الجمهورية العربية السورية
المعهد العالي للعلوم التطبيقية والتكنولوجيا
قسم الاتصالات

أطروحة

أعدت لنيل درجة الماجستير في هندسة الاتصالات

تحسين الخصوصية في شبكات انترنت الأشياء باستخدام سلسلة الكتل

Improving the Privacy in IoT Networks using BlockChain

إعداد

م. ضياء محمد

إشراف

د. محمد الجنيدي

دمشق – تشرين الأول 2019

المعهد العالي للعلوم التطبيقية والتكنولوجيا

Higher Institute for Applied Sciences and Technology
Institut Supérieur des Sciences Appliquées et de Technologie

مؤسسة سورية حكومية للتعليم العالي أحدثت في عام 1983 بموجب مرسوم تشريعي، بهدف إعداد أطر متميزة مؤهلة للبحث العلمي والتطوير في مجال العلوم التطبيقية والتقانة، لتساهم بفاعلية في التنمية العلمية والصناعية والاقتصادية في القطر.

يشكّل التأهيل الهندسي والدراسات العليا في المعهد العالي محور عمليّة إعداد الأطر المتخصّصة. يخرّج المعهد العالي مهندسين متميزين، بعد دراسة لمدة خمس سنوات، في اختصاصات الاتصالات والمعلوماتية والنظم الإلكترونية والميكاترونيكس وهندسة الطيران وعلوم وهندسة المواد. تقسم الدراسة في المرحلة الهندسية إلى جذع مشترك وسنوات اختصاص. تمتد مواد الجذع المشترك على السنتين الأولى والثانية وجزء من الثالثة بحيث تعطي الطالب قاعدة متينة في الرياضيات والفيزياء والكيمياء واللغات الأجنبية، وذلك على نمط الصفوف التحضيرية في نظام المدارس العليا الفرنسية الرائدة في إعداد طلاب متميزين. يتوزع الطلاب اعتباراً من السنة الثالثة على اختصاصات الهندسة المختلفة بحيث تبدأ المواد بالتمايز والتعمق في صلب الاختصاص تدريجياً وصولاً إلى سنة التخرج.

كما يمنح المعهد العالي درجة الماجستير الأكاديمي، ماجستير بحثي يمتد على سنتين، من خلال مجموعة من برامج الماجستير في نظم الاتصالات وفي التحكم والروبوتيك وفي علوم المواد وفي نظم المعلومات واتخاذ القرار وفي نظم معالجة المعطيات الكبيرة. تخصص السنة الأولى في الماجستير لدراسة عدد من المواد تتوزع بين مواد إجبارية وأخرى اختيارية بحسب الاختصاص الفرعي المطلوب. يعمل الطالب أثناء السنة الثانية على مشروع بحثي يقدم في نهايته أطروحة يدافع عنها ويشجع على نشر نتائج بحثه في مقالات علمية. وأخيراً يمنح المعهد العالي درجة الدكتوراه في عدة اختصاصات موازية لما ذكر في برامج الماجستير.

يعتمد المعهد العالي في تميز خريجيه من كافة المراحل على مجموعة من العوامل أهمها تركيزه على النوع وليس الكم. فالمعهد العالي ينتقي في المرحلة الهندسية شريحة الطلاب المتفوقين في شهادة الدراسة الثانوية السورية من الفرع العلمي أو من في حكمهم، إذ يقبل من ينتمون سنوياً إلى الـ 15% الأوائل على مستوى القطر، وذلك إثر مفاضلة خاصة لاختيار أفضل المتقدمين يجريها داخلياً على التوازي مع المفاضلة العامة للتعليم العالي. يدرس الطلاب في المعهد العالي كطلاب موفدين لصالح جهات عامة أو خاصة تغطي تكاليف دراستهم مقابل التزام بعد التخرج تحدد طبيعته هذه الجهات، أو كطلاب دراسة خاصة يدفعون تكاليف دراستهم بدون أية التزامات بعد التخرج.

أما في مرحلة الماجستير فيقبل المعهد العالي حملة الشهادات الجامعية المواتية للماجستير المطلوب، وذلك على أساس مفاضلة خاصة تأخذ بعين الاعتبار معدل وجهة التخرج في الهندسة ونتيجة اختبارين علمي ولغوي –في اللغة الإنكليزية– يخضع لهما المتقدمون. وأخيراً يجري القبول في برنامج الدكتوراه بناءً على السيرة الذاتية للمتقدم ونتائجه الدراسية السابقة وخبراته السابقة إن وجدت.

يقدم المعهد لطلاب الهندسات والدراسات العليا جواً متميزاً للدراسة والبحث بدءاً من كوادره المتفرغة عالية التأهيل ومناهجه المواكبة للتطورات العلمية، وانتهاءً بإمكانيات مختبراته المتميزة في القطر وبنيته التحتية المواتية من صالات حواسب وورش ومراكز تكنولوجية ومقدرات مادية وشبكات تعاون مع الصناعة والهيئات الأكاديمية داخل وخارج القطر. كل ذلك في ظل بيئة طبيعية مضيافة ووسائل للراحة والترفيه من سكن طلابي مجهز ومطعم وصالات رياضية وملاعب متنوعة ونشاطات ونوادٍ ثقافية واجتماعية وعلمية، تكمل بمجملها شخصية الخريج وتدعم تميزه.

تحظى شهادات المعهد العالي بتقدير كبير على المستوى المحلي والعالمي، إذ نجح عدد كبير من خريجي المعهد الموفدين إلى أكبر الجامعات في أوروبا وروسيا الاتحادية ودول شرق آسيا في الحصول على شهادات علمية بامتياز نظراً إلى سوية الإعداد الذي تلقوه في المعهد العالي، وساهم بعضهم، ممن درسوا لصالح المعهد العالي نفسه أو تعينوا فيه بعد التخرج، في رفد كوادر المعهد بخبراتهم عبر التدريس والبحث العلمي. كما يحظى خريجو المعهد العالي بفرص كبيرة للتوظيف في شركات القطاعين العام والخاص داخل وخارج القطر ويثبتون على الدوام تميزهم أينما حلوا. وتبوأ عدد كبير من قدامى خريجي المعهد العالي مناصب علمية وإدارية مرموقة في الشركات والوزارات والجامعات العامة والخاصة وحتى في بعض مراكز البحث والجامعات والمنظمات خارج القطر.

بالإضافة إلى نشاطه الأكاديمي، يضم المعهد العالي أقساماً علمية ومخابر متنوعة ومراكز تكنولوجية، كمخبر الدراسات البيئية ومركز تقانات اللحام ومركز الحوسبة عالية الأداء. تقدم هذه الأقسام والمراكز التكنولوجية والمخابر خدمات واستشارات للقطاعين العام والخاص، بالإضافة إلى المشاريع التطويرية والنشاطات البحثية والدورات التدريبية وتنظيم ورش العمل والمؤتمرات العلمية.

يعمل المعهد العالي باستمرار على تطوير مقدراته البشرية والمادية عبر الإيفادات القصيرة والطويلة وبرامج التعاون مع الجهات المختلفة المحلية والعالمية. كما يعمل ذاتياً على رفع سوية كوادره عبر الدورات التدريبية والمؤتمرات وورش العمل المختلفة التي ينظمها والتي يفيد من بعضها كوادر القطر من خارج المعهد العالي أيضاً. يسعى المعهد العالي باستمرار إلى فتح قنوات للتعاون العلمي والتقاني مع جهات القطاعين العام والخاص والجامعات والمنظمات الدولية، إذ يساهم في تنفيذ مشاريع بحثية وتطويرية مشتركة على المستوى المحلي والإقليمي والدولي بهدف نقل التقانة وتبادل الخبرات

أهدي هذا العمل

إلى وطني الحبيب الجريح الذي أتمنى شفاءه

إلى من أعانني وعلمني التغلب على مصاعب الحياة ..... أبي

إلى من ربتني وعلمتني ..... أمي الحنونة

إلى من عاشوا معي وتحملوني وساندوني ..... أخواتي

إلى من أصبحت الحياة ذات قيمة بوجودهم ..... أولاد أختي

إلى من سهّل عليّ كافة العقبات وكان خير داعم .... د. دريد درغام

إلى جميع أصدقائي وزملائي وإلى جميع طلاب المعهد العالي وإلى من يحتاج إلى هذا العمل.

If I have seen further it is by standing on the shoulders of Giants.

Isaac Newton

كلمة شكر

أتقدم بجزيل الشكر وعظيم الامتنان إلى الدكتور محمد الجنيدي الذي أفتخر بإشرافه وأخجل من تموضع اسمي بجوار اسمه على واجهة هذا العمل، على إشرافه واهتمامه البالغ ومعلوماته الثمينة، وإرشاداته التي تعادل أشهراً من البحث. كما أتقدّم بالشكر الكبير لكل الأصدقاء والصديقات الذين وقفوا معي وساندوني بأي شكلٍ من الأشكال لحين إتمام هذا العمل.

ضياء محمد

الملخص

وسّعَت أنظمة أنترنت الأشياء (IoT) مجالَ الشبكات إلى عشرات المليارات من الأجهزة المتّصلة، وأصبح من الصعب حماية أمنها وخصوصية بيانات مستخدميها بسبب عدم تجانس الأطراف المتّصلة وتمتّعها بخصائص مميّزة تجعل من الصعب تطبيق الحلول الأمنية التقليدية. لذا، نهدُف في هذه الأطروحة إلى إيجاد منصّة أمنية لحماية خصوصية أجهزة انترنت الأشياء في بيئة المنزل الذكي الذي يعتبَر من أهم تطبيقات IoT، وذلك اعتماداً على تقنية سلسلة الكتل (blockchain) التي حصدَت اهتماماً كبيراً من قبل الباحثين منذ نشأتها في العملة الرقمية بتكوين، نظراً لطبيعتها الثابتة وميزات الأمن والخصوصية التي تقدّمها، مما يكسبها القدرة للتغلّب على التحديات الأمنية لأنظمة انترنت الأشياء. لكن تعتبَر تقنية سلسلة الكتل مكلفة من حيث العمليات الحسابية، قابلية التوسّع، والتأخير الزمني، وهذا يشكّل تحدّياً في تطبيقها في أنظمة انترنت الأشياء التي يجب أن تكون ديناميكية في انضمام أو مغادرة الأجهزة المتّصلة وتقدِّم غالب خدماتها في الزمن الحقيقي.

يتكوّن النموذج المطروح من عدّة طبقات مصمّمة لتناسب إمكانيات أجهزة انترنت الأشياء، ويجري تطبيقه في المنزل الذكي الذي يحوي تجهيزات وحساسات محدودة الموارد بالمجمل.

يحقّق النموذج المطروح اللّامركزية من خلال استخدام الشبكة الغطاء (overlay) والتي تتكون من أجهزة عالية الموارد تتشارك معاً في إدارة سلسلة كتل عامة (Public BC) تضمن تحقيق الأمن والخصوصية لكافة أطراف الاتصال، يجري تقسيم شبكة الغطاء إلى عناقيد ولكل عنقود مدير هو الذي يمثل عنقوده في المشاركة بإدارة سلسلة الكتل مع المدراء الآخرين. يتضمّن النموذج العديد من التحسينات مثل خوارزمية التوافق الخفيفة وآلية الثقة الموزعة وخوارزميات التعمية المتناظرة وغير المتناظرة من أجل تحقيق السرية والخصوصية للأجهزة الموجودة. وذلك لمحاولة الوصول إلى حل أمثلي غير مكلف حسابياً، وقابل للتوسع الديناميكي، وبتأخير زمني أقل مايمكن.

هذه التحسينات التي سنقوم بها ستساهم في إعطاء العديد من الميزات وأهمها سهولة بناء الشبكة، وكذلك سهولة التحقق من العقد الخبيثة التي تحاول الدخول أو التنصت على الشبكة، وبالتالي المناعة العالية ضد أغلب الهجمات الأمنية المحتملة. أي أن النموذج المقترح قد ساهم في تأمين الخدمات الأمنية الأساسية: المصادقة، سلامة المعطيات، سريتها، عدم الإنكار، بالإضافة إلى تحسين الخصوصية.

سنقوم بتنجيز النموذج باستخدام أداة المحاكاة Cooja، والتي تعمل ضمن نظام التشغيل Contiki، واختباره أمنياً، من خلال منع محاولات دخول أي عقدة خبيثة إلى الشبكة.

Abstract

Internet of Things (IoT) systems have expanded any network to billions of connected devices. However, privacy and security for those networks have become main issues because of the heterogeneity of the parties involved, and the features that make it difficult to implement traditional security solutions. Therefore, the main aim of this study is to create a security platform to protect the privacy of IoT devices in the smart home environment, which is considered one of the most important applications of IoT, based on blockchain technology, which has gained more researchers' interest since the invention of digital currency. Blockchain technology have the ability to overcome the security challenges of IoT systems.

Blockchain technology is heavily costed, less scalability, and much time delay. Those challenges make it very difficult to dynamically join or leave connected devices in real time environment.

Our proposed solution tries to achieve decentralization through using of overlay, which is a network consists of high-resource devices that joint to manage a public blockchain to ensure the security and privacy of all network parties. Overlay is divided into clusters and each cluster has cluster head to participate in the management of the chain blocks with others.

Our solution includes many enhanced algorithms, such as light consensus algorithm, distributed trust mechanism, symmetric and asymmetric encryption algorithms, to achieve the confidentiality and privacy of existing devices. Also, find better solution that is inexpensively, dynamically scalable and less time delay.

These improvements will contribute to give many features in the network, as building network easily, as well as do the verification of malicious nodes that try to eavesdrop. Therefor, giving the network high immunity against most potential security attacks. This means that the proposed model has contributed in provision of basic security services, as well as improving privacy.

We will implement the proposed solution using Cooja emulation tool, which runs within Contici OS, and test its security by blocking any malicious node that attempts to enter the network.

المحتويات

قائمة الأشكال

قائمة الجداول

الاختصارات

IoT	Internet of Things
BC	BlockChain
SC	Smart Contract
WSN	Wireless sensor network
EEP	Embedded Edge Processor
EDI	Electronic Data Interfaces
GPS	Global Positioning System
EPC	Electronic Product Code
ONS	Object Naming Service
TLS	Transport Layer Security.
DTLS	Datagram Transport Layer Security.
HiFi	High fidelity.
RSA	Rivest–Shamir–Adleman.
AES	Advanced Encryption Standard.
SHA	Secure Hash Algorithm.
CIA	Confidentiality, Integrity, Availability.
PKI	Public Key Infrastructure.
RFID	Radio-frequency identification.
MLS	Multi-Level Security.
IDM	Identity Management
DoS	Denial-of-Service
DDoS	Disributed Denial-of-Service
SOA	Service Oriented Architecture
IETF	Internet Engineering Task Force
FCC	Federal Communications Commission
6LoWPAN	IPv6 over Low-power Wireless Personal Area Networks.
6LBR	6LoWPAN Border Router.
CoAP	Constrained Application Protocol.
TPM	Trusted Platform Module.
IBE	Identity-Based Encryption
RPL	Routing Protocol for LLNs.
ARP	Address Resolution Protocol
OWASP	The Open Web Application Security Project
LLNs	Low Power and Lossy Networks.
DAG	Directed Acyclic Graph.
DODAG	Destination-Oriented DAG.
AH	Authentication Header.
ESP	Encapsulating Security Payload.
IACAC	Identity Authentication and Capability based Access Control.
DIO	Destination Information Object.

IKE	Internet Key Exchange
NHC	next header compression
UDP	User Datagram Protocol
SA	security association
DSR	Dynamic Source Routing.
AAA	authentication, authorization and accounting
PoW	Proof of Work
PoS	Proof of Stake
PBFT	Practical Byzantine Fault Tolerance
DPoS	Delegated Proof of Stake
PoB	Proof of Bandwidth
PoET	Proof of Elapsed Time
PoA	Proof of Authority
DAO	Decentralized Autonomous Organizations.
ECC	Elliptic Curve Cryptography.
ECDSA	Elliptic Curve Digital Signature Algorithm.
CTB-Locker	Curve-Tor-Bitcoin-locker.
SGX	Software Guard eXtension.
EVM	Ethereum Virtual Machine.
BGP	Border Gateway Protocol.
MDP	Markov Decision Processes.
CFG	Control Flow Graph.
API	Application programming interface.
LAN	Local Area Network.
PAN	Personal Area Network.
WAN	Wide Area Network.
WLAN	Wireless Local Area Network.
WPAN	Wireless Personal Area Network.
WWAN	Wireless Wide Area Network.
LR-WPAN	Low-Rate Wireless Personal Area Network.
P2P	Point-to-Point.
P2MP	Point-to-MultiPoint.
ISM	The Industrial, Scientific, and Medical radio.
RF	Radio Frequency.
VLC	Visible Light Communication.
LoS	Line of Sight.
DSSS	Direct Sequence Spread Spectrum.
FHSS	Frequency Hopping Spread Spectrum.
IR	Infrared.
MIMO	Multiple Input Multiple Output.
WEP	Wired Equivalent Privacy.
WPA	Wi-Fi Protected Access.
LTE	Long Term Evolution.
LTE-A	Long Term Evolution-Advanced.
M2M	Machine-to-Machine.
IaaS	Infrastructure as a Service.

PaaS	Platform as a Service.
SaaS	Software as a Service.
3GPP	Third Generation Partnership Project.
LSB	Lightweight Scalable Blockchain
BaDS	Blockchain-based architecture for data sharing
ABE	Attribute-based Encryption
CP-ABE	Ciphertext ABE
ABS	Attribute-based Signature
ARX	Addition, Rotation, XOR

المصطلحات

Confidentiality	السرية
Integrity	السلامة
Availability	التوافرية
Authentication	المصادقة
Authorization	تخويل
Nonrepudiation	عدم الإنكار
Notarization	التوثيق
Untraceability	عدم التتبع
Unlinkability	إخفاء الترابط
Authenticity	التحقق من الأصالة
Anonymity	إخفاء الهوية
Pseudonymity	أسماء مستعارة
Access Control	التحكم في الوصول
Frame	إطار
Packet	رزمة
Hardware	عتاد صلب
software	برمجيات
firmware	برمجيات راسخة
Supply chain	سلسلة إمداد
Meta data	بيانات مترفعة
Chaff coins	عملات وهمية
dependability	الاعتمادية
jamming	تشويش
flooding	فيضان

Throughput	الإنتاجية
utilization	المردود
overhead	حمل أو عبء زائد
mining	تنقيب
fragmentation	تجزئة
clustering	عنقدة
Timestamp	بصمة زمنية
buffer	صِوان
platform	منصة
broadcast	بثّ
multicast	بثّ متعدد
Handshake	مصافحة
Token	وحدة رقمية
consensus	توافق
Transaction	مناقلة
Verification	التحقق من الصحة
Validation	التحقق من الصلاحية
Mining pool	حوض تنقيب
efficiency	فعالية
Bytecode	رماز ثماني
compile	تصريف
Requester	مولِّد المناقلة
Requestee	مستقبِل المناقلة
cryptosystem	أنظمة معمّاة
Risk	خطر
Issue	قضية
Fog Computing	الحوسبة الضبابية
Cloud Computing	الحوسبة السحابية

المنحنيات القطعية	Elliptic-curve
تعمية	Encryption
علم التعمية (تعمية + تحليل التعمية)	Cryptography
الشبكة الغطاء	Overlay network
قارئ RFID	RFID reader
رقاقة RFID	RFID tag
تقابل	Mapping
مخطط	Scheme
نموذج أوّلي	Prototype
وكيل	Proxy

مصطلحات خاصة بالنموذج المقترَح في الفصل الرابع

المفتاح العام للمرسِل، والمخصّص للتوقيع الرقمي	$sk_{s_{pub}}$
المفتاح الخاص للمرسل، والمخصص للتوقيع الرقمي	$sk_{s_{priv}}$
المفتاح الخاص للمستقبِل، والمخصص للتوقيع الرقمي	$rk_{s_{pub}}$
المفتاح الخاص للمستقبِل، والمخصص للتوقيع الرقمي	$rk_{s_{priv}}$
المفتاح المشترك	k_{sym}
قيمة تعمية المفتاح المشترك	C_{k}
قيمة تهشير البيانات المرسَلة	$hash_{\mathrm{p}}$
زوج المفاتيح للمرسِل، والمخصصة للتعمية وفكّ التعمية	$(sk_{\mathrm{pub}}\ ,\ sk_{\mathrm{priv}})$
زوج المفاتيح للمستقبِل، والمخصصة للتعمية وفكّ التعمية	$(rk_{\mathrm{pub}}\ ,\ rk_{\mathrm{priv}})$
مولّد المناقلة	Requester
مستقبِل المناقلة	Requestee

مقدمة عامة

تزايد استخدام الانترنت بشكل كبير في مختلف مجالات الحياة، ابتداءً بالحواسب الشخصية مروراً بالهواتف الذكية التي أصبحت أحد أهم متطلبات مستخدمي الانترنت، وانتهاءً باستخدام التجهيزات الذكية مثل الشاشات الذكية التي تسمح للمستخدمين بمشاهدة التلفاز، تصفح الانترنت وإجراء المكالمات الفيديوية، إضافةً إلى أمثلة أخرى كالثلاجات الذكية، منظمات الحرارة الذكية (thermostats) والمصابيح الذكية. ترافَق ذلك الازدياد مع تزايد فرص المجرمين الالكترونيين في الاستفادة من كافة الثغرات الموجودة في تلك الأجهزة للقيام بهجمات أمنية قد تؤثر على بيانات المستخدمين بشكل مباشر وتهدّد خصوصيتهم مما دفع الشركات المصنعة لتلك الأجهزة الذكية والباحثين إلى التفكير بحلول أمنية تحمي تلك الأجهزة من الفشل الوظيفي أو الأمني.

تتمتّع أنظمة انترنت الأشياء بخواص مميّزة فهي عبارة عن أعداد كبيرة من الأجهزة المتصلة التي قد تخرج من شبكة وتنضم إلى شبكة أخرى حسب التطبيق، وأغلب تلك الأجهزة محدودة الموارد الحسابية، وهي أنظمة لامركزية. تجعل الخواصُ السابقة مسألة تأمين تلك الأجهزة تحدياً كبيراً حيث نعلم أن معظم الحلول الأمنية هي ذات طبيعة مركزية وليست قابلة للتوسع بشكل ديناميكي وتحتاج إلى موارد حاسوبية عالية.

أما تقنية سلسلة الكتل، فهي عبارة عن سجلات ثابتة لها بصمة زمنية تستخدَم لتخزين ومشاركة البيانات بشكل موزَّع، تتنوّع البيانات المخزَّنة فيها بين مناقلات مالية، معلومات عقد ذكي، أو بيانات شخصية حسب التطبيق. تتمتّع سلسلة الكتل بطبيعة لا مركزية، آمنة، ويَصعُب تعديل البيانات المخزّنة فيها، مما جعلها تجلب اهتماماً كبيراً لاستخدامها في حماية أمن وخصوصية انترنت الأشياء.

نقدِّم في الفصل الأول دراسة نظرية ومرجعية شاملة عن انترنت الأشياء، حيث سنناقش مفهوم هذه الأنظمة وبنيتها وتطبيقاتها، ثم سنتحدّث عن متطلبات الأمن والخصوصية بشكل عام لأي نظام اتصالات، ثم سنقدّم دراسة مرجعية عن المتطلبات الأمنية الخاصة بإنترنت الأشياء وآخر الدراسات التي عملت في هذا المجال، لننتقل بعدها إلى مناقشة وتصنيف أهم القضايا الأمنية في تلك الأنظمة من وجهة نظر طبقات الشبكة، إضافةً إلى أحدث الحلول الأمنية المطروحة في الأدبيات لتلك القضايا.

بينما نعرض في الفصل الثاني بشكل مشابه دراسة نظرية ومرجعية معاً لتقنية سلسلة الكتل، حيث سنناقش بعض المفاهيم النظرية المتعلقة بها، ثم ننتقل إلى الجزء الأمني الذي يحوي أخطار وهجمات أمنية تتعرض لها سلسلة الكتل، لننهي الفصل بالحلول الأمنية المطروحة في الأدبيات.

انفرَد الفصل الثالث بأهمّ وأحدث الدراسات المرجعية التي تجمع بين تقنية سلسلة الكتل وأنظمة انترنت الأشياء معاً، لنبيّن فيه إمكانية استخدام سلسلة الكتل في تحسين أمن وخصوصية انترنت الأشياء مع التطرّق إلى أهم التحديات في دمج التقنيّتين.

سننتقل في الفصل الرابع إلى توصيف النموذج المقترح، وسنعرض في الفصل الخامس المحاكاة والنتائج العملية باستخدام الأداة Cooja في نظام التشغيل Contiki، بينما سنلخّص في الفصل السادس الخاتمة والآفاق المستقبلية.

الفصل الأول

انترنت الأشياء

Internet of Things (IoT)

نقدم في هذا الفصل نظرة عامة على انترنت الأشياء، بنيتها، تطبيقاتها، الثغرات الأمنية الموجودة فيها وبعض الحلو المقترَحة لتلك الثغرات، إضافة إلى نظرة عامة عن بعض المتطلبات الأمنية لأي نظام اتصالات.

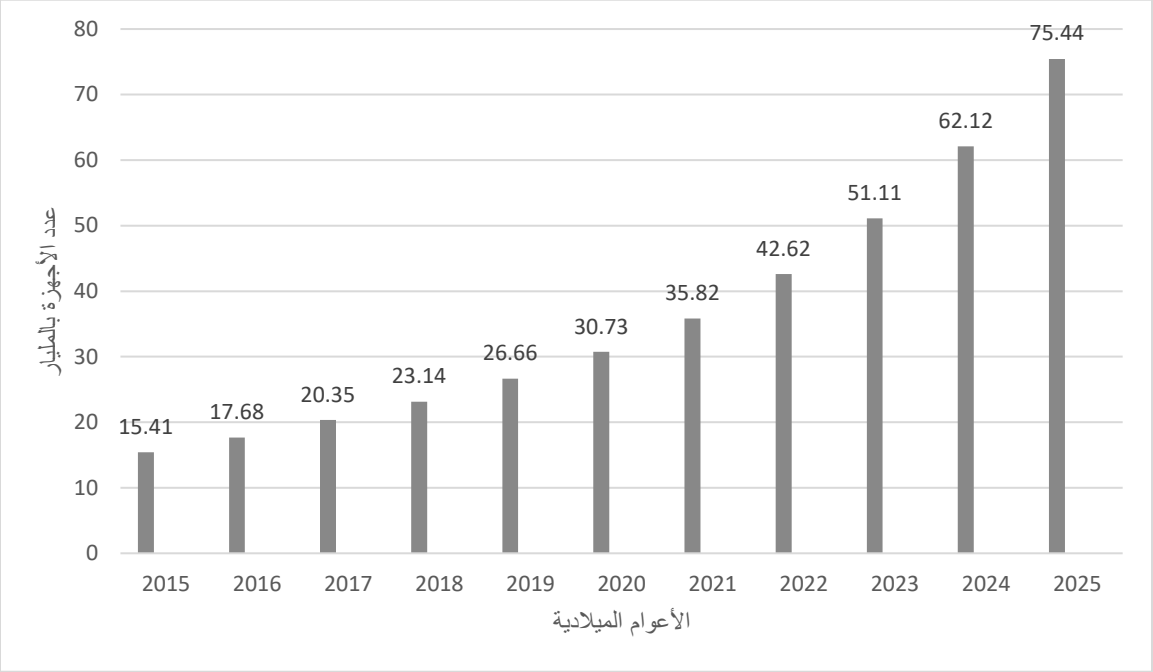
1.1- مقدمة

اكتسبَت أنظمةُ انترنت الأشياء (IoT) قبولاً واسعاً كمعيارٍ رئيسي للشبكات ذات الطاقة المحدودة والضياع في الرّزم (LLNs)، وذلك بفضل النمو السريع للأجهزة الذكية والشبكات عالية السرعة. حيث تمثِّل تلك الأنظمة شبكةً تكون فيها "الأشياء" أو الأجهزة التي تحوي حساسات مرتبطةً معاً عبر شبكة عامة أو خاصة، يجري من خلالها مشاركة البيانات التي تجمعها تلك "الأشياء" أو الحساسات. تتراوح "الأشياء" بين أدوات صغيرة قابلة للارتداء وبين آلات كبيرة. ترافَق نموّ أنظمة IoT كما في أي نظام معلومات أو اتصالات مع قضايا وتحدّيات على كافة الصّعد كالتحديات العتادية والتحديات الأمنية. لذا، سنتحدّث في هذا الفصل أولاً عن تعريف انترنت الأشياء، بنيتها، عناصرها وتطبيقاتها، ثم سنبيّن حالة المنزل الذكي كأحد تطبيقاتها، لنتطرّق بعدها إلى بعض التحديات والقضايا المفتوحة لتلك الأنظمة، كما سنقوم بإلقاء نظرة أدبية على المتطلبات الأساسية لأمن وخصوصية أي نظام معلوماتي قائم على الشبكات.

2.1- انترنت الأشياء

يمكننا إطلاق تسمية انترنت الأشياء على تلك الظاهرة الصاعدة التي تصبح فيها جميع أنواع "الأشياء"، مثل أجهزة الجيل الحالي الذكية، جزءاً من الانترنت. يجري في هذه الرؤية بناء بنية تحتية عالمية للمعلومات، تعتمد على الانترنت، حيث سيكون للعديد من الأشياء المادية الحقيقية نظيراً افتراضياً تتواصل وتتفاعل فيما بينها لخدمة العنصر البشري.

