In: 2019 International Conference on Artificial Intelligence in Information and Communication (ICAIIC). Feb. 2019, pp. 001-003.

[3] Bing-Qiang Huang and Guang-Yi Cao and Min Guo. "Reinforcement Learning Neural Network to the Problem of Autonomous Mobile Robot Obstacle Avoidance". In: 2005 International Conference on Machine Learning and Cybernetics. Vol. 1. Aug. 2005, pp. 85-89.

[4} A. A. Arroyo. "Reading up books: Artificial intelligence and expert systems: Academic guidelines and suggested reading in the field of artificial intelligence and its industrial arm — Expert systems". In: IEEE Potentials 5.3 (Oct. 1986), pp. 16-18. ISSN: 0278-6648.

[5] H. Azwar et al. "Intrusion Detection in secure network for Cybersecurity systems using Machine Learning and Data Mining". In: 2018 IEEE 5th International Conference on Engineering Technologies and Applied Sciences (ICETAS). Nov. 2018, pp. 1-9.

[6] E. Biglar Beigi et al. "Towards effective feature selection in machine learning-based botnet detection approaches". In: 2014 IEEE Conference on Communications and Network Security. Oct. 2014, pp. 247-255.

[7] Bitcoin.org Mining. https://en.bitcoin.it/wiki/Mining. Accessed: 2018-02-10.

[8] https://en.bitcoin.it/wiki/Weaknesses#Attacker_has_a_lot_of_computing_power. Bitcoin.org Weaknesses. Accessed: 2018-02-10.

[9] Amine Boukhtouta et al. "Network Malware Classification Comparison Using DPI and Flow Packet Headers". In: Journal of Computer Virology and Hacking Techniques 11 (July 2015), pp. 1-32.

[10] K. Christidis and M. Devetsikiotis. "Blockchains and Smart Contracts for the Internet of Things". In: IEEE Access 4 (2016), pp. 2292-2303.

[11] O. E. David and N. S. Netanyahu. "DeepSign: Deep learning for automatic malware signature generation and classification". In: 2015 International Joint Conference on Neural Networks (IJCNN). July 2015, pp. 1-8.

[12] Sinclair Davidson, Primavera De Filippi, and Jason Potts. "Disrupting governance: The new institutional economics of distributed ledger technology". In: (2016).

[13] S. Dhakal, F. Jaafar, and P. Zavarsky. "Private Blockchain Network for IoT Device Firmware Integrity Verification and Update". In: 2019 IEEE 19th International Symposium on High Assurance Systems Engineering (HASE). Jan. 2019, pp. 164-170.

[14] H. U. Dike et al. "Unsupervised Learning Based On Artificial Neural Network: A Review". In: 2018 IEEE International Conference on Cyborg and Bionic Systems (CBS). Oct. 2018, pp. 322-327.

[15] B. Dorsemaine et al. "A new approach to investigate IoT threats based on a four layer model". In: 2016 13th International Conference on New Technologies for Distributed Systems (NOTERE). July 2016, pp.1-6.

[16] B. Dorsemaine et al. "Internet of Things: A Definition amp; Taxonomy". In: 2015 9th International Conference on Next Generation Mobile Applications, Services and Technologies. Sept. 2015, pp. 72-77.

[17] C. Douligeris and A. Mitrokotsa. "DDoS attacks and defense mechanisms: a classification". In: Proceedings of the 3rd IEEE International Symposium on Signal Processing and Information Technology (IEEE Cat. No.03EX795). Dec. 2003, pp. 190-193.

[18] Gerard Draper-Gil et al. "Characterization of encrypted and vpn traffic using time-related". In: Proceedings of the 2nd international conference on information systems security and privacy (ICISSP). 2016, pp. 407-414.

[19] K. A. Eldrandaly, M. Abdel-Basset, and L. A. Shawky. "Internet of Spatial Things: A New Reference Model With Insight Analysis". In: IEEE Access 7 (2019), pp. 19653-19669. ISSN: 2169-3536.

[20] b. F. Ertugrul, R. Tekin, and Y. Kaya. "Randomized feed-forward artificial neural networks in estimating short-term power load of a small house: A case study". In: 2017 International Artificial Intelligence and Data Processing Symposium (IDAP). Sept. 2017, pp. 1-5.