تتحقق تلك البنية التحتية من خلال تحسين وتكامل عدد من التقنيات كالتّعرّف على الهوية، التّتبّع، الاتصالات والذكاء الموزَّع. ستتضمن انترنت الأشياء إذاً عدداً كبيراً من الأجهزة ذات الإمكانات المختلفة، وسيكون بالتالي لبعض الأشياء المشاركة إمكانات محدودة للغاية، حيث بلغ عدد الأجهزة المتصلة 15.41 مليار في عام 2015، و23.14 مليار في 2018، وهذا العدد قابل للازدياد بتقديرات مختلفة في السنوات المقبلة [1] إلى أن يتجاوز 75 مليار جهاز متّصل بحلول عام 2025 كما يظهِر الشكل 1-1.



الشكل 1-1 إحصائيات عدد الأجهزة المتّصلة منذ عام **2015** وحتى **2025** [1].

لابد أن يكون للتفاعل بين البشر وهذه الكثرة من الأجهزة تأثيراً كبيراً على الحياة اليومية والمهنية، من خلال إتاحة الفرص للخدمات الجديدة والمحسّنة، حيث يجري تصوّر وتطوير العديد من تطبيقات انترنت الأشياء إلى أن يجري استخدامها بالفعل: كالمنازل الذكية، المدن الذكية، المكاتب الذكية، التسوق الذكي، العناية الصحية الذكية، بيئات الإنتاج الذكية، الخدمات اللوجستية المحسَّنة والنقل ....

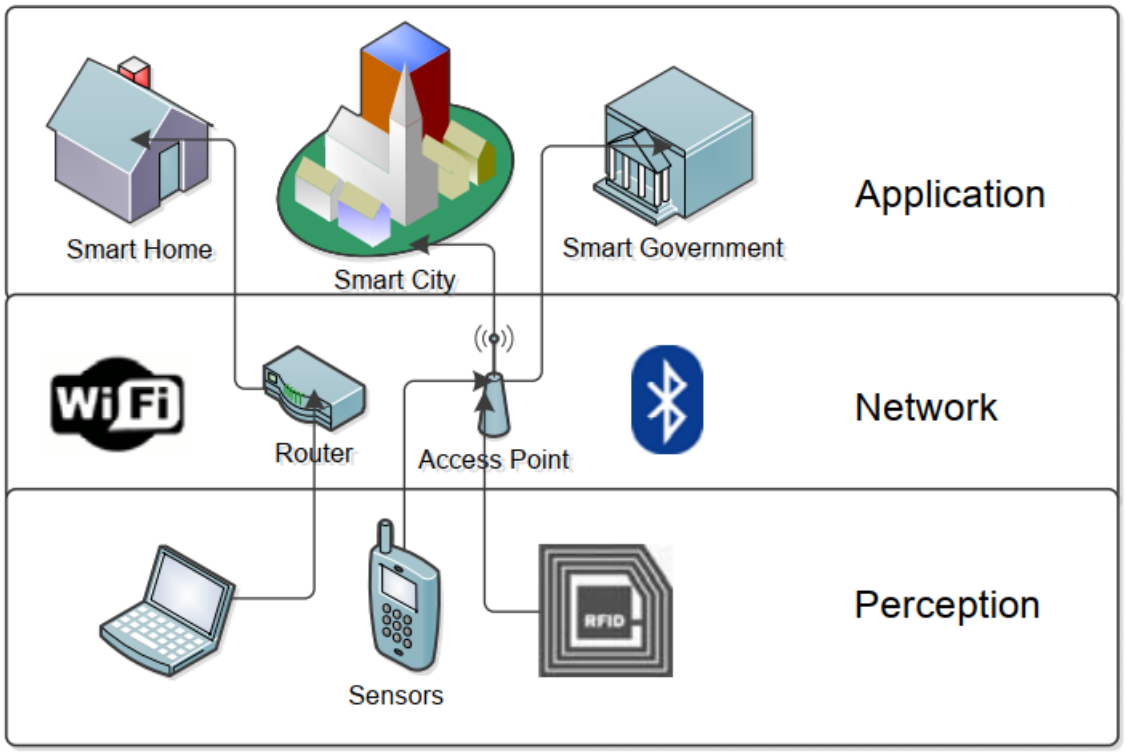
3.1- نظرة عامة على انترنت الأشياء

1.3.1- بنية انترنت الأشياء

تتألف هيكلية انترنت الأشياء من عدة طبقات، يجري تعريف كل طبقةٍ منها من خلال وظائفها والأجهزة المستخدمة فيها، ويختلف عدد تلك الطبقات في الأدبيات والمراجع بين ثلاث وأربع طبقات وفق المقاربات التالية [2]:

1.1.3.1- بنية IoT ذات ثلاث طبقات

تتفق معظم الأدبيات على البنية ثلاثية الطبقات لإنترنت الأشياء، يجري تعريف تلك الطبقات من الأسفل الأعلى كالتالي: Perception، Network وApplication. تحوي كل طبقة على مشاكل أمنية مرتبطة بها، يظهر الشكل 2-1 تلك البنية من وجهة نظر الأجهزة المستخدمة في كل طبقة.



الشكل 2-1 بنية **IoT** ثلاثية الطبقات.

طبقة Perception:

تُعرَف أيضاً بطبقة الحساسات (Sensors Layer)، تقوم الحساسات والمحركات التي تعمل في تلك الطبقة بجمع المعلومات من البيئة المحيطة، تعمل هذه الطبقة على اكتشاف، جمع ومعالجة المعلومات ثم نقلها إلى طبقة الشبكة، كما تقوم هذه الطبقة بدور عقدة IOT في الشبكات المحلية وقصيرة المدى.

طبقة Network:

تقوم هذه الطبقة في IOT بتوجيه البيانات وإرسالها إلى عقد وتجهيزات أخرى متصلة بالإنترنت، تعمل في هذه الطبقة منصات الحوسبة السحابية، بوابات الانترنت، الموجهات والمبدّلات (switches) باستخدام تقنيات حديثة

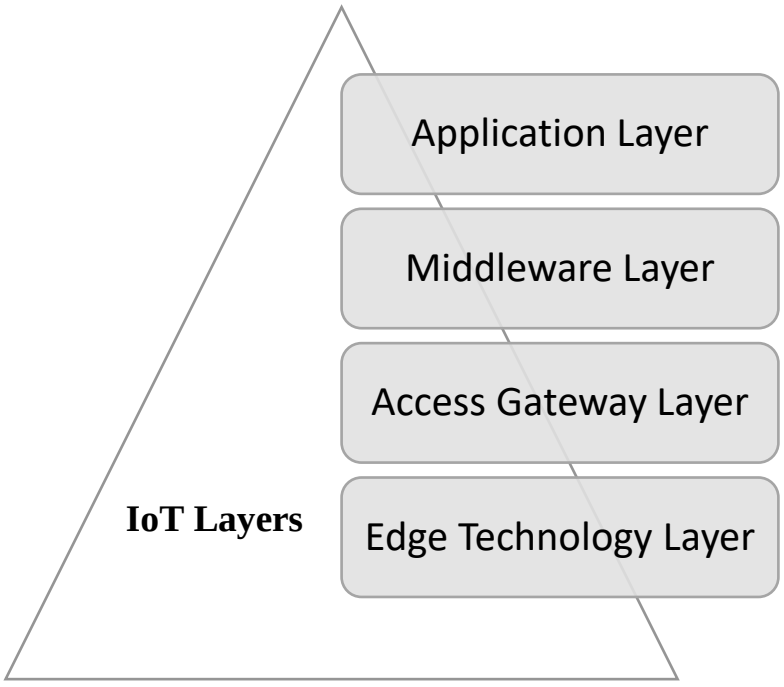
مثل Wi-Fi، LTE، Bluetooth، 3G، Zigbee الخ ... (كما سنرى في الفقرة 2.2.3.1-)، تعمل بوابات الشبكة كوسيط بين عقد IOT المختلفة عن طريق تجميع البيانات وترشيحها ونقلها من وإلى حساسات مختلفة.

طبقة Application:

تضمن طبقة التطبيقات صحة، سلامة وسرية البيانات، يجري في هذه الطبقة تحقيق الغرض من انترنت الأشياء في الوصول إلى بيئة ذكية. تسمى أيضاً طبقة Business، فهي تستقبل البيانات من طبقة الشبكة وتستخدم تلك البيانات لتنفيذ خدمات وعمليات معينة، وتُعنى على سبيل المثال بخدمات التخزين لأخذ نسخ احتياطية للبيانات المستلَمة ونقلها إلى قواعد البيانات، إضافةً إلى تحليل البيانات المستلمة والاستفادة منها في توقع حالة المكونات (الأجهزة) الفيزيائية.

2.1.3.1- بنية IoT ذات أربع طبقات

تبدأ من طبقة edge technology في الأسفل، وتنتهي بطبقة Application كما هو موضح في الشكل 1-3. تساهِم الطبقتان السّفليتان في جمع البيانات، بينما تُعنى الطبقتان العلويتان في استخدام تلك البيانات في التطبيقات.



الشكل 1-3 بنية **IOT** رباعية الطبقات.

يمكننا تصنيف وظائف الطبقات السابقة كالتالي:

1. Edge Technology Layer:

هي طبقة العتاد الصلب (Hardware)، تتضمن عناصر جمع البيانات مثل شبكات الحساسات اللاسلكية (WSNs)، أنظمة RFID، كاميرات، intelligent terminals، واجهات البيانات الالكترونية (EDIs) وأنظمة تحديد الموقع GPS. توفر تلك العناصر تحديد وتخزين المعلومات (بواسطة RFID tags)، جمع المعلومات (بواسطة الحساسات)، معالجة المعلومات (بواسطة Embedded Edge Processors)، الاتصالات، التحكم والتشغيل (بواسطة الروبوتات).

تجدر الإشارة إلى أن WSNs وأنظمة RFID هي تقنيات IOT الأكثر شيوعاً لذلك سنتحدث عنهما قليلاً:

- أنظمة RFID: تُعتبر من أهم عناصر ومكونات انترنت الأشياء، تقوم بنقل البيانات بواسطة جهاز محمول يدعى RFID tag، يقوم قارئ RFID بقراءة الـ tag ويعالج البيانات التي جرى الحصول عليها وفقاً لاحتياجات تطبيق معين. يستخدَم بشكل أساسي في المراقبة (monitoring)، التحكم بالوصول (Access Control)، والتتبّع (Tracking).
- WSNs: تتكون من عدد كبير من عقد الاستشعار، التي توصل نتائج قراءات الحساسات إلى عقد خاصة تسمى sinks.

2. Access Gateway Layer:

هي الطبقة المسؤولة عن التعامل مع البيانات، كإرسالها وتوجيه الرسائل ونشرها والاشتراك بها. فهي ترسل المعلومات الواردة من الطبقة السفلى (Edge) إلى الطبقة الأعلى (middleware) باستخدام تقنيات الاتصال المختلفة مثل: Wi-Fi, Li-Fi, Ethernet, GSM, WiMAX.

3. Middleware Layer:

هي عبارة عن منصة برمجية توفر التجريد للتطبيقات من الأشياء، كما تقدم العديد من الخدمات مثل اكتشاف الأجهزة، إدارتها، تجميع البيانات، ترشيحها، تحليلها، التحكم بالوصول واكتشاف المعلومات باستخدام تقنية EPC أو ONS.

4. Application Layer:

هي الطبقة العليا، مسؤولة عن إيصال كافة التطبيقات إلى مستخدمي انترنت الأشياء، تتألف من طبقتين جزئيَّتين هما:

- طبقة إدارة البيانات Data Management Sub-Layer: مسؤولة عما يلي:

- Directory Service
- جودة الخدمة QoS.
- تقنيات الحوسبة السحابية.
- خدمات الآلة للآلة M2M.
- .....

- طبقة خدمة التطبيق Application Service Sub-Layer: مسؤولة عن التفاعل مع المستخدم النهائي لتطبيقات انترنت الأشياء.

الجدول 1-1 طبقات وعناصر IoT.

طبقات IoT	عناصر IoT	المهام	التقنيات المستخدَمة
طبقة التطبيقات	التطبيقات	تقديم المساعدة للمستخدمين في البيئات الذكية، وتمكينهم من قراءة البيانات التي تخصّهم.	تقنية المنزل الذكي، الروبوتات، الحوسبتان السحابية والضبابية.
طبقة Middleware	اكتشاف الجهاز، التحكم بالوصول، إدارة البيانات	تمكين الاتصالات بين التطبيقات والأشياء.	CoAP, MQTT, REST, OMA Lightweight, OMA DM, EPC, ONS.
طبقة Access Gateway	تقنيات الاتصالات	WWAN: إرسال المعلومات من الجهاز أو البوابة عبر الانترنت.	2G, 3G, LTE, LTE-A, Satellite networks, etc.
		WPAN، WLAN: تمكين الأجهزة من مشاركة أو تبادل المعلومات.	RFID, Bluetooth, Wi-Fi, Li-Fi, ZigBee, 6LoWPAN.
طبقة Edge Technology	أشياء مادية (فيزيائية)	جمع، مراقبة، وتعريف البيانات في الأوساط الفيزيائية للحساسات.	RFID, sensors, actuators.

2.3.1- عناصر ومكوّنات انترنت الأشياء

تتضمن انترنت الأشياء عناصر مختلفة تعمل معاً، سنناقش الآن مكونات IOT المذكورة في الجدول 1-1:

1.2.3.1- العناصر الفيزيائية (المادية) لإنترنت الأشياء:

هي العناصر أو التجهيزات المادية (العتاد الصلب) التي تقوم بجمع، تحديد، ومراقبة المعلومات في الأوساط الفيزيائية الموجودة فيها (مثل حساس الحرارة، حساس قياس ضغط الدم للمريض، ...)، وإرسالها عبر الشبكة إلى وجهتها المحددة من قبل التطبيق.

2.2.3.1- عناصر تقنيات الاتصالات لإنترنت الأشياء:

تعتمد تطبيقات انترنت الأشياء على شبكات عديدة، منها PAN، LAN وWAN، يتضمّن كلٌّ منها عدداً من التقنيات اللاسلكية الموضّحة في السطر "طبقة Access Gateway " من الجدول 1-1. تستخدِم تطبيقات انترنت الأشياء العديد من تقنيات الاتصالات منها [3]:

- ZigBee: هي المعيار IEEE 802.15.4 للطاقة المنخفضة والمدى القصير، تعتمد على شبكة LR-WPAN، وهي أقل تكلفة من البلوتوث وتعمل في الحزمة 2.4 GHz.
- Bluetooth: هي المعيار IEEE 802.15.1 للترددات الراديوية لمسافات قصيرة منخفضة الطاقة، تستخدَم في تكوين الاتصال من نقطة لنقطة (P2P) ومن نقطة إلى مجموعة نقط (P2MP) بالاعتماد على شبكة WPAN التي تعمل في حزمة ISM (2.4 GHz) ، تتمتع أجهزة بلوتوث برخص ثمنها واستهلاكها المنخفض للطاقة.
- Light Fidelity (Li-Fi): هو نظام اتصال ضوئي (VLC) يستخدم الضوء المرئي بدلاً من الأمواج الراديوية بطريقة مشابهة لِ Wi-Fi (يستخدم بروتوكول TCP/IP) لإرسال واستقبال البيانات. يتمتّع بتكلفة منخفضة ومناعة ضد التنصت كونه لا يخترق الجدران، بينما يعاني من التشويش من مصادر الضوء الأخرى ويحتاج إلى خط نظر (LOS) بين المرسل والمستقبل.
- Wi-Fi: توجد العديد من إصدارات Wi-Fi، مثل IEEE 802.11x (WLAN)، تعمل على ثلاث تقنيات مختلفة هي النثر الطيفي بالسلاسل المباشرة (DSSS)، النثر الطيفي بالقفز الترددي (FHSS)، والأشعة تحت الحمراء (IR)، وتفيد في إعداد كِلتا الشبكتين P2P وP2MP. يوفّر IEEE 802.11n أداءً

جيداً بمعدّل نقل يصل إلى 600 Mbps باستخدام الحزمتين الترددیتین 2.4 GHz أو 5 GHz (RF)، ويمكنه استخدام تقنية MIMO للاستفادة القصوى من عرض الحزمة الترددية المتاح، يمكن توفير أمن Wi-Fi من خلال البروتوكولات التالية: WEP، WPA، وWPA2.

- Long Term Evolution (LTE): هو معيار عريض الحزمة الترددية لشبكة 4G اللاسلكية، جرى تطويره من قبل مشروع شراكة الجيل الثالث (3GPP) القائم على WWAN، يوفّر LTE معدّل نقل للوصلة الصاعدة (UL) يصل إلى 75 Mbps و 300 Mbps للوصلة الهابطة (DL)، كما توفّر حلاً فعالاً من حيث التكلفة لخدمات M2M لكافة تطبيقات انترنت الأشياء.
- Long Term Evolution-Advanced (LTE-A): هو معيار دقيق لاتصالات 4G الخلوية، وهو تحسين كبير لـ LTE، يوفّر معدلات نقل عالية تصل إلى 3 Gbps للوصلة الهابطة و1.5 Gbps للوصلة الصاعدة وتأخير زمني منخفض، يجب أن تكون LTE-A متوافقة مع أجهزة LTE، لذا يمكن لخدمات M2M المحدَّثة الاستفادة من شبكات LTE الحالية.

3.2.3.1- عناصر تطبيقات انترنت الأشياء

هي عناصر مسؤولة عن تنسيق البيانات وترتيب تدفقها من أجل تطبيقات معينة (مثل الرعاية الصحية)، توفّر المساعدة للمستخدمين من خلال التقنيات الذكية كالمنزل الذكي بواسطة الحساسات اللاسلكية داخل المنزل أو الحساسات القابلة للارتداء بطريقة تحافظ على خصوصية المستخدمين أثناء جمع بياناتهم وتقديم إشعارات مناسبة للتصرفات غير الطبيعية. تجري معالجة المعلومات في طبقة التطبيقات لإنترنت الأشياء باستخدام الحوسبة السحابية والضبابية، **حيث توفّر** الحوسبة السحابية ثلاثة أنواع من الخدمة:

- البنية التحتية كخدمة Infrastructure as a Service (IaaS): تتضمن البيئةُ التحتية العتادَ الصلب والمرن مثل أجهزة التخزين، الشبكات، البيانات، التطبيقات وأنظمة التشغيل، حيث يستطيع المستخدمون طلبَ إعدادات بنية تحتية معينة، ثم تقوم السحابة بمهام الإدارة والتنظيم بدلاً عنهم.
- المنصة كخدمة Platform as a Service (PaaS): تستطيع السحابة توفير مجموعة من الخدمات والأدوات التي تسهّل إنشاء تطبيقات المستخدمين وتشغيلها بشكل فعال، حيث يمكن للمستخدمين التحكم الكامل بتطبيقاتهم في السحابة ولكنّهم مقيّدون باستخدام نظام التشغيل[1]، العتاد الصلب والبنية التحتية للشبكة في السحابة.

[1] يمكن للمستخدمين تشغيل مدير آلة افتراضية والتحكم بنظام التشغيل داخل بيئة تحكم الآلة.

- البرمجيات كخدمة Software as a Service (SaaS): تؤمن للمستخدمين تطبيقاتٍ على الشبكة.

بينما توسّع الحوسبةُ الضبابية مفهومَ الحوسبةِ السحابية، فهي بنية تحتية للحوسبة الموزّعة، تقوم بتوفير نفس خدمات التطبيقات التي تقدمها الحوسبة السحابية للمستخدمين النهائيين مثل معالجة البيانات، التخزين، وتنفيذ التطبيقات، لكن يجري التعامل مع خدمات التطبيقات على حافة الشبكة من خلال جهاز ذكي بدلاً من مركز بيانات (data center) بعيد في السحابة، تهدُف الحوسبة الضبابية إلى تحسين الفعالية وتخفيض حجم البيانات المنقولة إلى السحابة.

3.3.1- تطبيقات انترنت الأشياء

تقدّم أنظمة انترنت الأشياء الكثيرَ من الخدمات في كافة المجالات [4]، يتضمن العديد منها تطبيقاتٍ جديدة تؤثر في حياتنا اليومية داخل أو خارج المنزل وفي العمل، لكن مازالت تلك التطبيقات مقتصرة على فئة صغيرة من مجتمعنا. إن معظم العناصر في البيئات المختلفة التي نعيش فيها ليست ذكية بعد بوجود انترنت الأشياء، لكن العمل على جعل العناصر ذكية سيغني العديد من مجالات الحياة، ومن هذه المجالات:

- مجال النقل واللوجستيات.
- مجال الرعاية الصحية.
- مجال البيئات الذكية (منزل، مكتب، مدينة، ....).
- المجال الشخصي والاجتماعي.

إن بعض تطبيقات انترنت الأشياء قابلة للتطبيق أو الإغلاق مباشرةً، وبعضها قابل للتطبيق في مجتمعاتنا في وقت لاحق تبعاً لتطور التكنولوجيا (الجدول 1-2)، سنقوم في هذه الفقرة بمناقشة تطبيقات انترنت الأشياء القصيرة إلى متوسطة المدى.

الجدول 1-2 مجالات التطبيقات والسيناريوهات الرئيسية المتعلقة بانترنت الأشياء.

النقل واللّوجستيات	الرعاية الصحية	البيئات الذكية	المجال الشخصي والاجتماعي	مجالات مستقبلية
لوجستيات	التّتبّع	المنازل والمكاتب الذكية	الهندسة الاجتماعية	روبوت تاكسي
المساعدة في القيادة	التعرف على الهوية والمصادقة	الخطط الصناعية	استعلامات تاريخية	نموذج معلومات المدينة

تذاكر الموبايل	جمع البيانات	النوادي الرياضية الذكية	الخسائر	غرف ألعاب محسّنة
مراقبة الوسط	التحسّس	المتاحف الذكية	السرقات	
خرائط واقعية				

1.3.3.1- مجال النقل واللّوجستيات

تقدم انترنت الأشياء الكثير من الإمكانات في مجال الخدمات اللّوجستية، وخصوصاً عندما يتعلق الأمر بمعلومات في الزمن الحقيقي عن أشياء في سلسلة الإمداد (supply chain)، وذلك اعتماداً على رقاقات وقارئات RFID، إضافةً إلى مراقبة كافة عناصر تلك سلسلة. ومن المحتمل أن تكون انترنت الأشياء قابلة للتطبيق على أجزاء متعددة من سلاسل الإمداد المتعلقة بشراء المواد الخام، النقل، التوزيع، البيع، خدمة ما بعد البيع وغيرها. قد يقلل استخدام انترنت الأشياء من زمن الاستجابة عند حدوث خطأ ما، فمثلاً، تستخدم شركة Walmart تقنية انترنت الأشياء لتتمكن دائماً من تقديم خدماتها لزبائنها دون أن تنفَذ مخزوناتها من أي شيء، توفر هذه التقنية للمستهلكين أيضاً إمكانية عرض معلومات في الزمن الحقيقي حول طلباتهم كالموقع الحالي والزمن المتوقَّع للوصول إضافة إلى معلومات أخرى.

تعدَّت خدمات انترنت الأشياء في المجال اللّوجستي، فلم تتوقف فقط على سلاسل الإمداد، وإنما ساهمت أيضاً في موضوع المساعدة في القيادة (Assisted Driving)، وذلك من خلال تزويد السيارات والحافلات والقطارات بحساسات، كما يجري تزويد الطرقات والسّكك الحديديّة بحساسات ومعالجات صغرية لتحسين خيارات السلامة والأمان لجميع مستخدمي تلك الطرق، فهي تقدّم وظائف عديدة مثل نظام تجنب التصادم، الوقوف الأوتوماتيكي، القيادة الذكية للسيارات على الطرق السريعة.

كما تساعد هذه التقنيةُ الحكومات في تتبّع النشاطات غير المشروعة، المساهمة في تحسين خارطة الطرق عند توسيعها واختيار المسار الأفضل للسيارات في حالات الازدحام المروري. إضافةً إلى خدمات أخرى في مجال سلسلة الإمداد الغذائية، مثل مراقبة وضبط الغذاء وضمان سلامته عند نقله من مكان إلى آخر.

2.3.3.1- مجال الرعاية الصحية:

تتمثّل الفوائد الرئيسيّة لإنترنت الأشياء في الرعاية الصحية بتتبّع المرضى والموظفين والأشياء، تحديد هوية الأشخاص، المصادقة والتحقق، جمع البيانات والتّحسّس الأوتوماتيكي، مما يساعد المستشفيات على تحسين سير العمل، وجدولة صيانة الآلات والمعدّات. يضمن تحديد هوية المرضى في المشافي تفادي الحوادث الضارة التي ممكن أن تصيبهم مثل الجرعات الخاطئة، كما يضمن التعرف على الرّضّع، وتضمَن المصادقة أماناً أكثر للمستشفى.

تهدف انترنت الأشياء فيما يتعلق بجمع البيانات في المشافي إلى تقليل الوقت المستغرَق في التسجيل اليدوي، والحد من عبء العمل على موظفي المستشفيات، وتمكينهم من القيام بوظائفهم الأخرى الأكثر أهمية، من خلال تكامل تقنية RFID مع المعلومات الصحية ومعلومات المستشفيات.

وأخيراً، يمكن أن يوفر التحسس (الاستشعار) في نظام الرعاية الصحية معلومات مفيدة عن صحة المرضى وتشخيصاتهم، حيث تقوم الحساسات بمراقبة المؤشرات الصحية للمرضى في الوقت الحقيقي، مما يساهم أيضاً في مراقبة استجابة المرضى لأدوية معينة ويوفر المراقبة والمعالجة عن بعد.

3.3.3.1- مجال البيئات الذكية

تجعل فكرةُ البيئاتِ الذكية البيئةَ المحيطة بنا سهلةً ومريحة في سياقاتٍ مختلفة، من خلال تطبيق تقنية انترنت الأشياء على تلك البيئات مما يجعل الأشياء المحيطة بنا ذكية تقوم بمهامٍ مختلفة، ومن هذه البيئات: المنزل، المكتب، والنادي الرياضي ....

يمكن جعل المنازل والمكاتب أكثر راحة من خلال تزويدها بحساسات ومحركات تقوم بالتحكم في تلك البيئات، من خلال التحكم في الإضاءة والتهوية ودرجة الحرارة وضبطها في المباني الكبيرة عن طريق توزيعها بالشكل المناسب دون الحاجة إلى تبريد الطوابق العلوية وتسخين الطوابق السفلية. يمكن في المحطات الصناعية أن يؤدي نشر رقاقات RFID على الأشياء التي تجري معالجتها إلى تقديم معلومات مفيدة عن اختناقات الإنتاج، التحكم بجودته، إضافةً إلى إعطاء الموظفين معلومات تفيدهم في عملهم واتّخاذ قراراتهم وخصوصاً في حالات الطوارئ. ومن الاستخدامات الأخرى لإنترنت الأشياء في البيئات الذكية، الصالات الرياضية الذكية حيث تقوم الأجهزة الذكية بتسجيل مجموعات تكرارات اللاعبين مما يساعدهم في التدريب ويقلّل من عناء التسجيل اليدوي ويقلّص الأخطاء، كما يساعد المدربَ الشخصي في مراقبة اللاعب وإرشاده بالشّكل السليم. كما تحوي المتاحف الذكية على رقاقات يجري وضعها بالقرب من التّحف المختلفة لتسهيل حركة الزوار وجعل زيارتهم أكثر إفادة وتفاعلية، إضافةً إلى تدخل المحركات الذكية في جعل صالات المتحف تلائم الطقس الحقيقي سواء كان جليدياً أم صحراوياً كزيارة متحف عن الأهرامات مثلاً.

1.3.3.3.1- المنزل الذكي

نجد مما سبق أن العديد من الأجهزة قد أصبحت ذكية بالفعل. ومع ذلك، فمن الواضح أن أغلب المشاكل المتعلقة بالأمن والخصوصية مازالت دون حلول. تقدّم جميع التطبيقات التي جرت مناقشتها في 2.1- مثل المكاتب والمدن الذكية مجالات مثيرة للاهتمام، لكن سنركّز في هذه الرسالة على حالة بيت ذكي حيث أن معظم تلك الأجهزة المنتشرة في السوق دخلت إلى بيوت المستخدمين والذين لا يمتلكون الخبرة التقنية الكافية، جزء من تلك الأجهزة متحرك نسبياً مثل الحساسات، الثلاجات والشاشات الذكية، والجزء الآخر قد يدخل ويغادر المنزل من وقت لآخر مثل الهواتف الذكية والأجهزة القابلة للارتداء. سيضمّ المنزل الذكي إذاً مجموعة متنوعة من الكائنات ذات الخصائص والقدرات

المتغايرة. يمكننا بشكل رسمي أكثر تحديد بعض الفئات لتصنيف أجهزتنا المنزلية الذكية، بعضها حساسات تقوم بقياس الظواهر الفيزيائية مثل درجة الحرارة والرطوبة (الشكل 1-4)، أو الكشف عن الحركة أو التواجد. وبعضها هي المحركات، التي تقوم بخلق ظواهر ميكانيكية مثل فتح وإغلاق الأبواب والنوافذ. تعتبر أيضاً أجهزة الإدخال جزءاً من المنزل الذكي، مثل لوحة الإدخال للتحكم في التسخين. كما توجد أجهزة إخراج مسؤولة عن تقديم المعلومات للمستخدمين عن طريق شاشات، سماعات ....

ستكون العديد من الأجهزة عبارة عن أجهزة مركبة تجمع خصائصَ مختلفِ التصنيفات التي ذكرناها سابقاً، تتفاعل مع المستخدم حيث تدمج وظائف المدخلات والمخرجات معاً كأن تقدم إشعارات (Notifications) للمستخدمين، وبنفس الوقت تقبَل أوامر تحكم من قبلهم.

نستنتج وضوحاً من الوصف السابق أن العديد من الأنظمة الفرعية ستصبح جزءاً من المنزل الذكي، وسيجري دمج التحكم في الإضاءة مع التحكم في الحرارة (التكييف والتدفئة). كما ستصبح أجهزة التلفزيون الذكية وأنظمة الصوت HiFi والثلاجات الذكية متّصلة. ستقدّم أيضاً بعض الأجهزة المنزلية الشائعة كالفرن والمحمصة خدماتها للمنزل الذكي، توجد أمثلة أخرى كرقاقات RFID واستخداماتها مع العناصر ذات الاستخدام اليومي كالملابس. لاتزال أشياء مثل السيارات الذكية تبدو مستقبلية، لكنها ستصبح أيضاً جزءاً من انترنت الأشياء مع تقدم التكنولوجيا، بينما نجد الأجهزة المتفاعلة مع المستخدم موجودة بشكل يومي كالأجهزة اللوحية والحواسب المحمولة ....

يمكن وضع عقدة على حافة المنزل الذكي تكون عبارة عن بوابة (Gateway) تفصل بين المنزل وبقية الانترنت (كما سنرى في الفقرة 3.4–)، تكون عبارة عن راوتر أو جهاز منفصل يضمن تدفق البيانات بأمان من وإلى المنزل الذكي. من الواضح أن إدخال بوابة لمراقبة الأجهزة يخلق درجة من المركزية، وهذا أمر جيد في ظروف معينة حيث أن بعض التجهيزات لا يمكنها توفير الأمن الكافي بمفردها.

4.3.3.1- المجال الشخصي والاجتماعي

تتعلق تطبيقات انترنت الأشياء في المجال الشخصي والاجتماعي بالحياة الاجتماعية للأشخاص والتفاعل الاجتماعي، وذلك من خلال مساعدة الأشخاص في التفاعل فيما بينهم للحفاظ على علاقاتهم وبناء علاقات جديدة. قد تصبح انترنت الأشياء أداةً أساسية للتواصل الاجتماعي، من خلال الحصول على تحديثات تلقائية حول نشاطاتنا الحياتية اليومية المنشورة على شبكات التواصل الاجتماعي كالفيس بوك، حيث يجري العمل على إتاحة المجال لتقنية RFID بإنشاء أحداث عن الأشخاص أو الأماكن، ثم نشر تلك الأحداث على الشبكات الاجتماعية من أجل تزويد المستخدمين في الزمن الحقيقي بما يجري حولهم وما يجري مع معارفهم، مما يتيح للمستخدمين مشاركة أصدقائهم في حياتهم ونشاطاتهم عن قرب. وتصبح ملاحقة الأشياء المفقودة أو المسروقة أكثر مرونةً عند تزويدها برقاقة RFID،

التي من الممكن أيضاً أن ترسل بنفسها إشعارات إلى المستخدم في حال وجدت نفسها في مكان غريب تزوره لأول مرة.

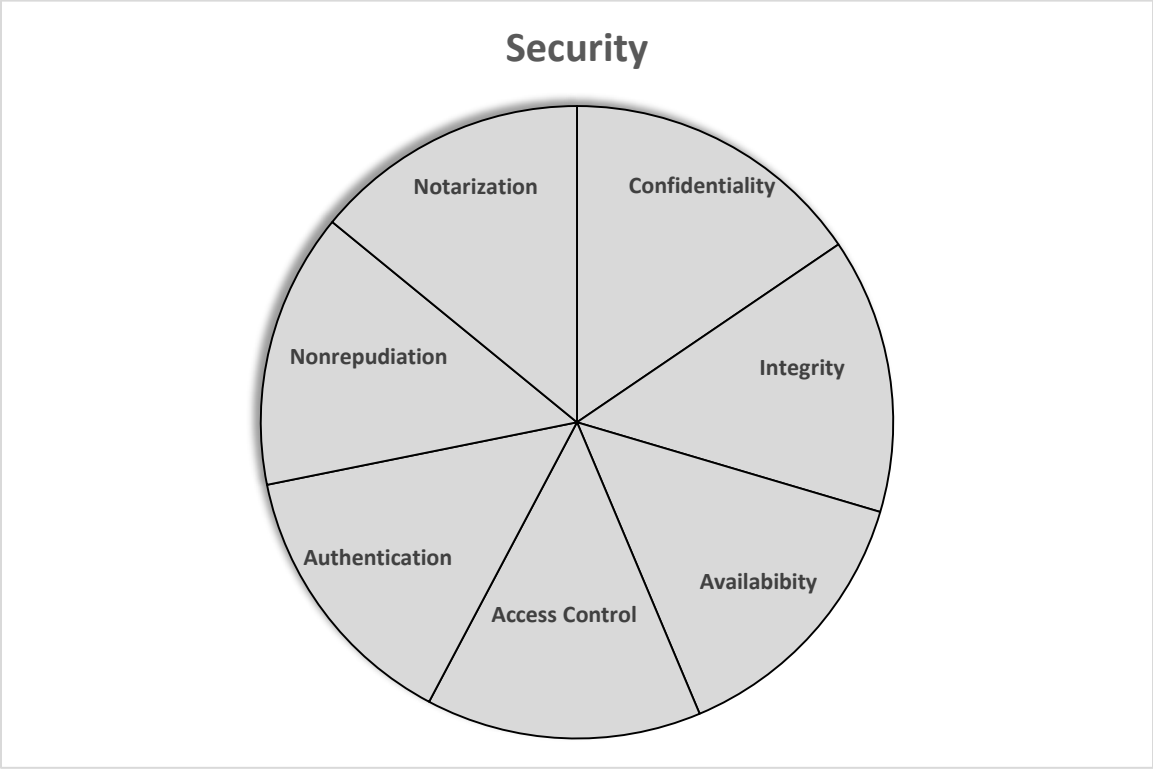
الشكل 1-4 كاميرا **HD** مع حساس حرارة ورطوبة.

4.1- الأمن والخصوصية

يمكننا تعريف الأمن بأنه منع الوصول إلى المعلومات أو الموارد من قبل المستخدمين غير المخولين بالوصول، إضافةً إلى الحماية ضد التعديلات غير المصرح بها أو إتلاف معلومات المستخدمين. يتضمن التعريف التقليدي للأمن الثلاثية الشهيرة CIA وهي السّريّة (Confidentiality)، السلامة (Integrity)، وَالتوافريّة (Availability). بينما يوسّع معيار ISO 7498-2 ذلكَ التعريف كما هو موضح في الشكل 1-5 إلى المتطلبات التالية التي تحمل الاختصار CIA-AANN [5] [6] :

- السرية: أي أن المعلومات غير متاحة أو لا يجري الكشف عنها لأفراد أو كيانات أو عمليات غير مخولة.

- السلامة: أي ألّا يجري تغيير أو إتلاف المعلومات بطريقة غير مصرح بها، وأن تصل إلى وجهتها كما خرجت من المصدر.
- التوافرية: أي الحفاظ على وظائف النظام عند الحاجة لها من قبل الكيانات المخوّلة.
- التحكم في الوصول Access Control: لا يدخل المستخدمون إلّا إلى الموارد والخدمات التي يحق لهم الوصول إليها، ولا يُحرَم المستخدمون المخوَّلون من الوصول إلى الموارد التي يحق لهم الوصول إليها.
- المصادقة Authentication: هي التحقق من صحة هوية كيان ما، أو التحقق من صحة البيانات المستلَمة.
- عدم الإنكار Nonrepudiation: هي منع مرسلي أو مستقبلي الرسائل من إنكار قيامهم بالفعل بالإرسال أو الاستقبال.
- التوثيق Notarization: أي تسجيل البيانات مع طرف ثالث موثوق يضمن دقة خصائصها مثل المحتوى، الأصل ووقت الإنشاء.



الشكل 1-5 خدمات الأمن.

بينما نعرف الخصوصية بأنها ضمان حق المستخدمين في التحكم بالمعلومات التي يجري جمعها عنهم، من يحتفظ بها، من يستخدمها، كيف يجري استخدامها والغرض من استخدامها [7]. يظهر الشكل 1-6 خدمات وخصائص الخصوصية التي سنعرّفها كما يلي:

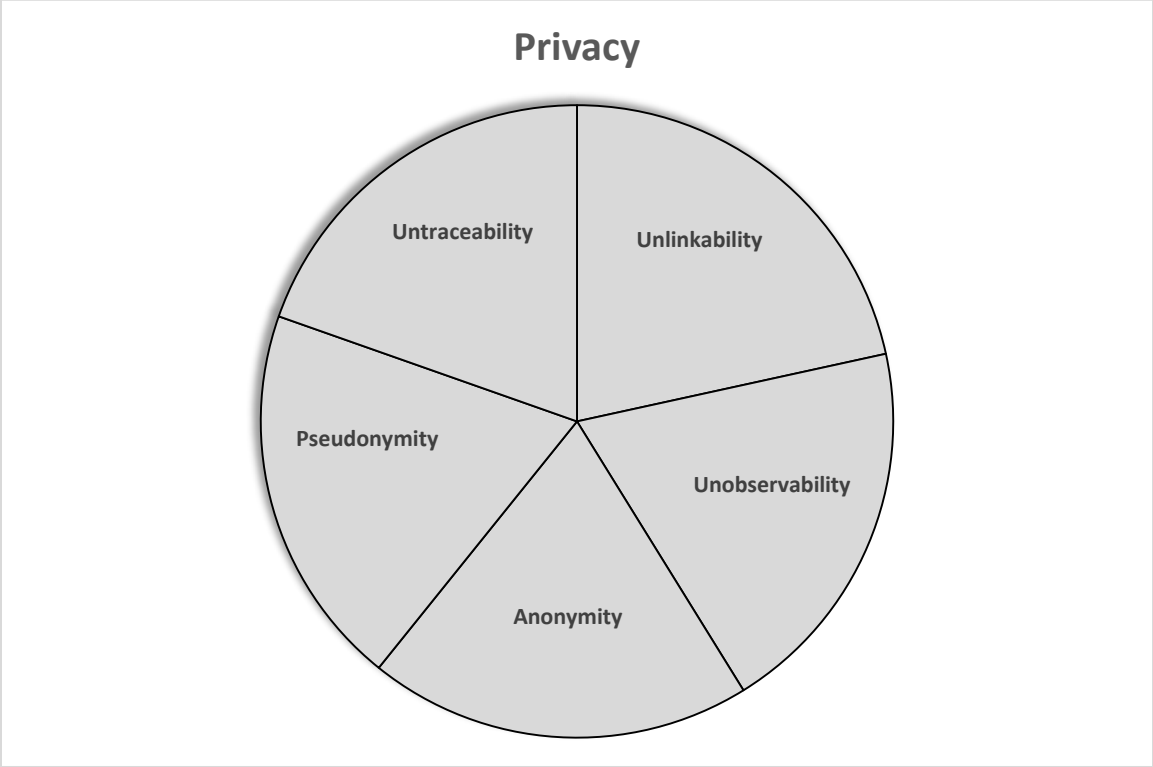
- عدم التّتبّع Untraceability: يهدف إلى عرقلة الخصم في تحديد الهوية الحقيقية لكيان ما تبعاً لمجموعة من النشاطات التي قام بها ذلك الكيان. يفيد إخفاء الهوية (Anonymity) في ضمان عدم التّتبّع لكنه غير كافٍ لأنه إذا عرف الخصم أن مجموعة معينة من النشاطات صادرة عن كيان معين دون معرفة هوية ذلك الكيان فلن يجري تحقيق عدم التتبع.

- إخفاء الترابط Unlinkability: هي تعميم لمفهومَي إخفاء الهوية وعدم التتبع، وتعني إخفاء المعلومات حول العلاقة بين أيّة عناصر (كالرسائل، النشاطات وغيرها). في حالة إخفاء الهوية، يصعُب على الخصم ربط النشاطات المراقَبة بالهوية الحقيقية لمرتكبِها. أما في حالة عدم التتبع، فلن يستطيع الخصم استنتاج النشاطات الصادرة عن نفس الكيان.

- Unobservability: هي إخفاء العناصر (بعكس Unlinkability الذي كان يركز على إخفاء العلاقات بين العناصر)، فمثلاً هي إخفاء حقيقة إرسال الرسالة (بدلاً من إخفاء هوية مرسل الرسالة).

- إخفاء الهوية Anonymity: هي إخفاء الهوية الحقيقية لمن قام بنشاط معيّن (غالباً نشاط اتصالات كإرسال أو استقبال رسالة)، وبالتالي يصعب على الخصم ربط نشاط معين بصاحبه مما يدعم خصوصية المستخدمين. لا يمكن تحقيق الغاية من إخفاء الهوية إلّا إذا كانت جميع الكيانات في النظام تتمتّع بسمات متشابهة وتقوم بنفس النشاطات، أي إذا وجد نشاط أو مهمة لا يمكن إنجازها إلّا من قبل كيان معين فإن الخصم سيستطيع ببساطة تحديد هوية الكيان بمجرد قيامه بذلك النشاط.

- الأسماء المستعارة Pseudonymity: هي استخدام معرّفات (هويات) مستعارة بدلاً من الهوية الحقيقية، وهي مفيدة في حال عدم حصول الخصم على أي ترابط بين الهوية الحقيقية والمستعارة.



الشكل 1-6 خدمات الخصوصية.

5.1- المتطلبات الأمنية لإنترنت الأشياء والحلول المقترَحة

تجلب شبكة صاعدة من "الأشياء" تحدياتٍ تتعلق بالأمن والخصوصية، تصبح فيها السرية، السلامة والتوافرية عناصراً في غاية الأهمية أثناء تبادل البيانات بين تجهيزات انترنت الأشياء التي وصلت إلى ذكاء وتوزع واستقلالية تتطلب مزيداً من المسؤولية عند العمل على حمايتها من التلف وما قد يرافقه من تأثيرات على الشبكة. تتوفر حلول تعمية مختلفة وحلول process-based لضمان وتحقيق السرية والسلامة والتوافرية، لكن أنظمة انترنت الأشياء لا تتطلب تلك الخدمات فحسب، وإنما تحتاج أيضاً إلى التركيز على كيفية تنفيذ تلك الحلول وتحسينها. تعتمد انترنت الأشياء اعتماداً كبيراً على الشبكات اللاسلكية المعروفة بأنها عرضة للكثير من أنواع الاختراقات مثل:

- Unauthorized router access.
- Faulty configurations.
- Jamming.
- Man-in-the-middle.

- Interference.
- Spoofing.
- Denial of Service.
- Brute-force.
- Traffic injections.

وغيرها من الهجمات التي سنتحدث عنها في الفقرة (2.6.1-). يمثّل الأمنُ مصدرَ قلقٍ رئيسي للشبكات الكبيرة. لذا، فإن المكونات المادية لإنترنت الأشياء معرضة لهجمات السرية، السلامة والتوافرية مما يستدعي تطبيق عمليات التعمية كخط دفاع أول لضمان السرية، وتطبيق منهجيات مصادقة الرسالة لضمان السلامة [8]. اعتادت تنجيزات WSN في البداية على التعامل مع نماذج التّهديدات التي تتطلّب الوصول الفعلي (الفيزيائي) إلى العقد، لكن تلك النماذج تغيّرت لاحقاً بعد فتح تجهيزات WSNs على الانترنت حيث يمكن للمهاجمين الوصول إلى العقد في أي مكان مستغلّةً ضعف الموارد الحسابية لعُقَد الحساسات، مما يستدعي تطبيق مستويات أمن مختلفة لجعل تطبيقات انترنت الأشياء موثوقة من قبل المستخدمين كون تلك التطبيقات وتجهيزاتها غير متجانسة ولها متطلبات مختلفة.

يمكن استخدام معيار IEEE 802.15.4 الذي يقدِّم توجيهات لحماية طبقات التحكم بالوصول الفيزيائي (Physical Access Control Layers) كأداة لإضافة ميزات الأمن التي تلخّص خصائص السرية والسلامة والتوافرية للنظام [9]. تحدّثنا في الفقرة (4.1-) عن المتطلّبات الأمنية العامة لأي نظام معلومات أواتصالات، وسنناقش فيما يلي أهم المتطلبات الأمنية والخصوصية التي تواجه انتشار أنظمة IoT بشكل خاص مع بعض الحلول الأمنية المقترَحة في الأدبيات:

- السرية: عرّف المؤلفون في [11] ,[10] سرية البيانات على أنها قضية أساسية لحلول انترنت الأشياء، ذات صلة خاصة بسياق الأعمال التجارية والصناعية، قد يصعب تطبيق حلول سرية البيانات الحالية بسبب قيدين: الأول هو كمية البيانات التي يجري إنشاؤها، والثاني هو فعالية التحكم في الوصول إلى البيانات المضمنة في تدفقات البيانات الديناميكية، كما ذكر المؤلفون أن الإدارة الصحيحة للهوية هي عامل رئيسي لضمان سرية البيانات. تحتاج بعض تجهيزات انترنت الأشياء إلى التعامل مع بيانات تصنَّف بأنها سريّة. لذا، يجب العمل على تحقيق سرية قناة الاتصال وذلك من خلال عمليات التعمية مع التأكيد على تحليل خوارزميات التعمية المتناظرة وغير المتناظرة قبل تنجيزها بناءً على نوع التطبيق والإمكانات والنقاط الحرجة لنظام انترنت الأشياء. قد تكون الاتصالات اللاسلكية للأشياء هي الأكثر عرضة لهجمات التنصت (eavesdropping attacks) التي تؤثر على سرية الاتصال وعلى مجموعة من العقد أو على الشبكة ككل.

تعتبِر بعض المرجعيات [12] أن السرية المطلوبة لبيانات الحساسات ليست بنفس أهمية السلامة (integrity) والتحقق من الأصالة (authenticity) نظراً لأن المهاجم قد يحصل على نفس البيانات بمجرد وضع حساس تنصُّت بجوار الحساس الشرعي. وتعتبر دراسات أخرى [13] أن جوهر حساسية السرية يكمن في الاتصالات، التخزين، التّموضع، التعقب وتحديد الهوية أكثر من الحساسات والمحركات، توجد أيضاً أعمال بحثية كافية متاحة لضمان الاتصالات، التخزين، .... مع الاتفاق على مدى تعقيد استخدام الآليات الحالية لتأمين انترنت الأشياء. يجب أن تستخدم حلول انترنت الأشياء آلياتٍ أمنية تسمح بالوصول إلى مجموعة محددة مسبقاً من الموارد (بناءً على قرار المستخدم النهائي)، وهذا ما يسمى ملكية البيانات (Data Ownership)، هناك حاجة إلى التمييز بين متطلبات الأمن للأشياء بناءً على النقاط الحرجة. تدير تقنيات انترنت الأشياء عمليات أمن البيانات، بما في ذلك إدارة المفاتيح (Key Management) التي ترهق موارد تجهيزات انترنت الأشياء مما يقلل من قدراتها (وخصوصاً المعالجة والتخزين) ويزيد الخطر. لذا، جرى اقتراح استخدام خوارزميات تعمية خفيفة الوزن تتناسب مع التجهيزات محدودة الموارد وتمكّنها من توفير حماية البيانات، وبالتالي توفير السرية. يمكن في هذا السياق استخدام DTLS كحل لمشاكل السرية من خلال توفير الأمن من النهاية إلى النهاية (end-to-end security) لطبقة التطبيق application، كما تقلل خصائص DTLS من تأثير وتكلفة موارد الأجهزة المقيدة مقارنةً بالحلول الأخرى. اتجهت دراسات أخرى إلى حماية سرية البيانات والاتصالات في الحلول القائمة على السحابة إلى إنشاء قنوات اتصال آمنة قائمة على ميزات التعمية المعتمدة على استخدام PKI، يجري فيها التحكم بتدفق المعلومات كحل آخر لحماية مشاركة البيانات لإنترنت الأشياء باستخدام منصة قائمة على السحابة لحماية المعلومات الحرجة. تعتبَر خصوصية البشر وسرية الأعمال قضيتين رئيسيتين يجب معالجتهما لضمان نجاح أنظمة انترنت الأشياء، قد تعمل أنظمة التعمية النموذجية على حل المشكلة. ومع ذلك، يجب استخدام موارد الطاقة والمعالجة بكفاءة، بما في ذلك آليات توزيع المفاتيح، لكي يجري اعتبارها حلاً صالحاً لإنترنت الأشياء. يجري عادةً ربط السرية والخصوصية معاً حيث تُعتبَر الخصوصية كسريّة تمثّل حلولاً لإخفاء هوية البيانات المجمَّعة (متضمنةً الاتصالات) وتقليل جمع البيانات إلى الحد الأدنى، أي أن الاتصال المجهول الذي يخفي بيانات الموقع، الهوية، الزمن، التردد وحجم التفاصيل ضروري لحماية تدفق البيانات من الوصول غير المصرَّح به. لذا، يجب تطبيق تصميمات قائمة على الخصوصية وتقنيات لتحسينها من أجل زيادة مستويات حماية السرية. تتعامل السرية أيضاً مع التشريعات والقوانين الحكومية التي تطالب بحماية البيانات وسريتها، حيث أن الثقة أمر أساسي لمستخدمي انترنت الأشياء لأن تلك الأشياء تقوم بمشاركة بياناتهم الخصوصية. لذا، تعدّ السرية والخصوصية والثقة من العوامل الرئيسية التي ستؤثر على الانتشار الواسع لتقنيات انترنت الأشياء وتطبيقاتها.

- السلامة: تتعامل سلامة انترنت الأشياء مع الأعطال والقصور الفيزيائي كنظرة أولى، تتضمن حماية السلامة العملَ ضد التخريب وضد استخدام مكونات مزيفة، كما تُعتبر المتانة والتسامح مع الخطأ عوامل حرجة في أنظمة انترنت الأشياء. تواجه مثلاً شبكات الحساسات مثل حلول RFID قضايا أخرى تحدّ من قدرتها على مواجهة مشاكل السلامة حيث أن معظم مكوناتها تقضي غالب وقتها دون حضورها، مما يمكّن المهاجمين من تعديل البيانات عند تخزينها في العقدة أو أثناء انتقالها عبر الشبكة. لذا، تعتبَر صلاحيات القراءة والكتابة إضافةً إلى التحقق والمصادقة حلولاً شائعة لتلك المشكلات. يجري أيضاً ضمان حماية سلامة البيانات باستخدام حلول قائمة على كلمة المرور، مع أخذ أوجه القصور في حماية كلمة المرور بعين الاعتبار مثل طول كلمة المرور والعشوائية في تكوينها. مع التذكير مجدداً بأن الموارد الموجودة في أنظمة انترنت الأشياء لا تدعم حلول التعمية النموذجية بسبب محدودية الموارد المتاحة. يجب حماية سلامة انترنت الأشياء ليس فقط من المصادر الخارجية وإنما من العمليات الداخلية أيضاً، مثلا سلامة الخدمة (service Integrity). تساعد منهجياتُ فصل العمليات لأنظمة التشغيل، المعروفة باسم MLS، الأجهزة على تجنّب التعديل غير المصرّح به من التعليمات البرمجية التي تعمل بامتيازات عالية. ومع ذلك، لم يجرِ بعد نشر مقاربات MLS على نطاق واسع بسبب اعتبارها باهظة التّكلفة في بعض الحالات وغير متوافقة مع برمجيات انترنت الأشياء الأخرى، بينما تلجأ مقاربات أخرى لحماية السلامة إلى استخدام قيم التهشير التي تُخزَّن خارجياً لضمان عدم مهاجمتها. كما جرى اقتراح حلول عتادية لأغراض السلامة، مثل استخدام الحل القائم على التحدي (challenge-based solution) باستخدام مفاتيح متناظرة أو غير متناظرة تعرف باسم TPM. تحتاج أجهزة انترنت الأشياء إلى سلامة العملية (Process integrity) أيضاً، والتي تعتمد على سلامة الجهاز، الاتصالات، وتنجيز الخوارزمية، حيث أن البيانات المعالَجة بشكل سليم مطلوبة بشكل كبير لتحقيق معالجة البيانات للخدمات الأعلى ولترابط البيانات. تعتمد سلامة البرمجيات غالباً على العزل الفيزيائي للأجزاء البرمجية الحساسة والبيانات الحساسة عن باقي المكونات الأخرى الأقل ارتباطاً، ويمكن فرض ذلك فيزيائياً. أما بالنسبة للتجهيزات المحدودة الموارد من حيث المعالجة، الطاقة وعمر البطارية، فتوجد حلول كثيرة [14] ومنها: SMART، SPM، SANCUS وTrustlite، ومع ذلك، يمكن للهجمات القائمة على العتاد الصلب (hardware-based) مثل fault attacks أن تهدّد السلامة إن لم يتمتع النظام بالحماية الكافية مثل حساسات perturbation. يمنع التحقق من سلامة تكوين البرمجيات (Software Configuration)، والذي يسمى مصادقة أي attestation، التعديلات الضارة وعادةّ ما يجري تنفيذها من خلال أجهزة آمنة، لكن أجهزة انترنت الأشياء مجبورة على الاعتماد على برمجيات مصادقة قائمة على افتراضات قوية يصعُب تحقيقها في المجال العملي. لذا، قد تستخدم الأجهزة المدمجة ذات النهايات المنخفضة (low-end) ما يسمى بِـ swarn attestation التي تتيح التحقق من سلامة البرمجيات بشكل جماعي من

أجهزة متعددة أو provers. لا تحاول مخططات المصادقة المستخدَمة في انترنت الأشياء إثبات هوية الكائن فحسب، بل تحاول أيضاً ضمان سلامتها، حيث توفر المصادقة من خلال إدارة الهوية IdM التحكمَ في الموارد وتساعد على تقديم تدقيق الحسابات وإدارتها والتحكم في الوصول أيضاً. غير أن تنجيز إدارة الهوية يواجه بعض التحديات عند نشره في بنية تحتية لإنترنت الأشياء مثل قضايا قابلية التوسع، القدرة والإدارة. نستنتج أن الإجراءات والمخططات الموحدة والمَعيرة مهمة لضمان السلامة والجودة أيضاً، حيث يسمح إجراء مشترك لتطوير عمليات المعالجة بتلبية احتياجات موثوقية البيانات وقابلية التتبع، كما أن التعاون المكثّف بين مختلف مؤسسات انترنت الأشياء أمر ضروري جداً.

- التوافرية: تحتاج شبكات المعلومات المعتادة إلى ضمان تحديد الهوية، السرية، السلامة وعدم الإنكار (الفقرة 4.1-)، لكن شبكات انترنت الأشياء وخصوصاً المستخدَمة في مجالات حساسة للاقتصاد الوطني تحتاج أيضاً إلى توفير اهتمام خاص للتوافرية والاعتمادية (dependability). يُعتبَر توفّر الجهاز [15] العامل الأكثر أهمية، حيث ترتبط متطلبات توفر انترنت الأشياء ارتباطاً كبيراً بمتطلبات الوثوقية. لذا، تحتاج أنظمة انترنت الأشياء إلى مرونة كافية للحفاظ على التوافرية في المستويات المطلوبة، كما تحتاج إلى ضمان مستوى معين من الأداء الذي تطلبه تطبيقاتها. تعتبر بعض الدراسات [2] أن توافرية شبكات انترنت الأشياء يجب أن تجري في الأجهزة والبرمجيات معاً للتمكن من التعامل مع متطلبات المستخدمين، حيث تشير توافرية البرمجيات إلى قدرة تطبيقات انترنت الأشياء على توفير الخدمات للجميع في أماكن مختلفة بوقت واحد، بينما تشير توافرية الأجهزة إلى وجود أجهزة كافية في أي وقت لتحقيق وظائف وبروتوكولات انترنت الأشياء. قد تواجه تجهيزات انترنت الأشياء المحدودة الموارد هجماتٍ مثل DoS الذي يعتبر من أخطر الهجمات التي تهدد التوافرية وتعيق الخدمات المقدَّمة، والتي يجب معالجتها، فهي تعيق الاتصال بين الأجهزة وتمنعها من الوصول إلى موارد الشبكة، ولا تؤثر فقط على الموارد التقليدية مثل مزودات الخدمة وعرض الحزمة الترددية فحسب، وإنما تؤثر أيضاً على البيانات المجمَّعة لا سلكياً من عقد انترنت الأشياء. يمكن تنفيذ تلك الهجمات عن بعد باستخدام أوامر بسيطة بالتعاون مع أدوات أكثر تطوراً قد تسمح بتنفيذ هجمات DDoS أيضاً، التي تعتبر من أكثر الهجمات خطورةً على أنظمة انترنت الأشياء التي تتكون من عقد تشكّل نقطة ضعف من وجهة نظر طبقة الشبكة. تتدرّج هجمات DoS ابتداءً من أبسطها وهي هجمات التشويش (jamming) إلى أعقدها وهي هجمات elaborated DDoS، تأتي خطورة تلك الهجمات أيضاً من كونها تتسبّب في خسارة الطاقة وتبديدها، وهو أمر بالغ الأهمية للأجهزة محدودة الموارد. كما يُعتبر التخريب المادي "للأشياء" أحد أنواع هجمات DoS التي يمارسها مهاجمون محدودوا الخبرة لإعاقة خدمات انترنت الأشياء عن طريق تخريب تجهيزاتها. لاتزال بروتوكولات الاتصال المعيارية الحالية الخاصة بـ IETF مثل بروتوكول CoAP فاشلة في توفير الحلول، وبالتالي تعزيز توافرية شبكة انترت الأشياء، لكن بما أن هجوم DDoS هو

عبارة عن مجموعة متعاونة من هجمات DoS. لذا، يمكن اقتراح بنية SOA لإنترنت الأشياء كاستراتيجية لمنع هجوم DDoS. بينما تعتمد الحلول التقليدية لمنع تلك الهجمات على أخذ عينات كثيفة لحركة تدفق البيانات في الشبكة، أو على استخدام أنظمة IDS التي تساعد في الاكتشاف المبكر لهجمات DoS قبل تعطيل العمليات الطبيعية للشبكة وذلك في شبكات LoWPAN6. بينما اقترحت بعض الدراسات [16] تطبيق هيكليات موزعة بدلاً من المركزية التي تقوم بتحسين خصائص التوافرية من حيث زمن تشغل الخدمة والتخلص من نقاط الفشل الفردية، والعمل على إيجاد آليات للتعافي بعد حدوث هجوم DoS.