[21] Preeth E N and F. J. P. Mulerickal, B. Paul, and Y. Sastri. "Evaluation of Docker containers based on hardware utilization". In: 2015 International Conference on Control Communication Computing India (ICCC). Nov. 2015, pp. 697-700.

[22] D. Fakhri and K. Mutijarsa. "Secure IoT Communication using Blockchain Technology". In: 2018 International Symposium on Electronics and Smart Devices (ISESD). Oct. 2018, pp. 1-6.

[23] Antonio Gulli and Sujit Pal. Deep Learning with Keras. Packt Publishing Ltd, 2017.

[24] Ibrahim Abaker Targio Hashem et al. "The rise of "big data" on cloud computing: Review and open research issues". In: Information Systems 47 (2015), pp. 98-115.

[25] J. Haugeland. "Computer Architecture". In: Artificial Intelligence: The Very Idea. MITP, 1989. ISBN: 9780262291149. URL: https://ieeexplore.ieee.org/document/6302873.

[26] F. Hock and P. Kortis. "Commercial and open-source based Intrusion Detection System and Intrusion Prevention System (IDS/IPS) design for an IP networks". In: 2015 13th International Conference on Emerging eLearning Technologies and Applications (ICETA). Nov. 2015, pp. 1-4.

[27] K. Hughes and Y. Qu. "Performance Measures of Behavior-Based Signatures: An Anti-malware Solution for Platforms with Limited Computing Resource". In: 2014 Ninth International Conference on Availability, Reliability and Security. Sept. 2014, pp. 303-309.

[28] A. Kapoor. Hands-On Artificial Intelligence for IoT. Packt Publishing Ltd, 2019.

[29] O. Kilinc and I. Uysal. "Source-Aware Partitioning for Robust Cross-Validation". In: 2015 IEEE 14th International Conference on Machine Learning and Applications (ICMLA). Dec. 2015, pp. 1083-1088.

[30] K. Kim et al. "DDoS Mitigation: Decentralized CDN Using Private Blockchain". In: 2018 Tenth International Conference on Ubiquitous and Future Networks (ICUFN). July 2018, pp. 693-696.

[31] C. Kolias et al. "DDoS in the IoT: Mirai and Other Botnets". In: Computer 50.7 (2017), pp. 80-84. ISSN: 0018-9162.

[32] S. Kraijak and P. Tuwanut. "A survey on IoT architectures, protocols, applications, security, privacy, real-world implementation and future trends". In: 11th International Conference on Wireless Communications, Networking and Mobile Computing (WiCOM 2015). Sept. 2015, pp. 1-6.

[33] N. Kshetri. "Can Blockchain Strengthen the Internet of Things?" In: IT Professional 19.4 (2017), pp. 68-72. ISSN: 1520-9202.

[34] B Kusmierz. "The first glance at the simulation of the Tangle: discrete model". In: (2017).

[35] Arash Habibi Lashkari et al. "Characterization of Tor Traffic using Time based Features." In: ICISSP. 2017, pp. 253-262.

[36] Suk Kyu Lee, Mungyu Bae, and Hwangnam Kim. "Future of IoT networks: A survey". English. In: Applied Sciences (Switzerland) 7.10 (Oct. 2017). ISSN: 2076-3417.

[37] E. Luchian et al. "Automation of the infrastructure and services for an openstack deployment using chef tool". In: 2016 15th RoEduNet Conference: Networking in Education and Research. Sept. 2016, pp. 1-5.

[38] H. Lv and H. Tang. "Machine Learning Methods and Their Application Research". In: 2011 2nd International Symposium on Intelligence Information Processing and Trusted Computing. Oct. 2011, pp. 108-110.

[39] J. McCarthy et al. "A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence, August 31, 1955". In: AI Magazine 27.4 (Dec. 2006), pp. 12-14. ISSN: 0738-4602.

[40] David C Mills et al. "Distributed ledger technology in payments, clearing, and settlement". In: (2016).

[41] Satoshi Nakamoto. "Bitcoin: a peer-to-peer electronic cash system, Oct. 2008". In: URL http://www.bitcoin.org/bitcoin.pdf (cited on pp. 15 and 87) (2017).

[42] K. Y. Nikolskaya et al. "Review of modern DDoS-attacks, methods and means of counteraction". In: 2017 International Conference "Quality Management,Transport and Information Security, Information Technologies" (IT QM IS). Sept. 2017, pp. 87-89.