- الخصوصية: أظهر النمو الكبير في انترنت الأشياء خلال السنوات الأخيرة العديدَ من المخاوف المتعلقة بالخصوصية، تزداد تلك المخاوف مع ازدياد حجم بيانات المستخدمين المنتشرة على الشبكة وبين عقد مازالت لا تحقق الضمانات المطلوبة، وتزايدت متطلبات المستخدمين في حماية بياناتهم الشخصية المرتبطة بحركاتهم وعاداتهم وتفاعلاتهم. كما يمكن أن يؤثر التوفير الخاطئ لسرية البيانات وسلامتها على خصوصية المستخدم حيث يمكن للأطراف الخبيثة الوصول إلى البيانات الحساسة دون أي تخويل أو موافقة، مما يضرّ بإمكانية اعتماد تقنيات انترنت الأشياء على نطاق واسع. قامت بعض المرجعيات [17] بالتمييز بين القضايا والتحديات التي تحتاج أنظمة انترنت الأشياء إلى معالجتها لمنع انتهاك الخصوصية، حيث تضمنت الدراسة سلوكاً ذاتي الإدراك (self-aware) للأجهزة المتصلة، سلامة البيانات، المصادقة، تقنيات التعمية الفعالة، الحوسبة السحابية الآمنة، ملكية البيانات، الحوكَمة، وتنفيذ السياسات والإدارة. يمكن أيضاً توفير الخصوصية استناداً إلى التصميم (Privacy by Design) من خلال امتلاك المستخدمين للأدوات اللازمة للتحكم الديناميكي في البيانات التي يجري جمعها، تخزينها ومشاركتها، عن طريق ربط طلب المستخدم وتقييمه مع السياسات الحالية من أجل اتخاذ قرار بشأن منح إذن الوصول إلى البيانات أم لا. يمكن أن تمثّل الشفافية حلاً للخصوصية لأنها تتيح للمستخدمين معرفة الأطراف التي تدير وتستخدم البيانات التي يجري جمعها بواسطة أجهزة انترنت الأشياء. تقترح بعض الدراسات [18] أن تكون إدارة البيانات أحد حلول الخصوصية من خلال تنفيذ سياسات متباينة وأدوات فرض للسياسة، كما تناقش ضرورة توصيف البيانات، الملكية، مدى الوصول (الحد الأدنى والأعلى من البيانات التي يجب قراءتها)، وقابلية إخفاء الهوية. يجدر الذكر هنا أن الحلول التقنية وحدها ليست كافية لمعالجة قضايا الخصوصية الحالية، بل يجب النظر أيضاً في الجوانب الاقتصادية والأخلاقية والاجتماعية لبيئة انترنت الأشياء، وتنقيح تشريعات الخصوصية الحالية على المستوى الخاص والحكومي إضافةً إلى تحسين وعي المستخدمين بكيفيّة قيام الأجهزة القائمة على حساسات بجمع وتخزين ومشاركة معلوماتهم، وهذا ليس بالأمر السهل حيث يصعب إعادة تصنيف وتمييز معلومات التعريف الشخصية من معلومات التعريف القانونية التي يمكن حمايتها عن طريق القانون مما يشكّل تحدياً جديداً لأنظمة انترنت الأشياء. ويبقى التساؤل فيما إن كان ينبغي تغطية تشريعات خصوصية انترنت الأشياء من

قبل هيئات حكومية أو هيئات تنظيم ذاتي (وهو الاتجاه الحالي)، لكن تبقى التشريعات الحكومية قابلة للتطبيق محلياً فقط عندما تتجاوز طبيعة بيانات انترنت الأشياء الحدود، ومع ذلك فقد أوصت بعض الكيانات الحكومية، مثل مفوضية الاتصالات الفيدرالية الأمريكية FCC، بنشر شبكات الحساسات والتعاون من قبل الجهات المعنية في المجتمع المدني لخلق إطار الخصوصية الذي يعمل على مستويات مختلفة [19].

6.1- التّحدّيات والمشاكل

أثار إدخال تكنولوجيا انترنت الأشياء بعض الاهتمامات الأمنية الهامة نظراً لارتباط تلك التكنولوجيا بالعالم الحقيقي، وبسبب احتمال العرضة لاختراق الأمن والسلامة في حال تبنّيها، فيمكن مثلاً للخصم أن يستغل ثغرة معينة في الهاتف الذكي ليستطيع الوصول إلى المنزل الذكي للضحية. كما أثار الانتشار المتزايد للحساسات المحيطة بالبشر، والتي تقوم بجمع وتبادل المعطيات، تهديداً كبيراً لخصوصية المستخدمين، حيث يزداد إدراك أولئك المستخدمين لأهمية حماية خصوصيتهم، كما يزداد قلقهم بشأن جمع بياناتهم وانتشارها، فأصبحوا يطالبون الشركات المصنعة لتجهيزات انترنت الأشياء بإيضاح سياساتهم وأساليبهم في حماية الخصوصية، إضافةً إلى المطالبة بتحديد الحاجة إلى الانفتاح فيما يخص جمع البيانات وأمنها.

ليست تلك المخاطر الأمنية مجرد إدراك من قبل المستخدمين، وإنما هي موجودة في العالم الحقيقي وفي الكثير من الأجهزة الذكية الحالية، وهذا ما أثبتته الكثير من الدراسات التي أجريت لتقدير مدى جدية وخطورة تلك المخاطر حيث تبيّن أن بعضها يفتقر للمصادقة والتخويل وأخرى تفتقر لتعمية طبقة النقل. يُعتبَر أمن الشبكات عنصراً أساسياً في تحقيق أمن انترنت الأشياء، لذا لابد من استخدام تعمية مناسبة خفيفة بما يتناسب مع إمكانيات الأجهزة ولكن قوية بما فيه الكفاية إضافةً إلى استخدام آليات التحقق والتحكم في الوصول المناسبة.

يجري الاعتراف بالحاجة إلى الخصوصية من قبل المشرّعين، وينتج ذلك على سبيل المثال في العديد من المبادئ والتوصيات المعدّلة من قبل الاتحاد الاوروبي، ومع ذلك، هناك حاجة إلى إطار عالمي ومبادئ قانونية عامة تعتمدها صناعة انترنت الأشياء بأكملها، إضافةً إلى تطوير التقنيات اللازمة لفرض تلك القوانين. هناك قضية رئيسية أخرى لا تقل أهمية عن تحديات الأمن والخصوصية، تتمثّل في التوافق والتنسيق بين المجموعات الواسعة من الأجهزة، البروتوكولات والخدمات، توجد جهود توحيد معيارية مختلفة لكن العديد من الأجهزة لاتزال تنفرد ببروتكولها الخاص على مستوى طبقة التطبيق للتحكم بها، لذا لابد من ضمان التوحيد الحقيقي على كامل الطبقات لتحقيق التكامل الفعلي. تتعلق مجموعة أخرى من القضايا المعلقة بالشبكات، وخصوصاً فيما يتعلق بعنونة وتحديد هوية كيانات انترنت الأشياء ودعم حركتها (Mobility). لذا، فإن اختيار البروتوكولات التي تناسب احتياجات انترنت الأشياء، مثل بروتوكول طبقة النقل الجديدة مهم جداً وخصوصاً لنمذجة تدفق البيانات وجودة الخدمة (QoS).

نحتاج أيضاً لمزيد من الأبحاث حول استهلاك وتوفير الطاقة للتجهيزات، وهذا أحد أهم العوامل التي تسمح بنشر الحساسات في البيئات المرنة. قمنا في الفقرة السابقة (5.1-) بعرض التحدّيات الأمنية لأنظمة IoT من حيث المتطلبات الأمنية، سنقوم فيما يلي بمناقشة القضايا المحيطة بتلك الأنظمة من وجهة نظر العتاد الصلب (الفقرة 1.6.1-)، ثم سنناقش بعض القضايا الأمنية أيضاً، لكن بتصنيف آخر غير المتطلبات الأمنية وهو من وجهة نظر بنية وهيكلية انترنت الأشياء (الفقرة 2.6.1-).

1.6.1- محدوديّة تجهيزات انترنت الأشياء

من الصعب تطبيق الحلول الأمنية التقليدية على تجهيزات انترنت الأشياء [20]، وذلك بسبب الطبيعة الخاصة لتلك التجهيزات من حيث عدم التجانس، إضافةً إلى القيود على الموارد كالبطارية والقدرة الحسابية:

1.1.6.1- عمر البطّاريّة

تتواجد بعض تجهيزات انترنت الأشياء في بيئات بعيدة عن التيار الكهربائي حيث تنقص إمكانية شحنها وتزويدها بالطاقة، مما يجعلها تمتلك طلقة محدودة للقيام بالأعمال المخصصة لها. لذا، فإن الحلول الأمنية المعقدة ستستنزف طاقتها على حساب قيامها بأعمالها الأساسية. طرحت الأدبيات ثلاثة مقاربات متباينة لمعالجة هذه المشكلة:

1. تقليص المتطلبات الأمنية على الجهاز، وهذا غير محبذ خصوصاً في حالة التعامل مع بيانات حساسة.
2. زيادة سعة البطارية، لكن معظم تجهيزات انترنت الأشياء مصممة لتكون صغيرة وخفيفة الوزن، ولا يوجد مكان زائد لوضع بطارية أكبر.
3. الحصول على الطاقة من مصادر طبيعية (الضوء، الحرارة، الرياح، الاهتزاز، ...)، لكن هذه المقاربة تحتاج إلى تطوير الهاردوير ويزيد التكلفة المالية.

2.1.6.1- محدوديّة القدرة الحسابية

ذكرت المقالة [20] أن طرق التعمية التقليدية غير قابلة للتطبيق في أنظمة انترنت الأشياء، وذلك بسبب محدودية الذاكرة التي تمنعها من تحقيق متطلبات التخزين والمعالجة لخوارزميات التعمية المتقدمة. لذا، اقترح المؤلفون إعادة استخدام التوابع (functions) الموجودة لدعم تقنيات الحماية للتجهيزات المحدودة الموارد، كاستخدام التحقق والمصادقة على مستوى الطبقة الفيزيائية من خلال تطبيق آليات معالجة الإشارة في طرف الاستقبال للتحقق فيما إذا كان الإرسال قد جرى من المرسِل المتوقع ومن موقعه المتوقع. أو يمكن استخدام صفات تماثلية مميّزة للمرسل لترميز (encoding) المعلومات التماثلية، علماً أنه لا يمكن التحكم بهذه الفروق البسيطة التماثلية أثناء التصنيع أي يمكن اعتبارها كمفتاح وحيد، تستهلك هذه الطريقة من المصادقة طاقة قليلة شبه معدومة لأنها تستفيد من الإشارات الراديوية.

بينما قدّم المؤلفون في [21] خوارزمية Encrypted Query Processing لأنظمة انترنت الأشياء، التي تسمح بالتخزين الآمن على السحابة لبيانات انترنت الأشياء المعمّاة، وتقدّم آليات استعلام فعالة عن قواعد المعطيات عبر البيانات المعمّاة. كما جرى استخدام خوارزميات تعمية خفيفة بدلاً من additive holomorphic encryption، واستخدام التعمية الحافظة للترتيب (Orderpreserving) مع خوارزمية "ElGamal"، حيث أجروا بعض التّعديلات لتتناسب مع الإمكانات الحسابية المحدودة لإنترنت الأشياء. استبدلت بنية النظام المطروح اتصالات تطبيق الوب بنظام End-to-End الذي يخزن البيانات المعمّاة من الأجهزة الشخصية على السحابة، حيث تجري عمليات التعمية وفك التعمية في طرف الزبون (client side). ستتواجد المفاتيح في الجهاز الشخصي فقط، مما يلغي الحاجة لاستخدام وكيل (Proxy) موثوق للوصول إلى جميع المفاتيح السرية، وتتضمن بنية النظام ثلاثة أجزاء رئيسية هي: تجهيزات انترنت الأشياء، المستخدمين والسحابة. يمكن تخزين بيانات التطبيق في السحابة عن طريق تحميلها مباشرةً بواسطة الجهاز الذكي أو عبر بوابة (Gateway) مثل جهاز قابل للارتداء. تناول الباحثون في هذا البحث فقط بعض أنظمة التعمية التي تدعم الاستعلامات الأكثر استخداماً في معالجة بيانات انترنت الأشياء، لكن، يمكن توسيع التصميم لتغطية المزيد من الأنظمة. أظهرت نتائج التجريب تحسناً في أداء الزمن مقارنةً بالأنظمة الحالية.

اقترحت الدراسة [22] نهجاً لتقليص التأخير الزمني في تجهيزات انترنت الأشياء عند إجراء استعلام على البيانات المعمّاة من خلال تطبيق تقنية إخفاء التأخير الزمني (Latency Hiding)، التي تعتمد على تقسيم نتائج الاستعلام للبيانات كبيرة الحجم إلى مجموعات بيانات صغيرة الحجم، مما يسمح بإجراء العمليات الحسابية على مجموعة من البيانات أثناء جلب ما تبقى من البيانات المعمّاة. لتحديد حجم البيانات المناسب المراد طلبه في كل تكرار لتقليل التأخير، اقترحت الدراسة خوارزمية تبدأ بحجم بيانات أولي، ثم تقوم بتعديل الحجم لتقليل الفجوة بين العمليات الحسابية وعمليات الاتصال في كل تكرار. يجري تنجيز الخوارزمية بنمطين: يبدأ الأول بحجم يمثّل جزءاً صغيراً من حجم الاستعلام الكبير، بينما يبدأ النمط الثاني بحجم ثابت. أثبتت التجارب أن النموذج المقترح يتفوق على الحلول الحالية من حيث زمن التأخير المرافق للاستعلام عن البيانات ذات الحجم الكبير.

بينما اقترحت الدراسة [23] نموذج تعمية خفيف للمنازل الذكية يعتمد على التعمية القائمة على الهوية (stateful IBE)، والذي تكون فيه المفاتيح العمومية مجرد سلاسل محارف من الهوية دون الحاجة إلى شهادة رقمية، تعرف هذه الطريقة باسم PMO's stateful IBE scheme نسبةً إلى Phong، Matsuka، وَ Ogata، وهي مزيج من IBE ونظام Diffie-Hellman. قامت الدراسة البحثية بتقسيم عملية التعمية إلى تعمية المفتاح وتعمية البيانات وذلك من أجل إضافة المزيد من الفعالية على النموذج المقترَح وتقليل كلفة الاتصال، مع التركيز على تعمية البيانات لأن حجم النص المعمى الناتج عن تعمية المفتاح أكبر من ذلك الناتج عن تعمية البيانات، وقد أدى ذلك التقسيم إلى وجود خوارزميتين جزئيتين هما KEYEncrypt لتعمية مفتاح الجلسة وDATAEncrypt لتعمية البيانات، حيث يجري بشكل منفصل إرسال النص المعمّى الناتج عن تلك الخوارزميات الفرعية بطريقة تضمن إرسال ناتج الخوارزمية الثانية

(تعمية البيانات) عدّة مرات دون إرفاق ناتج الخوارزمية الأولى (تعمية المفتاح). أظهرت نتائج التقييم أن النموذج المقترَح آمن ضد هجمات النص الواضح (Plaintext attacks)، كما أظهر تحليل الأداء أن النموذج يتفوق على نظام IBE العادي من حيث تسريع عمليات التعمية وتقليل ما يقارب ثلث الحمل الزائد على الاتصال.

2.6.1- التّحدّيات والقضايا الأمنية

تشمل أنظمة انترنت الأشياء مجموعة واسعة من التجهيزات والمعدّات بدءاً من رقائق المعالجة الصغيرة المدمجة إلى الخوادم الكبيرة. لذا، لابد من تصنيف ومعالجة مشكلات وقضايا الأمن على مستويات مختلفة، بعد أن قمنا بتصنيفها من وجهة نظر المتطلبات الأمنية (الفقرة 5.1–). يمكننا تصنيف التهديدات الأمنية فيما يتعلق بهيكلية وبنية نموذج انترنت الأشياء كالتالي [24]:

- القضايا الأمنية منخفضة المستوى.
- القضايا الأمنية متوسطة المستوى.
- القضايا الأمنية عالية المستوى.

1.2.6.1- القضايا منخفضة المستوى:

يتعلق هذا المستوى بمشكلات الأمن في الطبقتين الفيزيائية ونقل المعطيات وعلى مستوى الأجهزة أيضاً كالتالي:

- خصوم التشويش Jamming Adversaries: تستهدف هجمات التشويش على الأجهزة اللاسلكية في انترنت الأشياء استنزافَ الشبكات عن طريق إصدار إشارات راديوية دون اتباع بروتوكول محدّد، مما يسبب تداخلاً يؤثر على وظائف الشبكة وعلى عمليات إرسال واستقبال البيانات من خلال العقد القانونية (الشرعية)، مما يؤدي إلى خلل أو سلوك غير متوقع للنظام.
- التهيئة الأولية غير الآمنة Insecure initialization: تضمن الآلية الآمنة لتهيئة وإعداد انترنت الأشياء في الطبقة الفيزيائية تشغيلاً مناسباً للنظام بأكمله دون انتهاك الخصوصية وتعطيل خدمات الشبكة، كما يجب تأمين اتصال الطبقة الفيزيائية لجعلها صعبة الوصول من خلال المستقبلات غير المخولة.
- هجمات Sybil وSpoofing منخفضة المستوى: تنجم هجمات Sybil في الشبكات اللاسلكية عن عقد Sybil الخبيثة التي تستخدم هويات مزيّفة تضرّ وظائف انترنت الأشياء، حيث يمكن لعقدة Sybil في الطبقة الفيزيائية أن تستخدم قيم عشوائية مزوّرة للعناوين الفيزيائية MAC وبالتالي تغيير هويتها لاستنفاذ موارد الشبكة ومنع العقد القانونية من استخدام تلك الموارد.

- الواجهة الفيزيائية غير الآمنة (Insecure physical interface): هناك عدّة عوامل فيزيائية تزيد من خطورة التهديدات على حسن سير العمل في أجهزة انترنت الأشياء، فقد يجري استغلال ضعف الأمن العتادي، النفاذ إلى البرمجيات من خلال الواجهات الفيزيائية (interfaces)، وأدوات الاختبار وتصحيح الأخطاء من أجل الهجوم على عقد الشبكة.
- هجوم الحرمان من النوم (Sleep deprivation): يجري هذا النوع من الهجوم في بيئة 6LoWPAN، ويستهدف أجهزة انترنت الأشياء محدودة الطاقة حيث يبقيها مستيقظة مما يؤدي إلى نفاذ البطارية.

2.2.6.1- القضايا متوسطة المستوى

تتعلق مشكلات الأمن على المستوى المتوسط بشكل أساسي بإدارة الاتصالات، التوجيه، والجلسة التي تجري في طبقتي الشبكة والنقل كما يلي:

- هجوم الاستنساخ أو التكرار الناجم عن التجزئة (Replay or Duplication attack due to fragmentation): يتصف معيار IEEE 802.15.4 بحجم أطره (frames) الصغير. لذا، لابد من تجزئة رزم (packets) الـ IPv6. قد يؤدي إعادة تجميع حقول الإطار المجزّأة في طبقة 6LoWPAN إلى استنفاذ الموارد، خنق ذاكرة الصّوان (Buffer) وإعادة إقلاع الأجهزة، مما يمكّن الأجزاء المكررة المرسلة من قبل العقد الضارة من التأثير على إعادة تجميع الإطار وبالتالي إعاقة معالجة الأطر الشرعية.
- اكتشاف الجوار غير الآمن Insecure neighbor discovery: تتطلب بنية انتشار انترنت الأشياء تعريف كل جهاز بشكل فريد على الشبكة، كما يجب أن يكون اتصال الرسالة المخصصة للتعريف آمناً لضمان وصول البيانات المرسَلة إلى الوجهة الصحيحة، تبدأ مرحلة اكتشاف الجوار قبل مرحلة الإرسال وتتضمن خطوات مختلفة منها اكتشاف الموجهات (routers) ثم اكتشاف العناوين الفيزيائية ARP. لذا، فإن استخدام رزم اكتشاف الجوار دون الاعتماد على آليات التحقق المناسبة قد يتسبب في الحرمان من الخدمة DoS.
- هجوم حجز الصِوان Buffer Reservation Attack: يجب على العقد المستقبِلة حجز ذاكرة buffer لإعادة تجميع الأطر الواردة، ويمكن للمهاجمين استغلال تلك النقطة وإرسال أطر غير مكتملة، مما يؤدي إلى الحرمان من الخدمة حيث تمتلئ ذاكرة الصوان ويجري بعدها تجاهل الرزم الشرعية لعدم توفّر مساحة تخزين كافية.

- هجوم بروتوكول التوجيه RPL: تعاني بروتوكولات توجيه IPv6 في الشبكات اللاسلكية ذات الاستهلاك المنخفض للطاقة والضياع في الأطر من هذا النوع من الهجوم من خلال العقد المخترَقة في الشبكة، مما يؤدي إلى استهلاك الموارد والبقاء عرضة للتنصت.
- Sinkhole and wormhole attacks: تستجيب عقدة المهاجم في هجمات sinkhole لطلبات التوجيه (Routing) مما يجعل الأطر تمر عبر عقدة المهاجم التي يمكن استخدامها فيما بعد لتنفيذ نشاط ضار على الشبكة، كما قد تتأثر وظائف 6LoWPAN بهجمات wormhole التي يجري فيها إنشاء نفق بين عقدة خبيثة وأخرى سليمة، مما يؤدي إلى وصول نسخة إلى العقدة الخبيثة من كل المعلومات الواردة إلى العقدة السليمة. تُحدِث تلك الهجمات تهديدات خطيرة مثل التنصت، انتهاك الخصوصية والحرمان من الخدمة.
- Sybil attacks on intermediate layers: بشكل مشابه لهجمات Sybil على الطبقات منخفضة المستوى، يمكن نشر عقد Sybil لإنقاص أداء الشبكة وانتهاك خصوصية البيانات، كما قد يؤدي اتصال تلك العقد بواسطة هويات مزيفة إلى إرسال رسائل spamming أو نشر برامج ضارة أو شن هجمات phishing.
- المصادقة والاتصال الآمن: يجب مصادقة الأجهزة والمستخدمين في انترنت الأشياء عبر أنظمة إدارة المفاتيح، يمكن لأي نقطة ضعف أمنية في طبقة الشبكة أو أي حمل زائد في تأمين الاتصال أن يعرّض الشبكة للكثير من نقاط الضعف. يجب مثلاً تقليص حجم DTLS إلى الحد الأدنى بسبب محدودية الموارد، وإيجاد آليات تعمية لحماية بيانات انترنت الأشياء آخذةً بعين الاعتبار الفعالية وندرة الموارد معاً.
- Transport level end-to-end security: يهدف هذا المستوى من الأمن إلى توفير آلية آمنة لاستلام البيانات المرسَلة بشكل موثوق إلى الوجهة الصحيحة، ويتطلب آليات مصادقة شاملة تضمن اتصالاً آمناً للرسائل بشكل معمّى دون انتهاك الخصوصية وبأقل حمل ممكن.
- تأسيس جلسة الاتصال واستئنافها: يمكن أن يؤدي اختطاف (hijacking) جلسة العمل في طبقة النقل برسائل مزيفة إلى الحرمان من الخدمة، حيث تقوم العقدة المهاجمة بانتحال شخصية العقدة الضحية لمواصلة الجلسة بين عقدتين.
- انتهاك الخصوصية في أنظمة IoT القائمة على السحابة: يمكن شنّ هجمات مختلفة على السحابة أو على انترنت الأشياء القائمة على الشبكات المتسامحة بالتأخير مما يسبب انتهاك خصوصية الهوية والموقع. كما يمكن لمزودات خدمة السحابة الخبيثة الوصول إلى المعلومات السرية المتبادلة في أنظمة انترنت الأشياء.

3.2.6.1- القضايا عالية المستوى

تتعلق مشكلات الأمن عالية المستوى بشكل أساسي بالتطبيقات المنفّذة على انترنت الأشياء كالتالي:

- CoAP Security with internet: تعاني أيضاً طبقة التطبيقات من الهجمات، يقوم بروتوكول CoAP بالنقل عبر الويب للأجهزة المقيّدة ويعتمد على بروتوكول DTLS لتوفير الأمن بين أطراف الاتصال (end-to-end) ، وتتّبع رسائل CoAP تنسيقاً محدداً في RFC-7252 ومعمّى لتأمين الاتصال، كما تتطلّب عمليات البث المتعدد multicast في بروتوكول CoAP آليات مصادقة وإدارة مفاتيح فعّالة.
- الواجهات غير الآمنة: تستخدَم الواجهات، ويب أو موبايل أو سحابة، لوصول المستخدمين إلى خدمات انترنت الأشياء، وهي عرضة لهجمات مختلفة قد تؤثر على خصوصية البيانات.
- Insecure software/firmware: تنجم العديد من نقاط الضعف في انترنت الأشياء عن البرمجيات (والبرمجيات الراسخة firmware) غير الآمنة. لذا، يجب اختبار الرمازات البرمجية التي تحوي لغات برمجة مثل XML، XSS، SQLi وJSON بعناية إضافةً إلى إجراء التحديثات الدورية للبرامج.
- Middleware security: يجب أن تكون برمجيات انترت الأشياء الخاصة بربط التطبيقات مع نظم التشغيل وقواعد المعطيات في بيئة غير متجانسة آمنةً بدرجة كافية لتوفير الخدمات، حيث يجري دمج واجهات وبيئات مختلفة تستخدم middleware لتحقيق اتصال آمن.

3.6.1- الحلول الأمنية

تستغل التهديداتُ الأمنية نقاطَ الضعف في مختلف مكونات انترنت الأشياء مثل التطبيقات، الواجهات، مكونات الشبكة، البرامج والأجهزة الموجودة على مستويات مختلفة، حيث يتفاعل المستخدمون في نموذج انترنت الأشياء مع تلك المكونات من خلال بروتوكولات يمكن تفكيكها أيضاً لاعتبارات أمنية خاصة بالمستخدمين. تعالِج التدابير المضادة للتهديدات الأمنية نقاط ضعف ذلك التفاعل في طبقات مختلفة للوصول إلى مستوى أمن محدد، كما أن تنوّع البروتوكولات المستخدمة في أنظمة انترنت الأشياء تزيد من تعقيد تلك التدابير الأمنية. سنقدم في هذا الجزء نظرة عامة للحلول الأمنية الرئيسية المقترحة في الأدبيات، مع مقارنات تحليلية من حيث التهديدات الأمنية، تداعياتها، الطبقات المتأثرة بها، المستويات الموافقة لها والحلول الأمنية المقترحة [24]:

1.3.6.1- الحلول الأمنية منخفضة المستوى

تتعلق هجمات التشويش في شبكات الحساسات اللاسلكية بالتداخل الناتج عن تصادم الرسائل أو إغراق قنوات الاتصال، يمكن اكتشاف هجمات التشويش من خلال قياس قوة الإشارة ليجري استخدامها فيما بعد لاستخراج

الإشارات المشابهة للضجيج، ثم يجري مقارنة تلك الإحصائيات مع قيم عتبات معرّفة مسبقاً لكشف الهجمات. كما يمكن اكتشاف هجمات التشويش من خلال حساب نسبة نجاح تسليم الرزمة، حيث تعمل الخوارزميات المقتَرحة عن طريق إجراء اختبارات التوافق على قوة الإشارة ومواقع العقد. يمكن أيضاً مواجهة هجمات التشويش من خلال عمليات التعمية وآليات تصحيح الأخطاء، عن طريق ترميز الأطر من خلال تقسيمها إلى كتل وحشو بتات الإطار المرمَّز. أو من خلال استراتيجيات تصفح القناة والانسحاب المكاني، حيث يتيح تصفّح القناة للأجهزة الشرعية تغيير تردد قناة الاتصال، بينما يسمح الانسحاب المكاني لتلك الأجهزة بتغيير موقعها أثناء الانتقال إلى الموقع المطلوب لمسافة معينة. اقترحت بعض الدراسات منصةً لتوفير اتصال آمن على مستوى الطبقة الفيزيائية [25]، يجري فيها اعتماد الحد الأدنى من البيانات بين العقد المرسلة والمستقبِلة لضمان عدم وجود التنصت، كما يجري استخدام طرق أخرى باستخدام ضجيج اصطناعي لتأمين الاتصال.

يمكن لعقدة Sybil خبيثة استخدام قيم MAC مختلفة للتنكّر كعقدة أخرى، مما قد يسبب استنزاف الموارد والحرمان من الوصول إلى العقد الشرعية في الشبكة، يمكن كشف تلك الهجمات من خلال قياس قوة الإشارة عن طريق استخدام عقد كاشفة لحساب موقع المرسل أثناء إرسال الرسالة، وبالتالي فإن أي رسالة أخرى من نفس موقع المرسل وبهوية مختلفة تدلّ على وجود هجوم Sybil، ولكن تلك الطريقة صالحة للتطبيق في الشبكات الثابتة. كما يمكن استخدام طرق تقدير القناة باستخدام عدد من المعرفات والمعاملات الأخرى للكشف عن عقد Sybil، أو استخدام استجابة القناة للتمييز بين المهاجمين والمستخدمين القانونيين. تحوي الأجهزة التي لا تتمتع بأمن فيزيائي مناسب واجهاتٍ خارجية توفر الوصول إلى البرامجيات والبرامج الراسخة، كما توفر أدوات مساعدة غير آمنة مثل أدوات الاختبار والتصحيح (Testing and Debugging). لذا، يقدم مشروع أمن تطبيق الويب المفتوح OWASP توصياتٍ لتحسين الأمن الفيزيائي للأجهزة في انترنت الأشياء [26]، مثل تجنب استخدام منافذ USBs الغير ضرورية التي تسمح بالوصول المباشر إلى الأجهزة والبرامج، وتعطيل أدوات الاختبار والتصحيح، واستخدام نماذج المنصة الموثوقة TPM لتحسين الأمن الفيزيائي. قدّمت إحدى الدراسات [27] منصة عمل لتخفيف هجمات الحرمان من النوم (Sleep Deprivation Attacks) في شبكات الحساسات اللاسلكية، تقوم المنصة المقترحة على مفهوم العنقدة (clustering) وكل عنقود مقسّم إلى عدة قطاعات، يجري فيها تقليل استهلاك الطاقة من خلال تجنب الاتصال لمسافات طويلة. تعمل تلك المنصة كـ IDS بنموذج خمس طبقات في شبكات الحساسات اللاسلكية، يحتوي منسّق الكتلة على نظام IDS موسّع يعمل مع عقد sink، وعقد leaders في الطبقات العليا من نموذج WSN، بينما تكون عقد followers الموجودة في الطبقات السفلى مزودة بـ IDS بسيط. يوضّح الجدول 1-3 أبرز القضايا الأمنية التي ذكرناها مع تأثيرها والطبقات المتأثرة بها مع الحلول المقترحة.

الجدول 1-3 القضاية الأمنية منخفضة المستوى وحلولها

القضية الأمنية	تأثيرها	الطبقات المتأثّرة	مستويات IoT	الحلول المقترَحة
خصوم التشويش	تعطيل الشبكة والحرمان من الخدمة	الطبقة الفيزيائية	منخفضة المستوى	– قياس قوة الإشارة – حساب معدّل تسليم الطرد – ترميز الطرود برمّازات تصحيح الأخطاء – تغيير الترددات والمواقع
التهيئة الأولية غير الآمنة	انتهاك الخصوصية والحرمان من الخدمة	الطبقة الفيزيائية	منخفضة المستوى	– تحديد معدلات نقل البيانات للعقد. – إدخال ضجيج زائف.
هجمات Sybil وSpoofing منخفضة المستوى	تعطيل الشبكة والحرمان من الخدمة	الطبقة الفيزيائية	منخفضة المستوى	– قياسات قوة الإشارة. – تقدير القناة.
الواجهات الفيزيائية غير الآمنة	انتهاك الخصوصية والحرمان من الخدمة	العتاد الصلب	منخفضة المستوى	– تجنب وصول العتاد المرن والبرمجيات الراسخة إلى USB. – استخدام نماذج المنصة الموثوقة القائمة على العتاد الصلب.

				- تجنّب أدوات الاختبار وأدوات تصحيح الأخطاء.
هجوم الحرمان من النوم	هدر الطاقة	طبقة الوصلة (Link)	منخفضة المستوى	استخدام نظام IDS متعدد الطبقات.

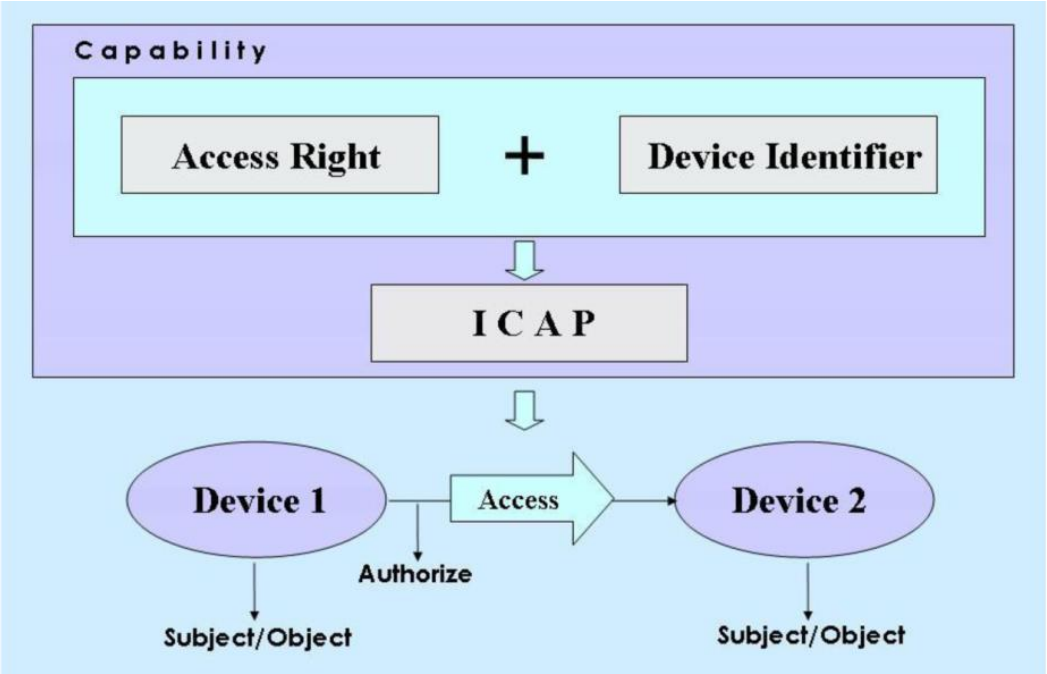
2.3.6.1- الحلول الأمنية متوسّطة المستوى

يجري التعامل مع هجمات التكرار (Replay) الناتجة عن تجزئة الرّزم في شبكات 6LoWPAN بإضافة حقول timestamp وnonce إلى الرّزم المجزَّأة، ثم يجري إضافة تلك الرزم إلى طبقة التكيّف (adaptation layer) الموافقة للرّزم المجزَّأة، وتعمل تلك الحقول المذكورة في الرزم أحادية وثنائية الاتجاه على التوالي [28]. تضمن قيمة timestamp القضاء على عمليات إعادة التوجيه والإعلانات الزائدة في الشبكة، بينما يضمن خيار nonce أن يجري الإعلان فقط في حالة الرد على طلب جديد. كما جرى اقتراح استراتيجية content-chaining التي تضمن ترتيب إرسال أجزاء رزم 6LoWPAN ويجري فيها إضافة محتويات كل جزء إلى سلسلة التهشير للتحقق من تلك الأجزاء. أما بالنسبة للاكتشاف الآمن للجوار، فقد جرى اقتراح منصات مع تطبيقاتها تضمن اكتشاف الجوار، المصادقة، توليد المفاتيح وتعمية البيانات بشكل آمن [29]، حيث يجري استخدام تعمية المنحنيات القطعية (ECC)، وتساعد التوقيعات الرقمية لـ ECC على تحديد هوية العقد أثناء مرحلة اكتشاف الجوار، كما يقترح النموذج استخدام أنظمة إدارة المفاتيح المتناظرة وغير المتناظرة بناءً على متطلبات التطبيق، ثم يجري توصيل البيانات المعمّاة لضمان الأمن من عقدة لعقدة. قدّمت بعض الدراسات [30] مقارباتٍ للتخفيف من هجوم حجز الصّوان (buffer reservation attack)، تعتمد تلك المقاربات على تقسيم الصّوان، مما يزيد من كلفة الهجوم لأنه يحتاج إلى إرسال كل الأطر المجزّأة في رشقاتٍ قصيرة، وتشارك كل العقد في احتساب النسبة المئوية لإكمال الرزمة وتسجيل سلوك إرسال أجزائها، ويمكن للعقدة عند التحميل الزائد تجاهل الرّزم ذات النسبة المئوية المنخفضة، أو التي فيها تغاير كبير في نمط إرسال الأجزاء. عملت دراسات أخرى على تخفيف هجمات الخصم على بروتوكول توجيه IPv6 الخاص بالشبكات ذات الاستهلاك المنخفض للطاقة والضياع في الرّزم RPL [31]، حيث اقترحت تلك الدراسات خدمةً أمنية للمصادقة على أرقام rank وversion الخاصة ببروتوكول RPL. حيث يعمل ذلك البروتوكول من خلال بناء ما يسمى بمخطط DAG مع عقدة جذر في كل بوابة (gateway)، ويجري تحديث قيمة الـ version عند كل بناء جديد لـ DODAG، بينما يستخدِم البروتوكول قيمةَ Rank للتعبير عن جودة التوجيه إلى عقدة sink الأخيرة، يمكن للعقدة المهاجِمة أن تنقص قيمة Rank الخاص بها من أجل القيام بعمليات التنصت. تستخدِم آلية الأمن المقترحة التي سُمّيَت بـ VeRA توابعَ

التهشير (SHA) وتوابع MAC (HMAC + Signature) وما إلى ذلك لمصادقة الرقمين المذكورين سابقاً. جرى اقتراح آلية للتعامل مع هجمات sinkhole في الشبكات ذات الاستهلاك المنخفض للطاقة والضياع في الرّزم (LLNs) [32]، تشمل تلك الآلية على عمليات المصادقة وfailover[2]، يجري فيها استخدام توابع تهشير وتوابع سلسلة تهشير للتحقق من رقم rank الموافق لرسالة DIO، التي يجري فيها بثّ قيمة التهشير لعدد عشوائي محدّد مسبقاً بواسطة عقدة الجذر، ثم تقوم العقد الصالحة بعملية تهشير إضافية قبل إعادة توجيه الرسالة، بينما تقوم العقد المصابة بتوجيه الرسالة كما هي، تقوم عقدة الجذر بعد حدوث التقارب (convergence) في شجرة التوجيه بإرسال القيمة العشوائية المعرّفة مسبقاً بغية التحقق من العقد الفردية، وبالتالي فإن أي عدم تطابق في أي عقدة يدل على قيمة غير صحيحة لـ rank الأب. تقوم تقنية parent failover بشكل مشابه بتزويد رسالة DIO بحقل خاص موقّع من العقدة الجذر ويمثّل العقد غير الجذرية التي لا تستطيع نقل 30% من بيانات الحساس في فترات زمنية محدّدة. لذا، يجري إدراج آباء تلك العقد في قوائم سوداء من أجل التواصل اللاحق. كما جرى طرح استراتيجيات أخرى [33] للتعامل مع هجمات sinkhole باستخدام مستويات ثقة مختلفة، يستخدم النموذج المطروح بروتوكول DSR لاكتشاف وتجنّب هجمات sinkhole وwormhole في الشبكات اللاسلكية، ويعتمد على مستويات الدقة والأمانة التي يجري حسابها عن طريق التحقق من الرّزم المعاد توجيهها من خلال بعض اختبارات السلامة. جرى بالمثل تصميم بروتوكول توجيه لشبكات ad hoc يشمل على خوارزمية قائمة على التعمية المتناظرة لتأمين العقد السليمة من العقد المخترَقة في الشبكة اللاسلكية. توجد طريقة أخرى للكشف عن هجمات wormhole في شبكات الحساسات اللاسلكية تعمل عن طريق بثّ المسافات المقدّرة بين الجيران، يجري بعدها تحليل تشوهات الشبكة للكشف عن wormholes واتصالات الجوار المشبوهة. كما جرى اقتراح مقاربة أخرى للكشف عن هجمات sinkhole وwormhole في شبكات الحساسات اللاسلكية الهرمية، حيث يجري فيها توزيع مكونات الشبكة في عناقيد يحوي كل منها على عقدة حساس عالي الطاقة يعمل على اكتشاف العقد المشبوهة في العنقود. تشكِّل هجمات Sybil تهديداً خطيراً للأنظمة الموزعة وأنظمة الند للند P2P بما في ذلك انترنت الأشياء، كما قد تؤثر على أنظمة الدفاع ضد العيوب البيزنطية مما يعيق البثّ الموثوق في الشبكة، يجري في الشبكات الاجتماعية إنشاء علاقات ثقة للحدّ من إنشاء هويات Sybil، كما تتيح الإجراءات المتّخذة باستخدام الرسوم البيانية الاجتماعية للعقد الشرعية باكتشاف عقد Sybil من خلال اجتياز الرسوم البيانية بمسارات عشوائية أو من خلال خوارزميات كشف المجتمع، ويجري بالمثل تحليل سلوك المستخدمين فيما يتعلق بالأنشطة على الشبكة، وبالتالي فإن المستخدمين ذوي النمط الثابت من الأنشطة هم مستخدمي Sybil، بينما يمكن بالنسبة لشبكات الأجهزة المحمولة الاحتفاظ بقوائم المستخدمين الموثوقين وغير الموثوقين للكشف عن عقد

[2] هي طريقة لحماية الأنظمة من الفشل، حيث يوجد نظام احتياطي بديل كنسخة عن الأساسي، وينزل إلى الخدمة أوتوماتيكياً عند فشل النظام الرئيسي.

Sybil. أما بالنسبة لتأمين طبقة الشبكة في IPv6 باستخدام طبقة التكيف في 6LoWPAN، فقد جرى في RFC 4302 طرح التنسيقات المضغوطة لترويسة المصادقة AH وطرح ESP. يجري استخدام ترويسة عنوان IPv6 بطول 8 بت وفقاً لمواصفات طبقة التكيف في 6LoWPAN لتعريف ترويسة الإرسال ونمط العناوين، كما يجري استخدام الترويسة المضغوطة في الاتصال بوضعين هما Transport وtunnel اعتماداً على تعمية payload، أوضحَ تقييم تقنيات التعمية المختلفة المطبقة لنموذج الأمن السابق أن خوارزمية SHA1 تتطلب وقتاً وطاقة أقل. جرى أيضاً اقتراح نموذج لتأمين طبقة الشبكة في 6LoWPAN من خلال دعم قيم نمط الإرسال الجديدة (dispatch) واستخدام القيم المحجوزة لبايت payload كما هو موضح في RFC 4944، حيث تعبّر البتّات الثلاثة الأولى من قيم نمط الإرسال عن ترويسة الأمن ونمط الاستخدام، بينما تعبّر البتّات الثلاثة المتبقية عن أنواع ترويسات عنونة 6LoWPAN، ويجري استخدام دليل معاملات الأمن SPI بطول 2 بايت لاستخراج المعلومات من إطار فيما يتعلق بخوارزميات التعمية والمفاتيح الواجب تطبيقها لمعالجة الإطار. كما جرى اقتراح بروتوكول [34] على عكس النهج السابق لتأمين انترنت الأشياء ضد هجمات الحرمان من الخدمة، الرجل في الوسط وهجمات التكرار replay، حيث من الممكن أن تؤثر هجمات الحرمان من الخدمة على موارد الأجهزة المقيدة، أو أن تقوم هجمات الرجل في الوسط إلى سرقة المفاتيح السرية من خلال التنصت وبالتالي سرقة الهوية ليجري استخدامها فيما بعد بهجمات التكرار والتأثير على تدفق البيانات في الشبكة. يقوم النموذج [34] المقترح المسمّى "التحكم في الوصول القائم على الصلاحيات ومصادقة الهوية IACAC" بإنشاء مفاتيح سرية باستخدام خوارزمية Diffie-Hellman القائمة على تعمية المنحنيات القطعية، وتجري مصادقة الأجهزة بشكل متبادل من خلال التعمية بمفاتيح سرية لضمان الاتصال والوصول، بينما يُطبَّق التحكم في الوصول القائم على الصلاحيات التي تمثّل بنية تحتوي على حقوق الوصول ومعرفات الأجهزة (الشكل 1-7)، ويجري فيها التحقق أولاً من الاتصالات بين جهازين، كما يجري فحص صلاحيات الجهاز على أداء الوظيفة المطلوبة قبل أن تتم العملية الفعلية.



الشكل 1-7 بنية الصلاحيات (**Capability**).

قدّمت بعض الدراسات طريقة للأمن من النهاية إلى النهاية (end-to-end) باستخدام مصادقة ثنائية الاتجاه من خلال تعمية المفتاح العام، وباستخدام مخدّم موثوق للتحكم بالوصول يُخزّن به حقوق الناشرين في الشبكة [35]، يجب أن تكون شهادة الناشر وسلطة الشهادة CA موجودة على موقع الناشر، وتجري المصادقة من خلال شرائح نموذج المنصة الموثوقة TPM باستخدام تعمية RSA، أو من خلال مفاتيح DTLS المشارَكة مسبقاً، ويبدأ الاتصال من النهاية إلى النهاية فقط بعد مصادقة المشتركين من خلال مخدّم التحكم بالوصول، يعمل النهج السابق مع متطلبات منخفضة من الطاقة والذاكرة. كما قدّمت دراساتٌ أخرى آليةً للمصادقة والتخويل باستخدام عدّة معاملات، تقوم بمصادقة كلمة المرور أثناء استخدام البطاقة الذكية، حيث يدعم بروتوكول المصادقة أربع عمليات رئيسية تتعلق بإنشاء المعاملات الأمنية، تخزين معلومات التسجيل في قواعد المعطيات، المصادقة وتعديل بيانات اعتماد المصادقة، كما تقترح الدراسة آلية مصادقة قائمة بذاتها يجري تطبيقها عند فقدان الاتصال بمخدّم المصادقة. قدّمت بعض الدراسات منصةً موزّعة للاتصال الآمن بين شبكات انترنت الأشياء، تسمح تلك المنصة بتكوين شبكة انترنت أشياء من موقع مركزي لحمايتها من مزودات الخدمة الخبيثة في السحابة، بينما تقوم بتسجيل رسائل التحكم في مواقع متعددة من أجل التحقق منها بواسطة بوابات مختلفة، يجري في تلك المنصة تقليل حجم رسائل السجل عن طريق حذف الرسائل القديمة بشكل مستمر، ثم يجري استخدام التحقق من رسائل السجل لكشف السلوك الضار وبالتالي حماية انترنت الأشياء القائمة على السحابة من تعديل الرسائل، حجزها، إدراجها وإعادة ترتيبها. قدّمت دراساتٌ أخرى آلية مصادقة مع إعادة توجيه آمن للرّزم بهدف الحفاظ على خصوصية الهوية والموقع لإنترنت الأشياء، حيث تستخدم

الخوارزمية المقترَحة تقابلاً (mapping) متجانساً متناظراً للشبكات المتسامحة مع التأخير الزمني والتي تفتقر إلى اتصال ثابت من النهاية إلى النهاية مما يتطلب تعاون العقد الوسيطة أثناء إرسال الرسائل. جرى أيضاً في مشروع SMARTIE [36] اقتراح منصة لتأمين مشاركة البيانات بين أجهزة انترنت الأشياء، تعرّف تلك المنصة آلية مصادقة للوصول إلى الخدمة إلى جانب مكتبات مختلفة لإدارة مفاتيح التعمية، يقدّم المشروع بروتوكول CoAP الآمن خفيف الوزن باستخدام ECC وذلك من أجل توفير قناة اتصال آمنة بين أجهزة انترنت الأشياء والسحابة، كما تتضمن المنصة خدمات قائمة على الموقع وmiddleware للحفاظ على الخصوصية اثناء مشاركة البيانات وللتّتبّع الآمن لمكونات انترنت الأشياء. كما جرى اقتراح استخدام TLS-PSK مع إتاحة الاتصال بين HTTP وCoAP لتوفير الأمن من النهاية إلى النهاية، يتطلب ذلك ترجمة الرسالة من طبقة DTLS وغيرها من البروتوكولات عالية المستوى. جرى بالمثل اقتراح توسعة DTLS لتأمين رسائل البث المتعدد (multicast)، ليصبح DTLS يتضمن PSK وnonce لدعم عملية التفاوض على مفاتيح الجلسة. أما بالنسبة للأمن على مستوى طبقة النقل، فقد جرى اقتراح آلية مصادقة مفوّضة باستخدام موجه الحافة (border router) في شبكات 6LoWPAN وهو 6LBR، حيث تمر جميع الرّزم من الموجه المذكور، فيقوم بعمليات حسابية لمصادقة المفتاح العمومي ويعيد توجيه الرّزم. وجرى استخدام مخدّم تحكم بالوصول لدعم المصادقة بين 6LBR والحساسات، واستخدام تعمية ECC لدعم الأمن على مستوى طبقة النقل، واستخدام مفاتيح تفاوض 6LBR والاتصال لخطوات المصادقة الأخرى بين كلا طرفي الاتصال لتأمينه من النهاية إلى النهاية، ينتج عن الحساب المفوض لموجه 6LBR أداءً أفضل للاتصال الآمن على الرغم من الحسابات الثقيلة التي تتطلّبها ECC. جرى اقتراح منصة أخرى تدعى BlinkToSCoAP لتأمين الأمن من النهاية إلى النهاية [37]، تتضمن المنصة تنجيزات خفيفة من CoAP، DTLS و6LoWPAN لتأمين انترنت الأشياء، وتعتمد فيها تعمية DTLS على خوارزميات AES بطول مفتاح 128 بت وSHA بطول 26 بت، أظهرت تلك المنصة نتائج جيدة للعمل مع الأجهزة مقيدة الموارد بمتطلبات صغيرة من ذاكرة الوصول العشوائي وذاكرة الفلاش واستهلاك الطاقة. يقدّم مشروع RERUM منصةً لضمان أمن وخصوصية تطبيقات انترنت الأشياء في المدن الذكية [38]، من خلال تكييف المقاربات القائمة على مصادقة وسلامة البيانات وذلك لتطوير تطبيقات جديرة بالثقة، يتضمن المشروع استخدام آليات جديدة للتحكم بالوصول للأنظمة القابلة للتحويل ديناميكياً مع استخدام المصادقة من النهاية إلى النهاية ومن عقدة إلى عقدة لضمان اتصال آمن بين مكونات انترنت الأشياء، كما يهدف المشروع إلى ضمان الخصوصية من خلال آليات التوقيع الرقمي وتقنيات تحسّس الضغط. جرى أيضاً تنجيز منصة لتجربة بروتوكولات الأمان في بنية تحتية قائمة على انترنت الأشياء في مشروع ARMOUR [39]، الذي يهدف إلى التحقق من الثقة والأمن في السيناريوهات القائمة على انترنت الأشياء كالمدن الذكية والرعاية الصحية، حيث تعرّف تلك التجربة بنية الأمن، تؤسّس اختبارات، تنفّذ التجارب، وتنتِج ملصقات الشهادات، يمكن استخدام تلك التجارب لضمان التوصيل من النهاية إلى النهاية وضمان متطلبات الأمن الخاصة بالطبقة. يوفّر أيضاً مشروع BUTLER دعماً لأنظمة معلومات

context-aware لأنظمة انترنت الأشياء بما في ذلك المنازل الذكية والتسوق الذكي والرعاية الصحية والمدن الذكية، تتيح الخدمات المنفّذة في المشروع اتصالاتٍ موثوقة لمكونات انترنت الأشياء باستخدام context information، كما يتضمن المشروع بروتوكولات تعمية خفيفة الوزن بهدف تحسين سرية وسلامة البيانات. جرى اقتراح تقنيات عديدة لضغط الترويسة لتوفير الأمن من النهاية إلى النهاية في طبقة النقل، منها من لجأ إلى ضغط ترويسات تسجيل DTLS (record) والمصافحة (Handshake) مع رسائل مصافحة مختلفة لتتناسب مع حجم وحدة الإرسال الأعظمية MTU في شبكات 6LoWPAN، يرمّز النهج المقترح بتّات ترويسة الترميز المركب من التسجيل والمصافحة وكذلك الترميز الفردي لترويسة السجل بعد اكتمال المصافحة. ومنها من قدّم نسخة محسّنة من DTLS تتضمن ضغط الترويسة لتأمين انترنت الأشياء، تقوم تلك النسخة في ضغط الترويسة التالية NHC القائمة على بروتوكول UDP باستخدام أول 6 بتّات في ترويسة DTLS لتحديد الترويسات المضغوطة، بينما تُستَخدَم البتّات الثلاثة المتبقية لتمثيل المجموع الاختباري (checksum) والمنافذ (ports)، وبشكل مشابه بالنسبة لترويسات التسجيل والمصافحة التي يبلغ حجمها 13 بايت و12 بايت، فتقوم الاستراتيجية المقترحة بضغط الترويسات بحجم 5 بايت و3 بايت على التوالي، أما بالنسبة لـ CoAP، فيقلّل التحسين في DTLS، الذي يتضمن ضغط الترويسة، من الحمل الإضافي لـ DTLS، مما يحسّن استهلاك الطاقة وزمن الاستجابة. اقترحت دراساتٌ أخرى [40] تنجيزاً خفيفاً لتبادل مفاتيح الانترنت IKE بهدف تحسين إدارة المفاتيح في 6LoWPAN، حيث يجري استخدام بروتوكول IKE من قبل IPsec لإدارة المفاتيح، لكن تلك المقاربة تعتبر غير مناسبة للأجهزة مقيدة الموارد، مما دعا إلى اقتراح إصدار مضغوط من IKEv2 باستخدام التنسيق المضغوط لبروتوكول UDP الذي يمثّل ترويسة IKE، حيث يجري ضغط حقول مختلفة في تلك الترويسة أثناء استخدام آلية ترميز NHC، كما تقترح تلك المقاربة استخدام حقل protocol ID في حمولة إطار SA الخاص بـ IKEv2 لأمن طبقة تبادل المعطيات في معيار IEEE 802.15.4. قدّمت دراسات أخرى [41] آلية مصادقة متبادلة (mutual authentication) لتأمين إدارة الجلسة باستخدام التعمية المتناظرة، يجري فيها بدايةً اختيار رقم عشوائي، ثم تقوم بالتعمية لإنشاء مفتاح جلسة يجري استخدامه فيما بعد لتعمية رقم عشوائي آخر لاستخدامه من أجل المصادقة، يمكن توليد مفتاح جديد لكل جلسة دون الحاجة إلى تكرار المعاملات، كما تقترح الدراسة طريقة أخرى للتعمية باستخدام توابع التهشير في الأجهزة محدودة الموارد التي تدعم التهشير، وهذه الطريقة ذات حمولة خفيفة بالنسبة للعمليات الحسابية. جرى طرح مخطط آخر باسم Octopus للمصادقة المتبادلة في البيئات القائمة على الحوسبة الضبابية والتي تحوي أجهزة مقيدة الموارد [42]، يتطلب ذلك المخطط الحصول على مفتاح سري طويل الأمد يستَخدَم للمصادقة مع كل مخدّمات الضباب. كما جرى تكيّف بروتوكول HIP DEX لتحسين أمن انترنت الأشياء من خلال دمج تقنية فعّالة لاستئناف الجلسة يجري فيها تقليل الحمل في استخدام العمليات القائمة على المفتاح العام، يؤدي استئناف الجلسة إلى قيام الأقران (peers) بعمليات ثقيلة أثناء تهيئتها، ويجري تخزين حالة الجلسة لسهولة استئنافها فيما بعد مع إعادة المصادقة، يمكن أيضاً دمج التفاوض المطلوب لاستئناف الجلسة في

DTLS وIKEv2. يظهِر الجدول 1-4 القضايا الأمنية متوسطة المستوى ومجال تأثيرها إضافةً إلى الحلول الأمنية المقترَحة.

الجدول 1-4 القضايا الأمنية متوسّطة المستوى وحلولها

القضية الأمنية	تأثيرها	الطبقات المتأثّرة	مستويات IoT	الحلول المقترحة
هجوم التكرار بسبب التجزئة (fragmentation)	تعطيل الشبكة والحرمان من الخدمة	6LoWPAN, adaptation, and network layers	متوسطة المستوى	– إدخال خيارات البصمة الزمنية وnonce. – التحقق من صحة التجزئة من خلال سلاسل التهشير.
اكتشاف الجوار غير الآمن	IP Spoofing	طبقة الشبكة	متوسطة المستوى	المصادقة باستخدام التواقيع الرقمية القائمة على ECC.
هجوم حجز الصِوان	Blocking of reassembly buffer	6LoWPAN, adaptation, and network layers	متوسطة المستوى	تقسيم الصِّوان يتطلّب الإرسال الكامل للأجزاء (fragments).
هجوم RPL Routing	التنصت، وجوم الرجل في الوسط	طبقة الشبكة IPv6.	متوسطة المستوى	– المصادقة القائمة على التوقيع الرقمي والتهشير. – مراقبة سلوك العقد.

هجوما Sinkhole وWormhole.	الحرمان من الخدمة	طبقة الشبكة	متوسطة المستوى	- التحقق من "Rank" من خلال سلاسل التهشير. - إدارة مستويات الثقة. - استخدام IDS لكشف التصرفات الغريبة. - إدارة مفاتيح التعمية. - قياس قوة الإشارة.
هجوم Sybil	انتهاك الخصوصية، spamming، بثّ زائف في الشبكة، وخلل في خوارزمية Byzantine.	طبقة الشبكة	متوسطة المستوى	- الاختيار العشوائي لـ graphs. - تحليل سلوك المستخدمين. - الاحتفاظ بقوائم عن المستخدمين الموثوقين وغير الموثوقين.

المصادقة والاتصال الآمن	انتهاك الخصوصية	6LoWPAN, adaptation, transport and network layers	متوسطة المستوى	استخدام التنسيقات المضغوطة لـ AH وESP. استخدام ضغط الترويسة والبرمجيات القائمة على AES. استخدام المصادقة الهجينة.
الأمن من النهاية إلى النهاية على مستوى طبقة النقل	انتهاك الخصوصية	طبقتا الشبكة والنقل	متوسطة المستوى	DTLS-PSK with nonces. 6LoWPAN border router with ECC. DTLD cipher based on AES/SHA algorithms. DTLS header compression.
إنشاء واستئناف الجلسة	الحرمان من الخدمة	طبقة النقل	متوسطة المستوى	المصادقة باستخدام مفتاح سري طويل الأمد. التعمية المتناظرة.