[43] A. Ozadowicz et al. "Application of the Internet of Things (IoT) Technology in Consumer Electronics - Case Study". In: 2018 IEEE 23rd International Conference on Emerging Technologies and Factory Automation (ETFA). Vol. 1. Sept. 2018, pp. 1037-1042.

[44] S. M. Patil, M. Vijayalashmi, and R. Tapaskar. "IoT based solar energy monitoring system". In: 2017 International Conference on Energy, Communication, Data Analytics and Soft Computing (ICECDS). Aug. 2017, pp. 1574-1579.

[45] P. Prasad et al. "3 dimensional security in cloud computing". In: 2011 3rd International Conference on Computer Research and Development. Vol. 3. Mar. 2011, pp. 198-201.

[46] A. O. Prokofiev, Y. S. Smirnova, and V. A. Surov. "A method to detect Internet of Things botnets". In: 2018 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus). Jan. 2018, pp. 105-108.

[47] K. Rahim, H. Tahir, and N. Ikram. "Sensor Based PUF IoT Authentication Model for a Smart Home with Private Blockchain". In: 2018 International Conference on Applied and Engineering Mathematics (ICAEM). Sept. 2018, pp. 102-108.

[48] Yuji Roh, Geon Heo, and Steven Euijong Whang. "A Survey on Data Collection for Machine Learning: a Big Data-AI Integration Perspective". In: arXiv preprint arXiv:1811.03402 (2018).

[49] R. Roman-Castro, J. López, and S. Gritzalis. "Evolution and Trends in IoT Security". In: Computer 51.7 (July 2018), pp. 16-25. ISSN:0018-9162.

[50] M. Samaniego and R. Deters. "Internet of Smart Things - IoST: Using Blockchain and CLIPS to Make Things Autonomous". In: 2017 IEEE International Conference on Cognitive Computing (ICCC). June 2017, pp. 9-16.

[51] R. Saravanan and P. Sujatha. "A State of Art Techniques on Machine Learning Algorithms: A Perspective of Supervised Learning Approaches in Data Classification". In: 2018 Second International Conference on Intelligent Computing and Control Systems (ICICCS). June 2018, pp. 945-949.

[52] Rudy Setiono and Huan Liu. "Feature extraction via Neural networks". In: Feature Extraction, Construction and Selection: A Data Mining Perspective. Ed. by Huan Liu and Hiroshi Motoda. Boston, MA: Springer US, 1998, pp. 191-204. ISBN: 978-1-4615-5725-8. URL: https://doi.org/10.1007/978-1-4615-5725-8_12.

[53] https://web.archive.org/web/20150426090206/http://ha.ckers.org/slowloris. Slowloris HTTP DoS. Accessed: 2019-04-19.

[54] http://repfiles.kallipos.gr/html_books/93/00e-introduction.html. Slowloris HTTP DoS. Accessed: 2019-04-19.

[55] Nitish Srivastava et al. "Dropout: A Simple Way to Prevent Neural Networks from Overfitting". In: Journal of Machine Learning Research 15 (2014), pp.1929-1958. URL: http://jmlr.org/papers/v15/srivastava14a.html.

[56] P. Suresh et al. "A state of the art review on the Internet of Things (IoT) history, technology and fields of deployment". In: 2014 International Conference on Science Engineering and Management Research (ICSEMR). Nov. 2014, pp. 1-8.

[57] S. N. Swamy, D. Jadhav, and N. Kulkarni. "Security threats in the application layer in IOT applications". In: 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC). Feb. 2017, pp. 477-480.

[58] That 'Internet of Things' Thing. https://www.rfidjournal.com/articles/view?4986. Accessed: 2019-04-13.

[59] The Internet of Things - How the Next Evolution of the Internet Is Changing Everything. https://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf. Accessed: 2019-04-22.

[60] E. Wall. IOTA is centralized. https://medium.com/@ercwl/iota-is-centralized-6289246e7b4d. Accessed: 2018-02-10. Jan. 2017.

[61] T. Xue et al. "Proof of Contribution: A Modification of Proof of Work to Increase Mining Efficiency". In: 2018 IEEE 42nd Annual Computer Software and Applications Conference (COMPSAC). Vol. 01. July 2018, pp. 636-644.

[62] F. Yihunie, E. Abdelfattah, and A. Odeh. "Analysis of ping of death DoS and DDoS attacks". In: 2018 IEEE Long Island Systems, Applications and Technology Conference (LISAT). May 2018, pp. 1-4.