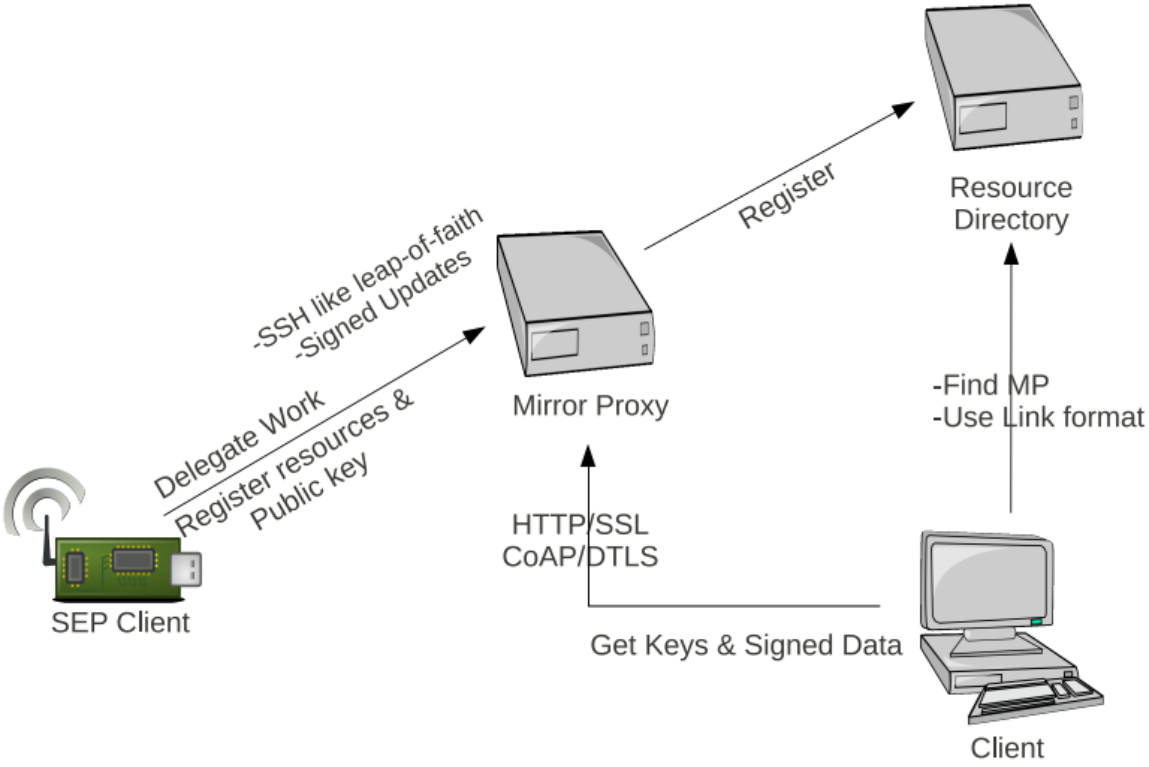
3.3.6.1- الحلول الأمنية عالية المستوى

جرى اقتراح مقاربة تعتمد على TLS وDTLS لتأمين شبكات LLN القائمة على بروتوكول CoAP والمتصلة بالإنترنت [43]، تعمل تلك المقاربة مع السيناريوهات التي يربط فيها موجه 6LBR شبكات LLN بالإنترنت من أجل الوصول إلى الأجهزة عن بعد، ويجري استخدام عقد LLN لتوفير الخدمة لعملاء (clients) بروتوكولات CoAP وHTTP، كما تعتمد المقاربة على إجراء تقابل (mapping) لِ TLS وDTLS لتوفير الأمن من النهاية إلى النهاية

الذي يحمي شبكات LLNs من الهجمات القائمة على الانترنت، لكن هذا التقابل قد يزيد الحمل على الأجهزة مقيدة الموارد. لذا، جرى اقتراح مقاربة أخرى لتأمين رسائل التطبيقات التي تتصل عبر الانترنت باستخدام خيارات أمن بروتوكول CoAP المختلفة، ومن تلك الخيارات الأمنية الجديدة: SecurityOn المسؤول عن حماية رسائل CoAP على مستوى التطبيق، SecurityToken الذي يسهل عمليات تحديد الهوية والتخويل لتوفير الوصول إلى موارد CoAP على مستوى التطبيق وSecurityEncap الذي يستخدم إعدادات خيار SecurityOn ويقوم بشكل أساسي بنقل البيانات المطلوبة للمصادقة والحماية من إعادة الإرسال، أدى استخدام الخيارات السابقة إلى تحسين عمل المقاربة المقترحة من حيث حجم حمولة الإطار واستهلاك الطاقة ومعدل الاتصال. جرى أيضاً اقتراح نموذج أمن لشبكات انترنت الأشياء القائمة على شبكات بروتوكول IP، باستخدام موجه 6LBR لترشيح الرسائل لتوفير الأمن من النهاية إلى النهاية، يمكن في ذلك النموذج إنشاء نفق TLS-DTLS يجري فيه استخدام موجه 6LBR لعمليات التقابل أثناء المصافحة، كما يمكن من خلال مضيفين يتشاركان مفتاح مشترك أن تجري عمليات التحقق من الرسالة وكشف هجمات التكرار في أجهزة CoAP. اقترحت دراسات أخرى [44] نموذجاً أمنياً (الشكل 1-8) يتميز بالفعالية في استهلاك الطاقة باستخدام تعمية المفتاح العام لنظام CoAP المستند إلى انترنت الأشياء، جرى تنجيز النموذج الأمني المقترَح من خلال نموذج أولي (prototype) يستخدم Mirror Proxy (MP) لتمثيل الطلبات من مخدّم إلى آخر أثناء مرحلة السكون، وَResource Directory لتمثيل قائمة الموارد في المخدّم، يسجّل MP المخدّمات أو النقاط النهائية (endpoints) ويضيف الموارد إلى شجرة الموارد ويخزّن أيضاً المفاتيح العامة للنقاط النهائية، يجري الوصول إلى الموارد من قبل العملاء من خلال معرفات الموارد، كما تنتقل المفاتيح العامة إلى العملاء ليجري استخدامها لاحقاً لمصادقة تحديثات البيانات، أظهرت التحليلات للنموذج المبدئي فعاليةً عالية مع الأجهزة محدودة الموارد.

يقدّم مشروع OWASP توصيات الإجراءات الاحترازية لتأمين انترنت الأشياء والتعامل مع الواجهات عالية المستوى وغير الآمنة [26]، من خلال توفير آليات أمان تقوم بتجنّب كلمات المرور الضعيفة، واختبار الواجهة ضد الثغرات الأمنية المعروفة في أدوات البرامج (XSS،SQLi) واستخدام HTTPS مع جدران الحماية (firewalls)، إضافة إلى تحديث البرامج والتعريفات المثبتة على الجهاز بانتظام من خلال آلية نقل معمّاة ومن مخدّمات آمنة بعد توقيع تلك التحديثات والتحقق من صحتها قبل التنزيل. اقترحت دراساتٌ أخرى [45] البرمجية الوسيطة VIRTUS middleware التي تقوم بالمصادقة والتعمية لتأمين التطبيقات الموزعة التي تعمل في بيئة انترنت الأشياء، تستخدم تلك البرمجية طريقة اتصال تستند إلى الحدث (event-driven communication) أثناء استخدام TLS وSASL لضمان سلامة البيانات وتعمية دفق XML والتحقق من صحته، تضمن آلية المصادقة المعتمَدة تبادل البيانات والوصول إلى الموارد فقط للمستخدمين المخولين، وقد أدّى تكامل تلك البرمجية الوسيطة مع خدمات الوب إلى تنفيذ تطبيقات انترنت الأشياء الموثوقة والقابلة للتوسّع. كما جرى اقتراح مخدّم وسيط يدعم ترشيح البيانات أثناء الاتصال بين بيئات انترنت الأشياء غير المتجانسة، ويدعم التسمية والعنونة والتوصيف في تلك البيئات، ويجري في ذلك المخدّم

تنجيز معيار AAA للمصادقة والتخويل وإدارة الحسابات من خلال التسلسل الهرمي للمفاتيح، مع وجود مفاتيح للجذر والتطبيقات والخدمات، كما يجري تسجيل الخدمة من خلال تنجيز بوابة (portal) قائمة على الوب لتوفير الوصول إلى الخدمات من قبل المستخدمين المخوّلين فقط.



الشكل 1-8 النموذج الأمني المقترَح في الدراسة [44].

جرى أيضاً اقتراح بنية معيارية مع طبقات مختلفة لتأمين الاتصال من آلة إلى آلة (M2M) في بيئة انترنت الأشياء، تشتمل البنية المقترحة على طبقات لخدمات الأمن، مثل طبقة خدمة أمن M2M التي يجري فيها تعمية محتويات المصدر (المرسِل) مع تبادل آمن للرسائل باستخدام جلسات TLS أو DTLS. ظهرت أيضاً نماذج أمنية لإنترنت الأشياء الوسيطة تستخدِم طرق التعمية المعيارية مثل AES لتوفير خصوصية البيانات، كما جرى فيها تطبيق الأمن من النهاية إلى النهاية وآليات المصادقة المفتوحة مما أدّى إلى تأمين اتصالات مكوّنات انترنت الأشياء بما فيها المستخدمين، التجهيزات والخدمات. يظهِر الجدول 1-5 القضايا الأمنية عالية المستوى، ومجال تأثيرها والطبقات المتأثرة مع الحلول المقترحة.

الجدول 1-5 القضايا الأمنية عالية المستوى وحلولها.

القضية الأمنية	تأثيرها	الطبقات المتأثّرة	مستويات IoT	الحلول المقترحة
أمن بروتوكول CoAP في الانترنت	عقدة الزجاجة في الشبكة، والحرمان من الخدمة.	طبقتا الشبكة والتطبيقات	عالية ومتوسطة المستوى.	- TLS/DTLS and HTTP/CoAP mapping. - Mirror Proxy (MP) and Resource Directory. - TLS/DTLS tunnel and message filtration using 6LBR.
الواجهات البرمجية غير الآمنة	انتهاك الخصوصية، الحرمان من الخدمة، وتعطيل الشبكة.	طبقة التطبيقات	عالية المستوى	- رفض كلمات المرور الضعيفة. - اختبار الواجهة البرمجية من ثغرات أدوات الاختبار (SQLi، XSS). - استخدام HTTPS مع الجدران النارية.
البرمجيات/البرمجيات الراسخة غير الآمنة	انتهاك الخصوصية، الحرمان من الخدمة، وتعطيل الشبكة.	طبقات التطبيقات، النقل، والشبكة	عالية، متوسطة ومنخفضة المستوى	- تحديثات آمنة للبرمجيات. - استخدام تواقيع الملف، والتعمية والتحقق.

Middleware Security	انتهاك الخصوصية، الحرمان من الخدمة، وتعطيل الشبكة.	طبقات التطبيقات، النقل، والشبكة	عالية، متوسطة ومنخفضة المستوى	- تأمين الاتصالات باستخدام المصادقة، سياسات الأمن، وإدارة المفاتيح بين العقد والبوابات وخدمات M2M.

7.1- خاتمة

قمنا في هذا الفصل بتقديم نظرة عامة عن أنظمة انترنت الأشياء (IoT)، حيث تحدّثنا عن مفهومها، بنيتها ثلاثية ورباعية الطبقات، عناصرها المختلفة وتطبيقاتها. ثم ناقشنا أهمّ القضايا والتحديات العتادية التي تواجهها مثل قيود استهلاك الطاقة، ومحدودية الموارد. تلك القضايا والميزات التي جعلتها غير قادرة على حماية نفسها إضافة إلى عدم وجود توحيد في المعايير والبروتوكولات الخاصة بها. كما تحدّثنا عن أهم التحديات والقضايا الأمنية التي تواجهها سواءً من حيث متطلبات الأمن والخصوصية الأساسية، أم من حيث طبقاتها منخفضة ومتوسطة وعالية المستوى، وأرفقنا ذلك بأهم الدراسات المرجعية لمعالجة تلك القضايا. سنتوجّه في الفصل القادم إلى الحديث عن سلسلة الكتل (blockchain) كتقنيّة واعدة معنيّة بحماية الأمن والخصوصية بدأت في عملة بتكوين الرقمية عام 2008، لننتقل بعدها إلى دراسة إمكانية سلسلة الكتل في حماية أمن وخصوصية انترنت الأشياء.

الفصل الثاني

سلسلة الكتل Blockchain

نعرِض في هذا الفصل تقنيةَ سلسلة الكتل، بنيتها، خواصّها، أنواعها، آلية عملها وتطبيقاتها المختلفة، إضافةً إلى بعض القضايا والهجمات الأمنية التي تتعرّض لها والحلول الأمنية الموافقة التي جرى طرحها في الأدبيات.

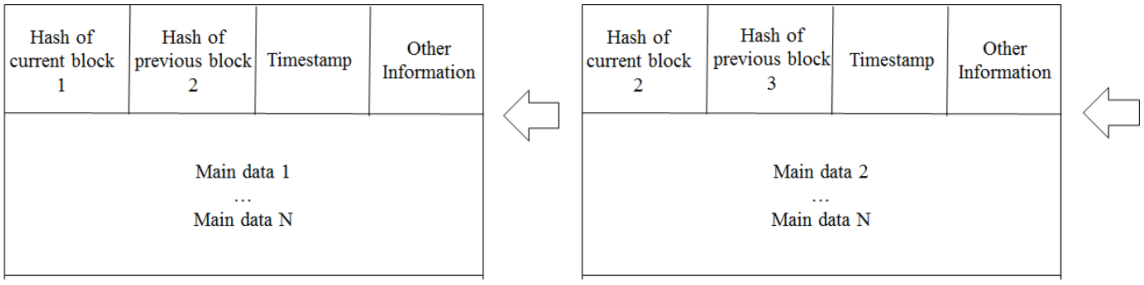
1.2- مقدمة

تعتبَر سلسلة الكتل إحدى أهم التقنيات شيوعاً في السنوات الأخيرة، أحدثت تغييرات كبيرة في مختلف مجالات الحياة بسبب تأثيرها الكبير على الكثير من الأنشطة التجارية والصناعية. تُعدّ Bitcoin أول تطبيقات سلسلة الكتل، وهي أحد أنواع العملة الرقمية القائمة على تقنيات سلسلة الكتل، تُستخدم للتجارة الالكترونية. بينما أصبحت العقود الذكية اليوم أحد أهم تطبيقات سلسلة الكتل. بعد النجاح الكبير الذي حققته سلسلة الكتل في مجال العملة الرقمية، جرى استخدامها في العديد من المجالات والخدمات الأخرى مثل السوق المالية، انترنت الأشياء، سلسلة الإمداد، التصويت، العناية الصحية والتخزين. لكن يتزامن تزايد استخدام تلك التقنية مع زيادة فرص المجرمين الالكترونيين في تحقيق هجمات الكترونية، تُشكّل مثلاً هجمات 51% مشكلة أمنية تقليدية في Bitcoin [46]، حيث يحاول المخترق التحكم بآلية النظام مستخدماً التقنية نفسها. تُعتبَر سلسلة الكتل مكوناً أساسياً مهماً في بحثنا، لذا، لابد من تقديم نظرة عامة عنها وعن كيفية عملها واستخدامها في كافة المجالات، ثم التطرق إلى استخدامها في انترنت الأشياء. جرى اختيار تقنية سلسلة الكتل في إنجاز هذا العمل نظراً لتمتّعها بخصائص عديدة سنتحدث عنها في هذا الفصل.

2.2- مفهوم سلسلة الكتل

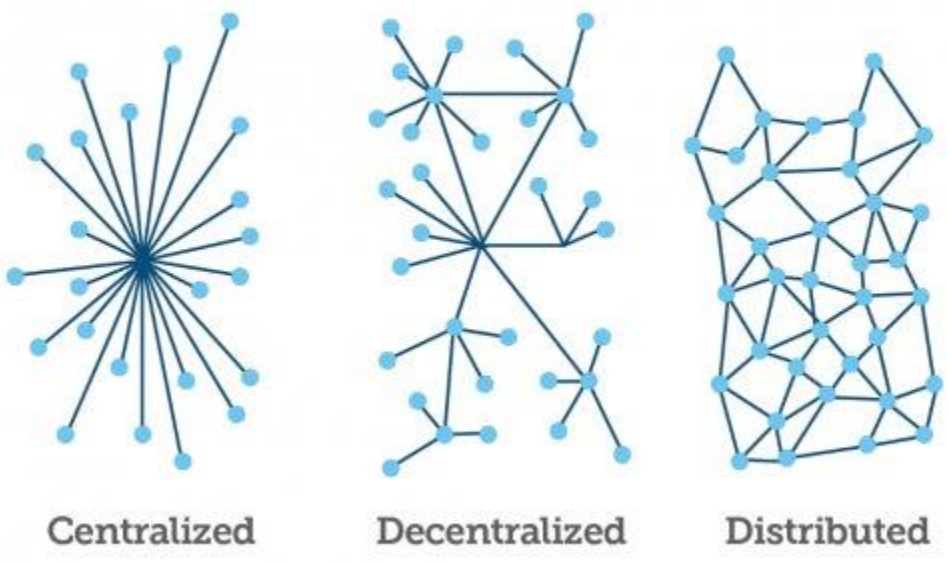
هي قواعد بيانات موزّعة تقوم بتسجيل قائمة مرتّبة زمنياً من السجلات والمناقلات التي تُربَط معاً بطريقة ثابتة عبر سلسلة من الكتل [47]، تُشكِّل تلك الكتل سلسلة خطية حيث تحوي كل كتلة على قيمة تهشير الكتلة السابقة

(الشكل 2-1) لينتج في النهاية سلسلة من الكتل المترابطة. يجري الاحتفاظ بسلاسل الكتل في شبكة من العقد، وتقوم كل عقدة بتنفيذ وتسجيل نفس المناقلات لديها وهي قادرة على قراءة أي مناقلة.



الشكل 2-1 بنية سلسلة الكتل.

لا تُعتبَر أنظمة سلسلة الكتل كتقنية واحدة مستقلة، وإنما تحوي تعمية، رياضيات، خوارزميات ونموذج اقتصادي، تجمَع شبكات الند للند وتستخدم خوارزميات توافق موزعة لحلّ المشاكل التقليدية لتزامن قواعد المعطيات الموزّعة، فهي تُعتَبر بنية تحتية متكاملة متعددة المجالات [48].



الشكل 2-2 طبولوجيات الشبكات.

يظهِر الشكل 2-2 الطبولوجيات المختلفة للشبكات، المركزيّة، اللّامركزيّة والموزّعة (الموزّعة هي نمط شبكة سلسلة الكتل)، حيث تتمتع شبكات سلسلة الكتل بعدّة ميزات أهمها [49]:

- عمومية (public): وهي الميّزة الأكثر أهمية، حيث يمكن لجميع المشاركين الاطّلاع على الكتل والمناقلات المخزّنة بها، لكن هذا لا يعني أنه يمكن للجميع رؤية المحتوى الفعلي لمناقلة معينة فهي محمية بواسطة المفتاح الخاص.
- لا مركزية decentralized: لا تعتمد على عقدة مركزية او سلطة واحدة للموافقة على المناقلات أو وضع قواعد محدّدة لقبولها، يمكن إنشاء البيانات وتخزينها وتحديثها بشكل موزّع، ويتوجّب على جميع المشاركين في الشبكة التوصّل إلى توافق في الآراء لقبول المناقلات.
- شفّافة Transparent: كل البيانات المخزَّنة في سلسلة الكتل شفّافة لجميع العقد المشارِكة، وشفافة أيضاً في تحديث تلك البيانات، لذا تعتبَر سلسلة الكتل موثوقة
- آمنة Secure: يمكن فقط توسعة قاعدة البيانات دون تغيير السجلات السابقة (هنالك كلفة مرتفعة جداً لتغيير السجلات السابقة).
- مفتوحة المصدر Open Source: معظم أنظمة سلسلة الكتل مفتوحة للجميع، حيث يمكن التحقق من التسجيل علناً، كما يمكن للمستخدمين استخدام تقنيات سلسلة الكتل لأي تطبيق يريدون.
- الاستقلالية Autonomy: يمكن لأي عقدة في نظام سلسلة الكتل نقل البيانات وتحديثها بأمان بسبب وجود قاعدة التوافق (consensus)، حيث تعتمد على بناء شبكة موثوقة من عقد غير موثوقة.
- ثابتة Immutable: وغير قابلة للتغيير، حيث يحفظ فيها أي تسجيل إلى الأبد، ولا يمكن تغييره إلّا في حالة السيطرة على أكثر من 51% من العقد في نفس الوقت.
- متخفّية الهوية Anonymity: حلّت تقنيات سلسلة الكتل مشكلات الثقة من عقدة إلى عقدة، لذا، يمكن أن يكون نقل البيانات والمناقلات مجهولاً، يكفي فقط معرفة عنوان المستقبِل.

3.2- مفاهيم أساسية

وصف العديد من المؤلفين في الأدبيات معنى مصطلح blockchain بطرق مختلفة، لكن الأساس المشترك هو أن المصطلح مشتق من تطبيقه الأول، Bitcoin، وبنية البيانات المستخدمة فيه، ساتوشي ناكاموتو هو الاسم المستعار لمؤسس ومطور Bitcoin، والذي لاتزال هويته الحقيقية غير معروفة حتى الآن فيما إن كانت تدل على شخص أو مجموعة أشخاص أو مؤسسة ما. نحتاج أولاً إلى تعريف مصطلح blockchain والمصطلحات ذات الصلة لنكون قادرين على التحليل الأكاديمي لأنظمة سلسلة الكتل، وذلك اعتماداً على المقالة الأساسية لناكاموتو عام 2008 [50] كالتالي:

سلسلة الكتل:

هي سلسلة متزايدة مستمرّة من الكتل (أي سجلات)، تشكِّل قائمة متسلسلة مترابطة من البيانات المنفصلة مع مؤشرات تهشير، يجري عادةً توزيع ونشر سلسلة الكتل عبر شبكة الند للند، التي تتحقق من سلامة الكتل الموجودة وتضيف كتلاً جديدة إلى السلسلة لتكون بمثابة قاعدة بيانات موزّعة، تجري عمليات التحقق باتّباع قواعد البروتوكول والمسمّاة codebase، وذلك لتأمين الأنظمة عن طريق التصميم من خلال التحقق من صحة البيانات في الوقت المناسب.

نظام سلسلة الكتل:

هو نظام قائم بأكمله على سلسلة الكتل، بما فيه البيانات وهيكليتها، الشبكة وبنيتها التحتية وقواعد المعطيات.

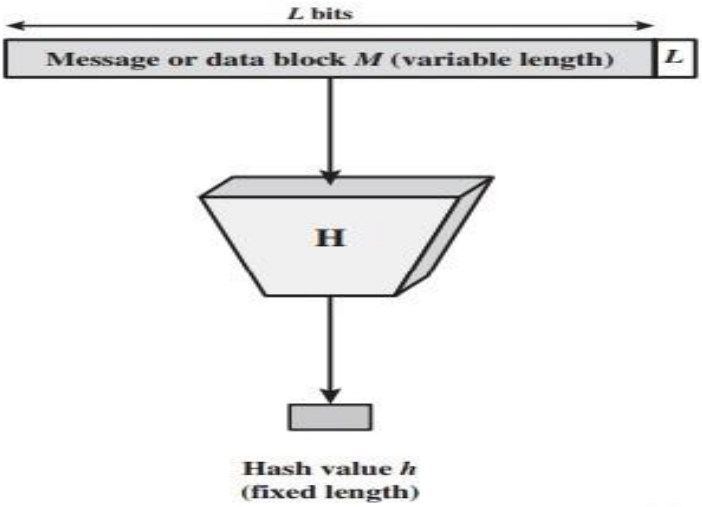
الوحدة الرقمية (Token) لسلسلة الكتل: هو حامل افتراضي اختياري يستخدَم في بيانات سلسلة الكتل كوسيلة للملكية أو التعريف أو أي شكل من أشكال الحقوق والالتزامات.

الكتلة: هي وحدة بيانات تعمل كسجلّ يشتمل على ترويسة للبيانات المترفّعة (meta data)، ومتن للبيانات الأخرى المنفصلة وهي البيانات الرئيسية لسلسلة الكتل، تحتوي الترويسة على قيم تهشير بيانات الكتلة نفسها ومؤشر تهشير إلى ترويسة كتلة أخرى موجودة، توجد حالة خاصة وحيدة دون مؤشر على كتلة سابقة وهي حالة كتلة genesis التي تمثّل بداية السلسلة (كما سنرى في الفقرة 1.1.2.4-).

توابع التهشير والتوقيع الرقمي

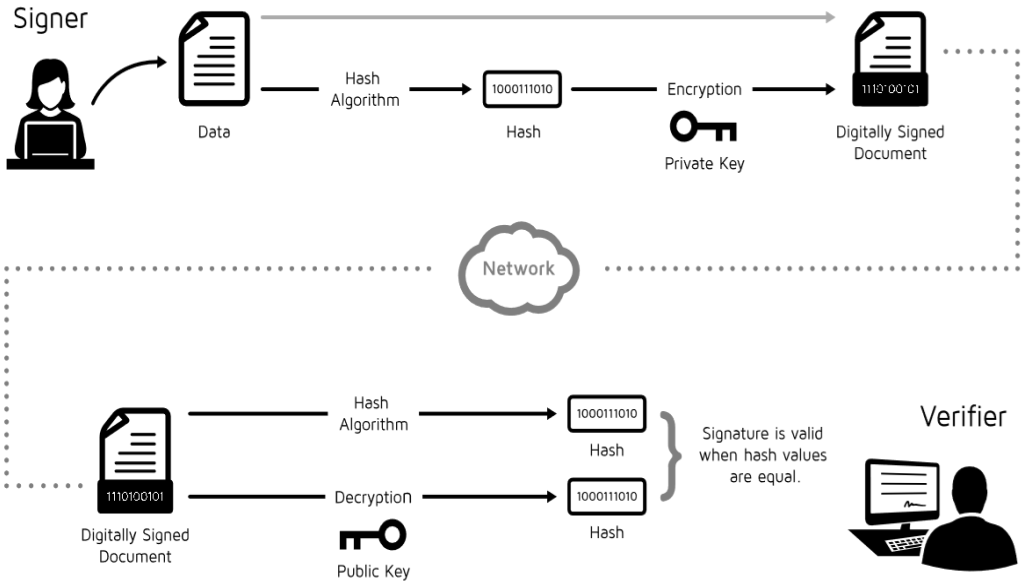
هي توابع وحيدة الاتجاه تقوم بشكل عام بتحويل أي دخل من البيانات بطول متغير من البتات إلى خرج بطول ثابت (الشكل 2-3) باستخدام توابع رياضية، أي يقوم بإجراء تقابل بين دخل بطول متغير وخرج بطول ثابت [6].

يعطي استخدام خوارزميات تهشير مختلفة نتائجَ متمايزة مع مجموعة من الخصائص المميزة، فعلى سبيل المثال، يمكن أن يؤدي التهشير إلى تسريع عمليات البحث عن بيانات معينة في قرص تخزين، وذلك عن طريق فهرسة البيانات في مصفوفة ثم البحث عن قيم التهشير في المصفوفة والتي تدل على المواقع الأصلية للبيانات. كما تضمن توابع التهشير سلامةَ البيانات من خلال ربطها ببصمتها الخاصة (التوقيع الرقمي) مما يضمن عدم التلاعب بالبيانات أو تغييرها كما يبيّن الشكل 2-4.



الشكل 2-3 مخطط صندوقي لتابع التهشير **h=H(M)**.

حيث يقوم المرسِل بتهشير الرسالة ثم تعمية قيمة التهشير بمفتاحه الخاص لتَنتُج قيمة التوقيع الرقمي للرسالة، ثم يرسِل الرسالة وبصمتها (توقيعها)، ليقوم المستقبل باستخدام المفتاح العام للمرسل بفكّ تعمية التوقيع ومقارنته مع نتيجة تهشير الرسالة الأصلية (الشكل 2-4) للتحقق من عدم التلاعب بالبيانات مما يضمن سلامتها (Integrity).



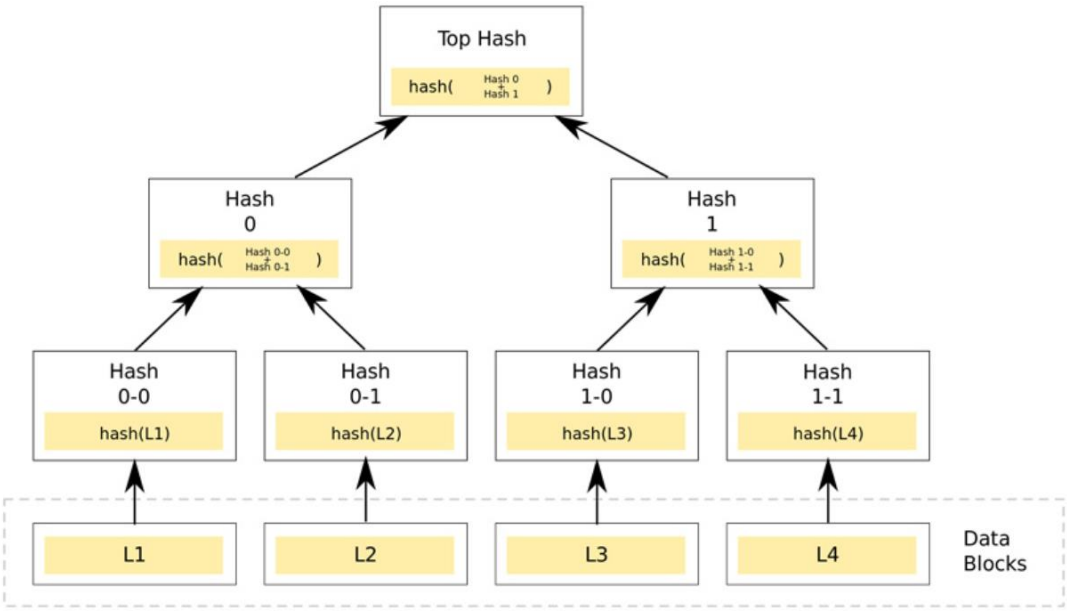
الشكل 2-4 استخدام توابع التهشير في التوقيع الرقمي.

يمكن أيضاً استخدام توابع التهشير عند تخزين البيانات بشكل غير آمن، حيث يمكن في أي وقت إعادة حساب بصمة البيانات للتحقق من تطابقها مع البصمة القديمة مما يضمن سلامة البيانات. تختلف عملية التهشير عن التعمية

حيث ينتِج التهشير بصمة مميزة للبيانات وغير قابلة للاسترجاع بينما نستطيع استعادة البيانات الأصلية من المعمّاة عند معرفة مفتاح التعمية.

جذر شجرة Merkle

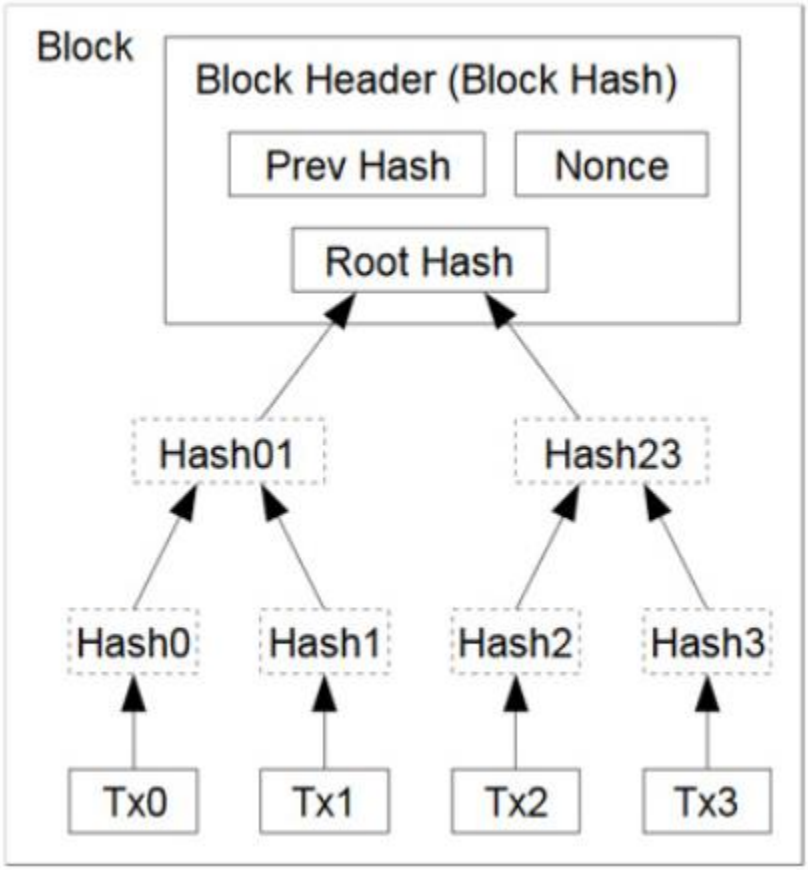
تعتبَر أشجار ميركل عنصراً أساسياً في سلسلة الكتل، حيث تسمح بالتحقق الفعال والآمن من بنيات (structures) البيانات الكبيرة، كما تفيد في التحقق من سلامة البيانات بالاعتماد على توابع التهشير [50]، جرى اختراعها في العام 1979 من قبل العالم Ralph Merkle. وهي تعتبَر كأشجار بنية بيانات كما يوضّح الشكل 2-5، حيث يجري تمثيل كل عقدة ورقية (العقد الورقية هي المستوى الأدنى من الشجرة) بعقدة غير ورقية (أو فرع) هي قيمة تهشير العقدة الورقية، حيث يمثّل الفرع Hash 0-1 قيمة تهشير العقدة L2 على سبيل المثال.



الشكل 2-5 مثال عن شجرة تهشير ثنائية.

يمثِّل الشكل 2-5 أبسطَ مثالٍ عن شجرة ميركل وهي شجرة ميركل الثنائية، وتمثِّل عقدةُ الجذر (Top Hash) قيمةَ تهشير الشجرة بالكامل وتسمّى تهشير الجذر، وبالتالي تمثِّل تلك الشجرة بنية بيانات تحوّل n عملية تهشير إلى قيمة تهشير واحدة. تسمح شجرة ميركل بإجراء تقابل فعّل لكميّات عشوائية كبيرة من البيانات وتمكّن من الكشف عن حصول أي تغيير فيها، كما تساعد على عمليات التحقق باستخدام عقدة الجذر فقط دون الحاجة إلى التحقق من كل عمليات التهشير. جرى استخدام شجرة ميركل في بروتوكول عملة بتكوين [50] كما يوضح الشكل 2-6، وتستَخدَم لتوفير المساحات التخزينية وفي عمليات التحقق من خلال تهشير كل مناقلات الكتلة ووضعها في حقل "Root Hash" الخاص بها في ترويسة الكتلة كما سنرى في الفقرة (4.2-) عندما سنتحدّث عن بنية الكتلة، مما

يساهم في كشف عمليات التعديل غير المصرح به لأيّ مناقلة مخزنة في سلسلة الكتل ويساعد في ترابط الكتل مع بعضها.

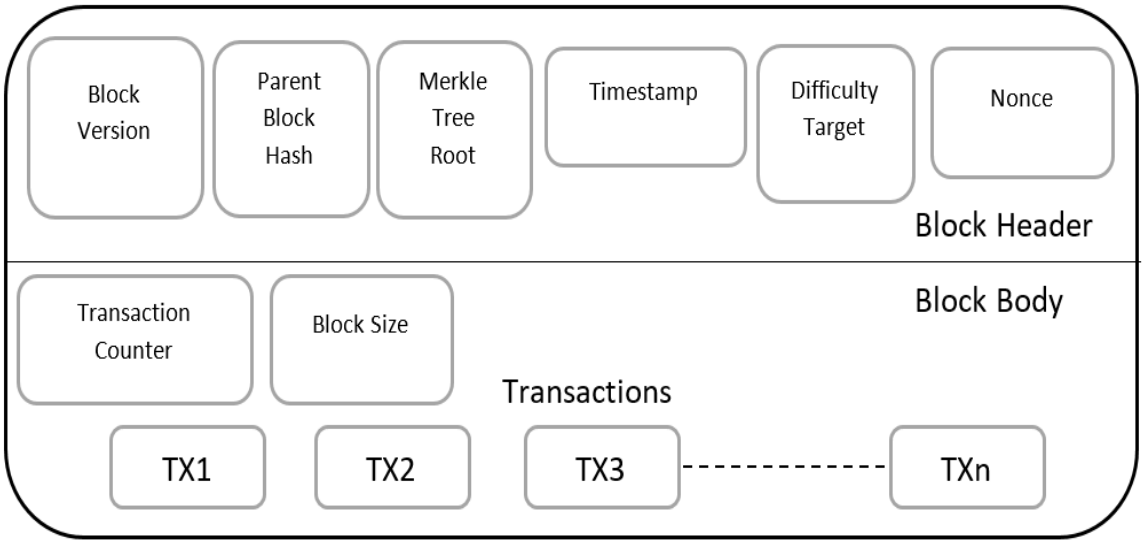


الشكل 2-6 تهشير مناقلات الكتلة في شجرة ميركل [50].

4.2- آلية عمل سلسلة الكتل

جرى طرح مفهوم سلسلة الكتل لأول مرة عام 2008 في المقالة [50] من قبل مؤلف مجهول الهوية كما ذكرنا سابقاً، تصِف تلك المقالة نظام عملة الند للند الذي يسمح بمناقلات نقدية آمنة عبر الانترنت دون الحاجة إلى مؤسسة مالية وسيطة، وذلك بسبب ظهور بنية بيانات جديدة موضّحة أيضاً في المقالة السابقة تدعى سلسلة الكتل. ساعدت تقنية سلسلة الكتل أنظمة Bitcoin وغيرها من العملات الرقمية المعمّاة على تبادل عملاتها بشكل آمن عبر الانترنت. نستطيع أن نستنتج من اسم تلك التقنية أنها عبارة عن مجموعة من الكتل المتسلسلة والمترابطة معاً، حيث تحوي كل كتلة على قيمة تهشير محتواها إضافةً إلى قيمة تهشير الكتلة السابقة في السلسلة. يمكن اعتبار سلسلة الكتل وكأنها قاعدة بيانات شفافة تحتوي على سجل المناقلات بالكامل لجميع عملات بتكوين التي جرى إنشاؤها، مما يمكِّن

المستخدمين من معرفة رصيد العملات لأي مستخدم. يملك كل مستخدم في سلسلة كتل البتكوين زوجاً من المفاتيح المنشَأة بشكل عشوائي، أحدها عام والآخر خاص. تعبّر المفاتيح العمومية عن عناوين مستخدمي بروتوكول البتكوين ويجري استخدامها لاستقبال العملة (بتكوين)، بينما يستخدمون المفتاح الخاص لإرسال العملات من خلال توقيع المناقلة بذلك المفتاح الخاص بالمستخدم، ويقوم باقي المستخدمون بالتحقق من المناقلة باستخدام المفتاح العام للمرسِل.



الشكل 2-7 بنية الكتلة في سلسلة الكتل.

يظهِر الشكل 2-7 بنية الكتلة الواحدة في سلسلة الكتل، والتي تتألف بشكل رئيسي من ترويسة الكتلة (Block Header) و جسم الكتلة (Block Body)، يوضّح الجدول 2-1 الحقول الرئيسية الموجودة في الكتلة [49]:

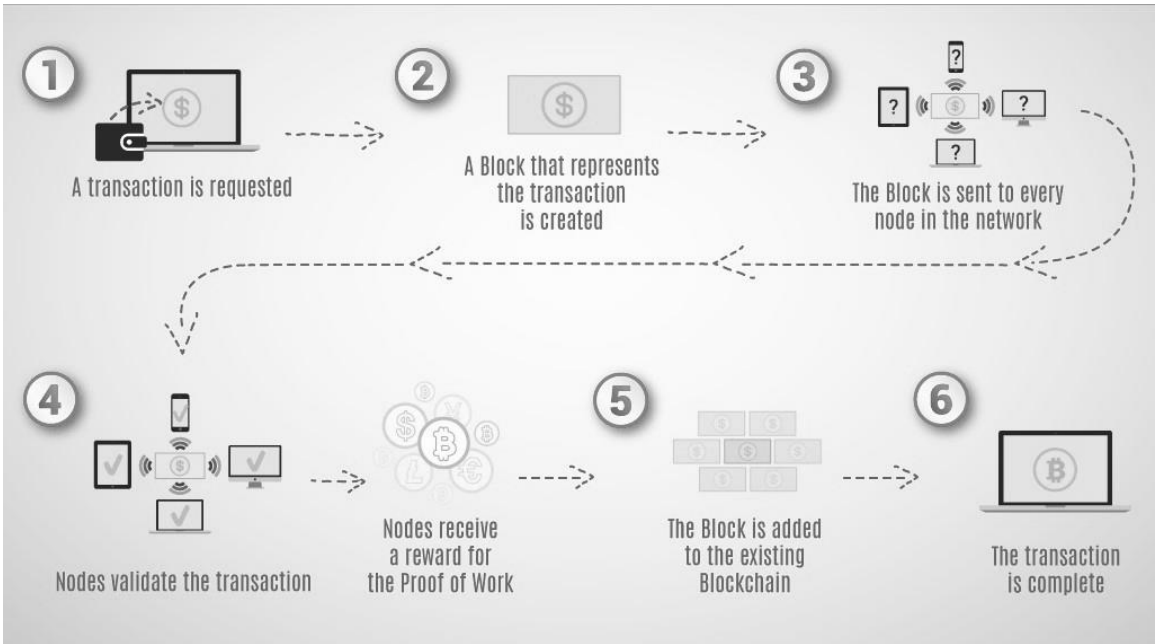
الجدول 2-1 بنية الكتلة في سلسلة الكتل.

	الحقل	**الحجم**	**الوصف**
ترويسة الكتلة (80 بايت)	الإصدار version	4 بايت	إصدار سلسلة الكتل (1.0 من أجل العملات الرقمية)
	تهشير الكتلة الأب	32 بايت	قيمة تهشير ترويسة الكتلة السابقة
	جذر ميركل	32 بايت	قيمة تهشير جذر شجرة ميركل لمناقلات الكتلة (الفقرة 3.2-)

	البصمة الزمنية Timestamp	4 بايت	البصمة الزمنية المعبّرة عن زمن إنشاء الكتلة بتنسيق UNIX[3].
	Difficulty Target	4 بايت	هدف التهشير الحالي، ويعبر عن صعوبة خوارزمية التوافق المستخدَمة (الفقرة 6.2-).
	Nonce	4 بايت	عداد يستخدَم من قبل المنقِّبين (miners) لتوليد التهشير الصحيح، حيث يبدأ من الصفر ويزداد عند كل عملية حساب للتّهشير.
جسم الكتلة (حجم متغير)	حجم الكتلة	4 بايت	حجم الكتلة بالبايت
	عداد المناقلات	1-9 بايت	عدد المناقلات في الكتلة
	المناقلات	حجم متغير	هي المحتوى الرئيسي للكتل، تختلف باختلاف التطبيق، حيث يمكن أن تعبر عن معلومات مالية أو معلومات خاصة بإنترنت الأشياء .....

نلاحظ مما سبق أن حقل عداد المناقلات يتراوح بين 1 و9 بايت من الحجم، بينما يتغير حجم حقل المناقلات حسب عدد المناقلات الموجودة في الكتلة، كما يعتمد العدد الأعظمي للمناقلات الذي تستطيع الكتلة احتواءه على حجم الكتلة وحجم كل مناقلة. تلعب ترويسة الكتلة دور المعرّف للكتلة وتتكوّن من قيم تهشير، يجري توليده باستخدام خوارزمية SHA-256 وحيدة الاتجاه والتي تعطي خرج ثنائي بطول 256 بت، نجد أيضاً أن حجم ترويسة الكتلة هو 80 بايت يجري حسابها اعتماداً على ثلاث مجموعات من البيانات المترفّعة للكتلة: المجموعة الأولى هي مؤشر على الكتلة الأخيرة وهي قيمة تهشير الكتلة السابقة (الكتلة الأب)، والتي تربط الكتلة بالسلسلة بشكل فعال، تمثّل المجموعة الثانية البيانات المتعلقة بمنافسة التنقيب: الصعوبة، البصمة الزمنية، والـ Nonce. بينما تمثّل المجموعة الثالثة جذر شجرة Merkle لمناقلات الكتلة الحالية. تستخدِم سلسلة الكتل آليات التعمية غير المتناظرة للتحقق من مصادقة المناقلات، كما يجري استخدام التوقيع الرقمي القائم على التعمية غير المتناظرة في البيئات غير الموثوقة.

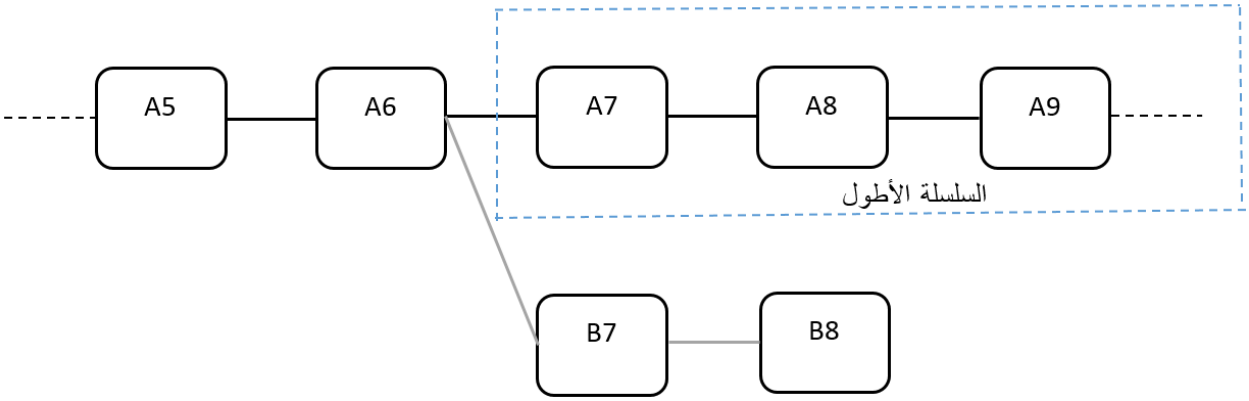
[3] تنسيق UNIX هو عدد الثواني بين الوقت الحالي وبين بداية توقيت UTC بتاريخ 01-01-1970.



الشكل 2-8 آلية عمل سلسلة الكتل.

لإضافة كتلة جديدة إلى سلسلة الكتل، يجري في البداية التنقيب عنها بواسطة عقدة التنقيب في شبكة بتكوين، وهي عقدة مسؤولة عن تجميع الكتل استناداً إلى تعريفات بروتوكول سلسلة كتل البتكوين، يجب على تلك العقدة ملء الجدول 2-1 للتنقيب عن كتلة ما وإضافتها إلى سلسلة الكتل ابتداءً برقم الإصدار الذي يصف إصدار بنية الكتلة، ثم إضافة قيمة تهشير ترويسة الكتلة السابقة، تقوم العقدة بعد ذلك بالحصول على عدد من المناقلات غير المنقَّب عنها ثم تولّد شجرة ميركل الخاصة بتلك المناقلات وتخزّن قيمة جذر الشجرة (يلخّص جذر شجرة ميركل جميع مناقلات الكتلة كما ذكرنا سابقاً)، تقوم العقدة بعدها بإضافة البصمة الزمنية مرمّزةً بترميز UNIX. يجب أن تستغرق عملية التنقيب عن الكتلة 10 دقائق على الأقل [50]، وللحفاظ على هذا الزمن يجب ضبط قيمة هدف الصعوبة (difficulty Target) على هذا الأساس (المعادلة (2-1))، حيث يجري ضبط تلك القيمة وفقاً لطاقة التنقيب الموجودة في الشبكة في الوقت الحالي، وبالتالي، تقوم العقدة بعد إضافة البصمة الزمنية بضبط قيمة هدف الصعوبة استناداً إلى قوة الشبكة، وأخيراً تقوم العقدة بإضافة قيمة Nonce بقيمة ابتدائية هي الصفر. تبدأ عملية التنقيب بعد ملء جميع الحقول السابقة، وهدف تلك العملية هو العثور على قيمة لِ nonce تجعل قيمة تهشير الكتلة أقل من هدف الصعوبة (المعادلة (2-1))، حيث تقوم العقدة بتجريب (brute forcing) مليارات القيم المتزايدة لـ nonce وحساب قيمة تهشير ترويسة الكتلة لكل قيمة حتى الحصول على قيمة تحقق المطلوب، تثبِت العقدة عملها (POW) من خلال تلك العملية السابقة كما أوضَح ساتوشي [50]. يجري بثّ الكتلة إلى الشبكة بعد العثور على قيمة التهشير الصحيحة، لتقوم باقي عقد الشبكة بالتحقق منها، ثم إضافتها إلى سلسلة الكتل. نستنتج مما سبق أن عملية إنشاء مناقلة ما تستغرق 10 دقائق، ولكن هذه هي الحالة المثالية أما في الواقع **فيوجد تأخير زمني** في النظام حيث لا يحصل

جميع المنقّبين (miners) على نفس المناقلات دفعةً واحدة، مما يجعلهم يقومون بالتنقيب عن كتل مختلفة لإضافتها إلى سلسلة الكتل وهذا غير مسموح حيث أن تلك الكتل قد تحوي مناقلات مشتركة وبالتالي لا يمكن إضافة نفس المناقلة إلى سلسلة الكتل أكثر من مرة، يترتّب على ذلك إنفاق طاقة حسابية دون جدوى من قبل العقدة المنقِّبة أثناء قيامها بالتّنقيب عن كتلة تحوي على مناقلة مضافة مسبقاً إلى إحدى الكتل في السلسلة قبل الوصول إلى قيمة nonce الصحيحة. **كما يوجد احتمال** تشكيل سلسلتين من الكتل عند قيام عقدتي تنقيب بإضافة كتلتين مختلفتين بنفس اللحظة كما يظهِر الشكل 2-9، جرى إيجاد حل لتلك المشكلة في بروتوكول بتكوين عند إنشاء سلسلتين أو أكثر من خلال اعتماد السلسلة الأطول وإهمال السلاسل الأخرى.



الشكل 2-9 حالة إنشاء أكثر من سلسلة (تفرّع السلسلة).

عند إنشاء أكثر من سلسلة معاً **بنفس الطول** لكن باختلاف الكتلة الأخيرة، يكون للعقد المنقِّبة حق الاختيار بين السلاسل لتكمِل التّنقيب على أساس إحداها، إلّا في حال جرى إضافة كتلة معينة إلى إحدى السلاسل فعندها تصبح هي الأطول وعلى جميع المنقّبين إكمال تلك السلسلة الأطول وإهمال البقيّة، حتى وإن كانت تحوي مناقلات صحيحة لكنها تصبح غير صالحة بمجرّد عدم انتمائها إلى السلسلة الأطول، هذا يعني وجوب إعادة تنقيبها وضمّها إلى سلسلة الكتل الأطول لتصبح صالحة. لذا، يجري في البتكوين اعتبار المناقلة صالحة فقط عندما تبلغ 6 كتل من العمق في السلسلة، أي يجب على المستخدم (العقدة) انتظار زمن تنقيب 6 كتل أي ساعة على الأقل لاعتبار مناقلته صالحة. يجري استخدام أفكار مشابهة لزمن الانتظار في التقنيات الأخرى لسلسلة الكتل، فمثلاً يستغرق التنقيب عن الكتلة الواحدة في الإثريوم (Ethereum) 14 ثانية تقريباً مما يزيد احتمال وجود أكثر من سلسلة معاً. لذا، يجب على العقد انتظار 12 كتلة من العمق في السلسلة لاعتبار مناقلاتهم صالحة، توجد أيضاً آليات أخرى في الإيثيريوم ناجعة أكثر منها في البتكوين فيما يخص التنقيب.

نجد من كل ماسبق وكما يوضّح الشكل 2-8: يقوم المستخدمون بإنشاء المناقلات، تقوم العقد المنقِّبة بتجميع المناقلات في كتل، وإجراء العمليات الحسابية على الكتل لإيجاد التهشير الصحيح للكتلة، وإيجاد شبكة من المنقِّبين

للتحقق من صحة تلك العمليات الحسابية، ثم إضافة الكتلة إلى سلسلة الكتل. تُعتَبّر العمليات السابقة هي جوهر بنية بيانات سلسلة الكتل، لكن من الممكن أن يكون للتقنيات القائمة على سلسلة الكتل تنجيزاتٍ مختلفة لها، حيث يتمثَّل الاختلاف في حجم الكتلة، بنية الكتلة، إثبات العمل الذي يحتاج المنقِّبون إلى تقديمه، خوارزمية التهشير، الصعوبة، زمن التّنقيب وغيرها ....

تتكوّن بروتوكولات سلسلة الكتل بشكل عام من العقد الشبكية، وتكون العقدة إما عاملة/منقِّبة أو مجرد عقدة مستخدم عادية، لكن جميع العقد لديها عنوان عام وعنوان خاص سرّي، يحتوي بروتوكول سلسلة الكتل عادةً على وحدة رقمية "Token" (الفقرة 3.2-) أو عملة للقيام بالمناقلات، ويجري استخدام توقيع المناقلات بالمفاتيح الخصوصية للمستخدمين لإثبات ملكية الوحدة الرقمية أو العملة. لكن ذلك لا يكفي لإجراء المناقلات، وإنما يجب على العقد المنقِّبة تجميع المناقلات في كتل، وتقديم بعض الإثباتات والاختبارات للوصول إلى توافق (consensus) حول الكتل التي يجب إضافتها إلى السلسلة، وهي عملية التنقيب. يجري إقرار كيفية وصول العقد المنقِّبة إلى توافق حول الكتل الواجب إضافتها وإلى محتواها من المناقلات بناءٍ على خوارزمية التوافق المتَّبَعة (سنتحدّث عن آليات التوافق المستخدَمة في سلسلة الكتل في الفقرة 6.2-)، وهذا ما يجعل سلسلة الكتل لامركزية حيث يمكن لجميع العقد الوصول إلى السلسلة كما يجري بناء السلسلة اعتماداً على خوارزمية التوافق.

5.2- أنواع سلسلة الكتل

يمكننا تقسيم تقنيات سلسلة الكتل إلى أربعة أنواع رئيسية [48]:

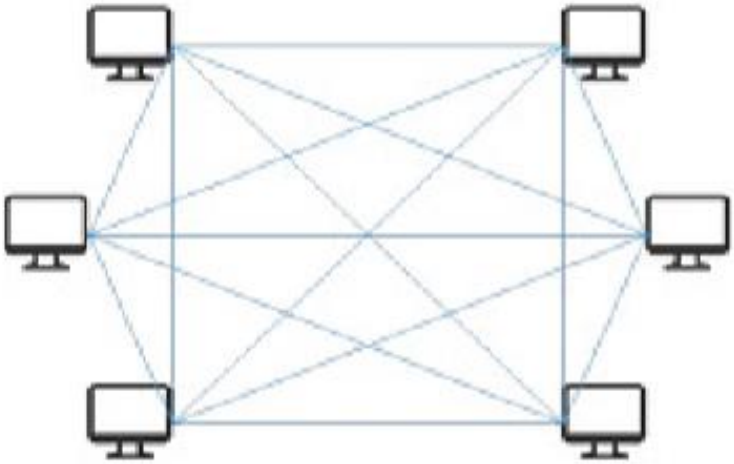
1.5.2- سلسلة الكتل العامة (Public)

هي سلسلة مفتوحة المصدر، يمكن أن يشترك بها أي مستخدم أو مطوّر أو عقدة منقِّبة، تستطيع فيها أي عقدة مشارِكة أن تتفحّص المناقلة وتتحقق من صحتها (أي أن جميع مناقلاتها شفافة كما رأينا في الفقرة 2.2-)، كما تستطيع المشاركة في عملية التوافق (الفقرة 6.2-)، تعتبَر بتكوين وإثريوم مثالين عن سلسلة الكتل العامة، ويوضّح الشكل 2-10 تلك السلسلة.

يتمتّع هذا النوع بالخواص التالية:

- لامركزية بالمطلق ولا يوجد أي كيان وحيد قادر على التحكم بالمناقلات التي تسجَّل في السلسلة أو الترتيب الذي يجري معالجتها به.
- منيعة ضدّ الرقابة، حيث يمكن لأي أحد أن يشترِك بها بغض النظر عن موقعه أو جنسيته، مما يجعل من الصعب على السلطات إغلاقها.

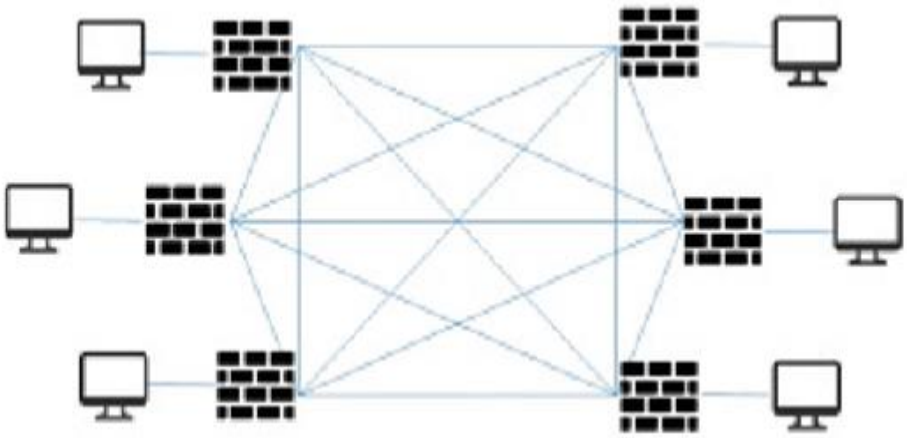
- تحوي على حامل رقمي مرتبط بها لتحفيز ومكافأة العناصر المشارِكة في الشبكة.



الشكل 2-10 سلسلة الكتل العامّة.

2.5.2- سلسلة الكتل الخاصة (Private)

تُعرَف أيضاً باسم " permissioned"، يجري فيها تقييد العقد، حيث لا تستطيع العقدة المشارَكةَ في سلسلة الكتل إلّا بعد حصولها على الموافقة، ويحوي هذا النوع إدارة سلطة صارمة في الوصول إلى البيانات، يوضّح الشكل 2-11 سلسلة الكتل الخاصة.



الشكل 2-11 سلسلة الكتل الخاصّة.

تتمتّع سلسلة الكتل الخاصة بالميزات التالية:

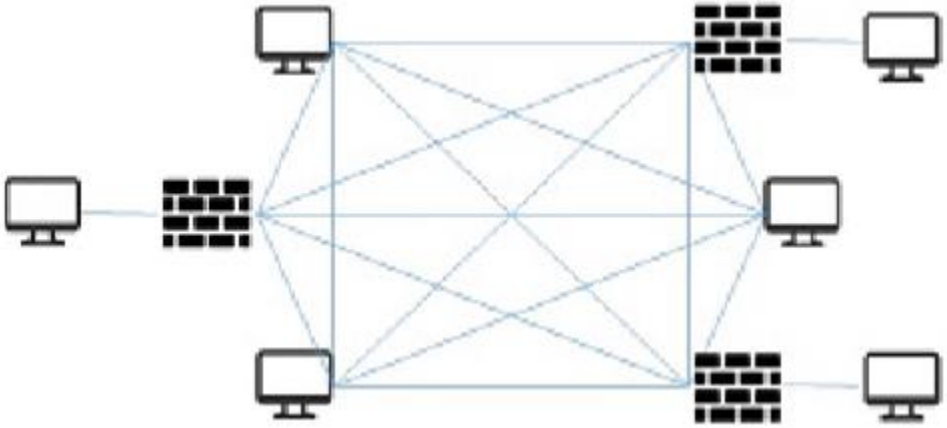
- يحتاج المشاركون إلى موافقة للانضمام إلى الشبكة.

- المناقلات سرية ومتوفّرة فقط لمشتركي ecosystem الذين حصلوا على موافقة للانضمام إلى الشبكة.
- أكثر مركزية من سلسلة الكتل العامة.
- لا تحوي على حامل رقمي مثل سلسلة الكتل العامة.

تستخدَم سلسلة الكتل الخاصة من قبل المؤسسات التي ترغب بالتعاون ومشاركة البيانات دون أن تظهِر بيانات الأعمال الحساسة الخاصة بها على سلسلة الكتل العامة.

3.5.2- سلسلة الكتل المتّحدة (Consortium)

يعتبَر هذا النوع حالة خاصة من سلسلة الكتل الخاصة، ولكنّها تُدار من قبل مجموعة كيانات وليس كيان واحد يجري فيها الاختيار المسبق للعقد صاحبة السلطة، وتحوي عادةً شراكات في الأعمال التجارية، يمكن أن تكون البيانات المخزَّنة في سلسلة الكتل عامةً أو سرية، ويمكن اعتبار هذا النوع من سلسلة الكتل شبه لا مركزي، مثل Hyperledger وR3CE ، يوضّح الشكل 2-12 سلسلةَ الكتل المتّحدة.



الشكل 2-12 سلسلة الكتل المتّحدة.

تتمتّع سلسلة الكتل المتّحدة بالخواص التالية:

- نموذج تعاوني يوفّر أفضل حالات الاستخدام لسلسلة الكتل، حيث يجمع بين عدد من الشركات المتنافسة معاً.
- يمكن للمشتركين أن يكونوا أكثر فعالية، سواءً فردياً أم جماعياً، من خلال التعاون في بعض جوانب أعمالهم.
- يمكن أن يشارك في هذه السلسلة أفراداً من البنوك المركزية، الحكومات، وسلاسل التوريد.

4.5.2- سلسلة الكتل الهجينة (Hybrid)

يجمع هذا النوع بين مزايا الخصوصية لسلسلة الكتل الخاصة ومزايا الأمن والشفافية لسلسلة الكتل العامة، مما يمنح المشاركين مرونةً كبيرة في اختيار البيانات التي يريدونها عامة وشفافة وبين البيانات التي يريدون الاحتفاظ بها كبيانات سرية، تعتبر منصّة Dragonchain مثالاً عن سلسلة الكتل الهجينة، يتمتّع هذا النوع بالخصائص التالية:

- الاتصال بسهولة مع البروتوكولات الأخرى لسلاسل الكتل، وبالتالي إنشاء شبكات multi-chain.
- تسهيل عمل الشركات بالشفافية التي تريدها، دون الاضطرار إلى التضحية بالأمن والخصوصية.
- زيادة أمن المناقلات، حيث تستفيد من قوة التهشير المشتركة في سلسلة الكتل العامة.

6.2- آليّات التوافق (Consensus) المستخدَمة في سلسلة الكتل

لا تحتاج أنظمة سلسلة الكتل إلى سلطة خارجية موثوقة لضمان وثوقية البيانات والتوافق على المناقلات بسبب كونها أنظمةً لا مركزية، حيث تستخدِم آليات توافق لا مركزية، توجد أربع آليات رئيسية للتوافق في أنظمة سلسلة الكتل الحاليّة هي [49]:

- Proof of Work (PoW)
- Proof of Stake (PoS)
- Practical Byzantine Fault Tolerance (PBFT)
- Delegated Proof of Stake (DPoS)

كما توجد آليات توافق أخرى أقل استخداماً مثل:

- Proof of Bandwidth (PoB)
- Proof of Elapsed Time (PoET)
- Proof of Authority (PoA)

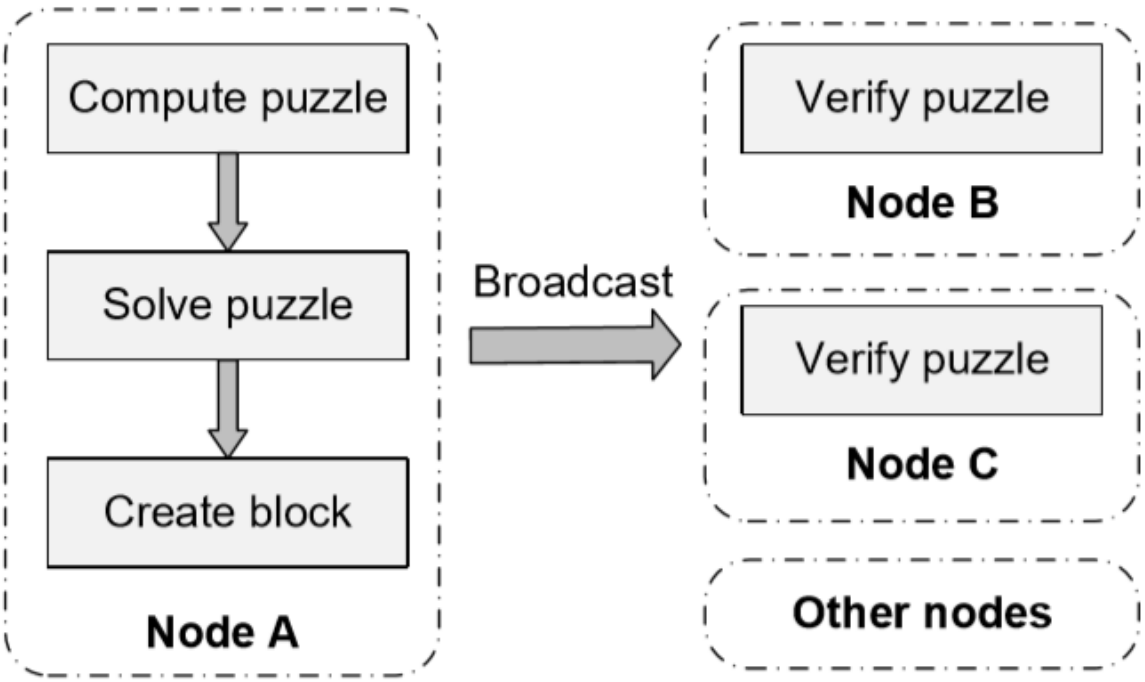
وغيرها من الآليات الأخرى، يجري استخدام PoW من قبل أكثر أنظمة سلسلة الكتل شيوعاً وهي بتكوين وإثريوم، كما تستخدِم إثريوم أيضاً آليةَ PoA، بينما تستخدِم بعضُ العملات الرقمية الأخرى آليةَ PoS مثل عملة PeerCoin وShadowCash وغيرها.

1.6.2- Proof of Work

تقوم آلية PoW على حلّ الألغاز (Puzzles) لإثبات مصداقية (credibility) البيانات [46]، حيث يكون اللغز غالباً صعب الحل حسابياً لكنه سهل من حيث التحقق منه. يجب على العقدة حساب اللغز وحلّه من أجل إنشاء

كتلة جديدة، ثم يجري بثّها للعقد الأخرى لتحقيق الهدف من التوافق كما يبيّن الشكل 2-13. تختلف بنية الكتلة قليلاً في الأنظمة التي تستخدِم سلسلة الكتل كما رأينا في الفقرة 4.2–، فتحوي الكتلة في نظام بتكوين مثلاً على قيمة تهشير الكتلة السابقة (PrevHash أو Parent Block Hash)، الحقل nonce و مناقلات Tx، يجري الحصول على قيمة nonce الصحيحة من خلال حلّ لغز PoW (الفقرة 4.2–)، حيث تضمن تلك القيمة أن تكون قيمة تهشير الكتلة أصغر من Difficulty Target كما توضح المعادلة (2-1)

$$SHA256\left(PrevHash\,||Tx1||Tx2||\ldots..||nonce\right) < Difficulty\ Target \qquad (1\text{-}2)$$



الشكل 2-13 آلية التوافق **PoW**.

Proof of Stake -2.6.2

تستخدِم آليةُ PoS إثباتَ ملكية العملة الرقمية المعمّاة لإثبات مصداقية البيانات، حيث يتوجّب على المستخدمين دفع كمية معيّنة من تلك العملة أثناء عملية إنشاء الكتلة أو المناقلة، فإن جرى في النهاية التأكد من صلاحية الكتلة أو المناقلة، يجري إرجاع العملة إلى العقدة الأصلية كمكافأة وإلّا فسيتمّ تغريم تلك العقدة. تقلّل آلية PoS من مقدار العمليات الحسابية التي تحتاجها بخلاف آلية PoW مما يؤدّي إلى زيادة إنتاجية (throughput) سلسلة الكتل.

7.2- أمن وخصوصية سلسلة الكتل

أصبحت سلسلة الكتل واحدة من أهم التقنيات في صناعة التقانة المالية FinTech (Financial Technology)، مما دعا المستخدمين إلى الاهتمام بالقضايا الأمنية المتعلقة بها، وخصوصاً بعد اكتشاف بعض الثغرات الأمنية في عقود إثريوم الذكية، حيث اكتشفت الدراسة [51] أن 46% من العقود الموجودة هي ضعيفة أمنياً (الفقرة 2.2.1.7.2-)، مما قد يسبب الكثير من الخسائر المالية لمستخدميها. فعلى سبيل المثال، هاجم بعض المهاجمين عقود DAO الذكية في حزيران 2016 من خلال استغلال ثغرة الاستدعاء العودي (recursive calling) وسرقوا حوالي 60 مليون دولار، واستغل مهاجمون آخرون في آذار 2014 قابليةَ تحويل المناقلات في بتكوين لمهاجمة MtGox وهي أكبر منصة لتداول بتكوين وسرقوا عملات بتكوين بقيمة 450 مليون دولار.

سنقدِّم فيما يلي بعض المخاطر الأمنية المحيطة بأنظمة سلسلة الكتل الرائجة، إضافةً إلى الهجمات الأمنية، ثم سنتحدث عن التحسينات الأمنية الموجودة في الأدبيات. سنقسِّم المخاطرَ الأمنية الشائعة على سلسلة الكتل إلى 7 فئات بشكل مشابه لما جاء في [46]، إضافةً إلى الأسباب والنتائج المحتملة لكل خطر، كما هو موضح في الجدول 2-2. سنتحدّث أولاً (الفقرة 1.1.7.2-) عن المخاطر المحيطة بسلسلة الكتل ذات الإصدارَين 1.0 وَ 2.0 التي ترتبط أسبابها غالباً بآلية تشغيل سلسلة الكتل، ثم سنتحدّث في الفقرة 2.1.7.2- عن المخاطر المتعلّقة فقط بسلسلة الكتل 2.0 والتي تنتج غالباً عن تطوير العقود الذكية ونشرها وتنفيذها.

الجدول 2-2 تصنيف المخاطر الأمنية لسلسلة الكتل.

الفقرة	الخطر	سبب الخطر	مجال تأثير الخطر
1.1.1.7.2-	ثغرة 51%	خوارزمية التوافق	سلسلة الكتل 1.0، 2.0
2.1.1.7.2-	أمن المفتاح الخاص	مخطط تعمية المفتاح العام	
3.1.1.7.2-	النشاط الإجرامي	تطبيقات العملة الرقمية المعمّاة	
4.1.1.7.2-	الإنفاق المزدوج	آلية التحقق من المناقلة	
5.1.1.7.2-	ضعف خصوصية المناقلة	خلل في تصميم المناقلة	
1.2.1.7.2-	العقود الذكية الإجرامية	تطبيقات العقود الذكية	سلسلة الكتل 2.0
2.2.1.7.2-	ثغرات في العقود الذكية	خلل في تصميم البرنامج	

1.7.2- المخاطر الأمنية على سلسلة الكتل

1.1.7.2- المخاطر الأمنية الشائعة لسلسلة الكتل 1.0 و2.0

1.1.1.7.2- ثغرة 51% (51% Vulnerability)

تعتمد سلسلة الكتل على آلية التوافق الموزعة (distributed consensus) لبناء الثقة المتبادلة كما رأينا في الفقرة (6.2-)، وتعاني تلك الآلية بحد ذاتها من ثغرة 51% التي يمكن استغلالها من قبل المهاجمين للسيطرة على كامل سلسلة الكتل. **فنجد مثلاً** في السلسلة القائمة على خوارزمية POW، إذا تجاوزت طاقة تهشير عقدة منقِّبة واحدة نسبةَ 50% من إجمالي طاقة التهشير لكامل السلسلة، فباستطاعتها القيام بهجوم 51%. لذا، فإن طاقة التّنقيب المتركّزة في عدد قليل من أحواض (Pools) التنقيب قد تسبّب خطر حدوث حالات طائشة أو غير مقصودة، كأن يتحكم حوض وحيد بأكثر من نصف الطاقة الحاسوبية. وصلَ حوض التنقيب "ghash.io " في كانون الثاني 2014 إلى نسبة 42% من إجمالي طاقة بتكوين الحاسوبية، فانسحب عدد من المنقّبين طوعاً من المجموعة، وأصدرت ghash.io بياناً صحفياً لطمأنة مجتمع بتكوين بأنه سيجري تجنّب الوصول إلى العتبة 51%. **قد يحدث** ذلك الهجوم أيضاً على سلسلة الكتل القائمة على خوارزمية POS إذا كان عدد العملات التي يملكها منقِّب واحد أكثر من 50% من إجمالي السلسلة، مما يمكِّن المهاجم من التعديل والتلاعب بمعلومات سلسلة الكتل اعتباطياً، ويمكِّنه على وجه الخصوص من استغلال تلك الثغرة للقيام بالهجمات التالية:

- عكس المناقلات وبدء هجوم الإنفاق المزدوج.
- إقصاء وتعديل ترتيب المناقلات.
- عرقلة عمليات التنقيب الاعتيادية للمنقِّبين.
- إعاقة عمليات تأكيد المناقلات الاعتيادية.

2.1.1.7.2- أمن المفتاح الخاص Private Key Security

يُعتبَر المفتاح الخاص عند استخدام سلسلة الكتل بمثابة بيانات اعتماد (credential) الهوية والأمن، ويجري إنشاء وإدارة ذلك المفتاح من قبل المستخدم ذاته دون الاعتماد على سلطة خارجية، كأن يقوم المستخدم باستيراد مفتاحه الخاص عند القيام بإنشاء محفظة التخزين في سلسلة كتل البتكوين. أثبتت الدراسة [52] وجودَ ثغرة أمنية في نموذج ECDSA، يقوم المهاجم من خلالها بالحصول على المفتاح الخاص للمستخدم لأنه لا يولد عشوائية كافية أثناء عملية التوقيع الرقمي. عند فقدان المفتاح الخاص للمستخدم أو سرقته، يصبح من الصعب استرداده ويكون حساب المستخدم

الشخصي على سلسلة الكتل عرضةً للتلاعب، كما يصبح من الصعب تتبّع سلوكيات المجرم واستعادة المعلومات المعدَّلة لسلسلة الكتل، وذلك لأن سلسلة الكتل لا تعتمد على مؤسسة مركزية موثوقة لتوزيع المفاتيح.

3.1.1.7.2- النشاط الإجرامي Criminal Activity

يمكن لمستخدم بتكوين أن يملك أكثر من عنوان في بروتوكول بتكوين دون وجود ارتباط بين العنوان والهوية الحقيقية له، مما سهَّل استخدام بتكوين في أنشطة غير شرعية، حيث يمكن للمستخدمين شراء وبيع أي نوع من المنتجات باستخدام منصات بتكوين التجارية دون القدرة على تتبّع سلوكياتهم نظراً لكون العملية مجهولة. تشمل بعض الأنشطة الإجرامية الشائعة في بتكوين ما يلي:

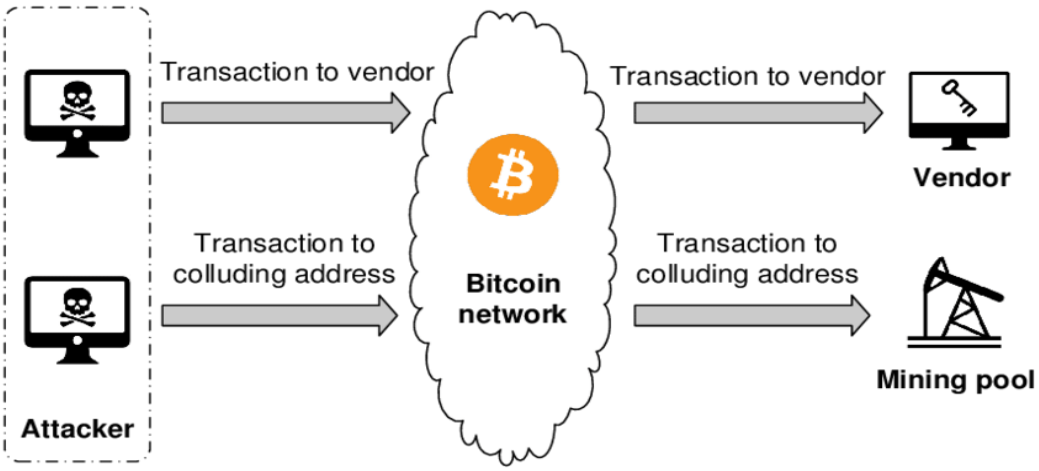
- الفدية Ransomware: هي نوع من البرمجيات الخبيثة، يستخدمها المجرمون في الابتزاز للحصول على الأموال باستخدام بتكوين كعملة تداول. انتشر أحد أنواعها في تموز 2014 باسم CTB-Locker في جميع أنحاء العالم عن طريق التقنّع كمرفقات بريدية، حيث يجري تشغيلها في خلفية النظام عند نقر المستخدم على المرفق وتقوم بتعمية حوالي 114 نوع من كل ملف [53]، يستوجب عندها على الضحية أن تدفع مبلغاً معيناً من بتكوين خلال 96 ساعة وإلّا فلن تكون قادرة على استرجاع ملفّاتها. أصابت فدية أخرى في أيار 2017 باسم WannaCry (أو WannaCrypt) حوالي 230000 ضحية في 150 دولة خلال يومين [54]، وانتشرت بسرعة من خلال استغلال ثغرة في نظام Windows، وقامت بتعمية ملفات الضحايا لطلب فدية بتكوين.

- السوق السرّية Underground Market: يجري غالباً استخدام بتكوين كعملة للتعامل في السوق السرية. فمثلاً، يُعتبَر Silk Road (طريق الحرير) سوقاً دولياً مجهول الهوية يعمل على الانترنت كخدمة Tor مخفية، تنتشر في هذا السوق أغلب العناصر الخاضعة للرقابة الدولية كالمخدرات، ويستخدم بتكوين كعملة للتداول بسبب كون أغلب مناقلاته دولية مما يسهّل عملية التبادل التجاري لكنه يسبّب في نفس الوقت ضراراً كبيراً بالأمن الاجتماعي.

- غسيل الأموال Money Laundering: تُعتبَر بتكوين أقل احتمالاً من غيرها من العملات في خطورة استخدامها في غسيل الأموال، وذلك بسبب تمتّعها بخصائص مثل إخفاء الهوية وشبكة الدفع الافتراضية إضافةً إلى اعتمادها في العديد من بلدان العالم. جرى اقتراح تطبيق المحفظة المظلمة (Dark Wallet)، وهي أحد تطبيقات بتكوين التي تستطيع جعل المناقلة مخفية وخصوصية بشكل كامل من خلال تعميتها ومزج العملات الصحيحة للمستخدم مع عملات وهمية (chaff) مما يصعِّب عملية غسل الأموال.

4.1.1.7.2- الإنفاق المزدوج Double Spending

يَحدُث الإنفاق المزدوج عندما يستخدم المستهلك نفس العملة الرقمية المعماة عدّة مرات للمناقلات، حيث يمكن للمهاجم مثلاً الاستفادة من هجوم السباق (Race Attack[4]) من أجل الإنفاق المزدوج، من السهل نسبياً تنفيذ ذلك النوع من الهجوم في سلسلة الكتل القائمة على خوارزمية POW حيث يمكن للمهاجم استغلال الزمن الفاصل بين إنشاء المناقلة وتأكيدها لشنّ الهجوم بشكل سريع، والحصول على خرج المناقلة الأولى قبل اكتشاف عدم صحة المناقلة الثانية. لايزال من المستحيل تجنّب الإنفاق المزدوج على الرغم من استخدام خوارزميات التوافق للتحقق من صحة المناقلات.



الشكل 2-14 الإنفاق المزدَوج [55].

أجرت الدراسة [55] تحليلاً للإنفاق المزدوج مقابل الدفع السريع في بتكوين، واقترحت نموذج الهجوم كما هو مبيّن في الشكل 2-14، وبفرض أن المهاجم يعرف عنوان البائع قبل تنفيذ الهجوم، الذي يبدأ بإرسال المهاجم مناقلتين معاً وبنفس عملة البتكوين كمدخلات لهما، الأولى تحمل عنوان البائع المستهدَف كمستقبِل والأخرى عنوان تحت سيطرة المهاجم، ينجح الإنفاق المزدوج عندها إذا تحققت الشروط التالية:

- جرت إضافة المناقلة الأولى إلى محفظة البائع المستهدَف.
- جرى تنقيب المناقلة الثانية إلى سلسلة الكتل واعتبارها صالحة.
- حصل المهاجم على نتائج المناقلة الأولى قبل أن يكتشف البائع ذلك النشاط.

[4] عندما يجري إنشاء مناقلتين بنفس الرصيد وفي نفس الوقت، بغية إنفاق ذلك الرصيد مرتين.

سيجري عندها اكتشاف عدم صلاحية المناقلة الأولى، بعد أن يكون المهاجم قد حصل على الخدمة المتاحة من البائع دون أن يدفع أيّة عملة كون العنوان الثاني يعود له.

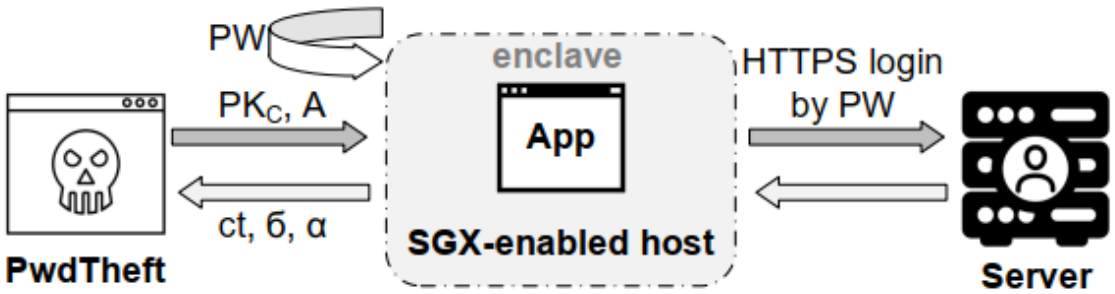
5.1.1.7.2– ضعف خصوصية المناقلة Transaction Privacy Leakage

يمكن تتبّع سلوكيات المستخدمين في أنظمة سلسلة الكتل، لذا، قامت تلك الأنظمة باتخاذ إجراءات لحماية خصوصية مناقلاتهم، فيجري مثلاً في بتكوين وZcash استخدامُ حساب لمرة واحدة لتخزين العملة الرقمية المستلَمة، كما يتوجّب على المستخدم إسناد مفتاح خاص لكل مناقلة، مما يصعّب على المهاجمين عملية استنتاج عائدية المناقلات المتعددة لنفس المستخدم. يمكن لمستخدمي العملة الرقمية Monero تضمين بعض العملات الوهمية (chaff) (تسمى "mixins") عند إنشاء مناقلة كي لا يتمكن المهاجم من استنتاج ارتباط العملات الفعلية التي تنفقها المناقلة. مازالت إجراءات حماية خصوصية سلسلة الكتل ليست قوية كفاية، فقد قدّمت الدراسة [56] تقييماً تجريبياً لآلية التقطيع وأخذ العينات في mixins واكتشفت أن 66.09% من المناقلات الكلية لا تحتوي على أيّ mixins مما يؤدي إلى إضعاف خصوصية مرسِلها. نظراً لاستخدام خرج المناقلة الخالية من المزج كـ mixins، فإنها ستكون قابلة للاستنتاج.

2.1.7.2- مخاطر أمنية متعلّقة بسلسلة الكتل 2.0

1.2.1.7.2– العقود الذكية الإجرامية Criminal Smart Contracts (CSCs)

يمكن للمجرمين الاستفادة من العقود الذكية للقيام بمجموعة متنوعة من النشاطات الخبيثة التي قد تشكّل تهديداً لحياتنا اليومية، مثل تسريب المعلومات السرية، سرقة مفاتيح التعمية والعديد من جرائم العالم الحقيقي. اقترحت الدراسة [57] مثالاً عن نموذج لسرقة كلمة المرور أسمَته CSC PwdTheft الذي يظهر في الشكل 2-15، يمكن استخدام ذلك النموذج لإجراء تبادل عادل (fair exchange) بين المتعهّد C (Contractor) والمجرم P (Perpetrator)، حيث سيدفع المتعهّد مكافأة للمجرم إذا وفقط إذا قدّم الأخير كلمة مرور صالحة للمتعهد دون تدخّل أي وكالات خارجية موثوقة لإتمام المناقلة بشكل كامل. بما أن العقد الذكي القائم على سلسلة الكتل لا يمكنه الوصول إلى الشبكة بشكل مباشر، يجري دمجه مع تقنية العتاد الصلب الموثوقة مثل Intel SGX لإثبات صحة كلمة المرور من خلال HTTPS. ستقوم SGX بإنشاء بيئة تنفيذ موثوقة تسمّى enclave يمكنها حماية التطبيق من التعرّض للهجوم من قبل الآخرين، حيث لا يمكن لأي برنامج بامتيازات معينة الوصول إلى بيئة تشغيل enclave، تستطيع SGX إنشاء quote وهي شهادة موقّعة رقمياً تقوم بالحصول على قيمة تهشير التطبيق الذي يعمل في بيئة enclave وبالتالي الوصول إلى البيانات ذات الصلة أثناء زمن تشغيل التطبيق.



الشكل 2-15 إجرائية **PwdTheft** باستخدام منصة **SGX**.

تجري عملية تبادل كلمة المرور بثلاث خطوات:

1. يقوم نموذج PwdTheft بتوفير pk_c (المفتاح العمومي لِـ C)، والحساب المستهدَف للسرقة A.
2. يقوم التطبيق الذي يجري تشغيله في SGX، باستخدام كلمة المرور (PW) الموفّرة من قبل P، بتسجيل الدخول إلى حساب المخدّم A عن طريق إنشاء اتصال HTTPS.
3. إذا نجحت الخطوات السابقة، فسيجري إرسال البيانات ct ، α، σ إلى نموذج PwdTheft، حيث:

$$ct = enc_{pk_c}[PW]$$

$$\sigma = Sig_{sk_{\text{app}}}[ct]$$

sk_{app} هو المفتاح الخاص لتوقيع التطبيق.

α هي الquote التي يجري تنفيذها على مضيف SGX الخاص بالمجرم P.

بعد تحقق الخطوة الأخيرة وحصول النموذج على قيم ct ، α، σ، يمكن للمتعهد C فك تعميتها للتحقق من البيانات، ثم تحديد ما إذا كان يجب دفع مكافاة لـ P أم لا. لمنع P في هذه العملية من تغيير كلمة المرور بشكل خبيث بعد إرسال البيانات إلى PwdTheft، يمكن إضافة بصمة زمنية إلى البيانات. يمكن إضافةً إلى ما سبق توسعة النموذج المذكور للقيام بأنشطة خبيثة أخرى كالاستفادة من العقود الذكية الإجرامية (CSC) لإنشاء مناقلات بثغرة 0-day[5] التي تعتبَر سلاحاً الكترونياً هاماً.

[5] ثغرة 0-day هي ثغرة أمنية يجري استغلالها من قبل المهاجمين في نفس يوم اكتشافها.

2.2.1.7.2– ثغرات في العقد الذكي Vulnerabilities in Smart Contract

قد تحتوي العقود الذكية على ثغرات أمنية ناتجة عن عيوب في البرامج (Program Defects) التي تعمل في سلسلة الكتل، قدّمت الدراسة [58] تحقيقاً منهجياً (Systematic) لـ 12 نوعاً من نقاط الضعف في العقد الذكي، يوضّح الجدول 2-3 بعضاً منها.

الجدول 2-3 تصنيف الثغرات في العقد الذكي [58].

	الثغرة	السبب	المستوى
1	Call of the unknown	التابع المستَدعى غير موجود	Contract source code
2	Field disclosure	نشر قيمة خاصة وسرية من قبل المنقِّب	
3	Immutable bug	تزوير عقد بعد نشره	EVM bytecode
4	Ether lost	إرسال إثريوم إلى عنوان غير مُسنَد إلى أي مستخدم أو أي عَقْد (orphan address).	
5	Timestamp dependence	جرى تغيير قيمة البصمة الزمنية من قبل أحد المنقِّبين المهاجِمين.	Blockchain mechanism

حيث قامت الدراسة السابقة بتصنيف ثغرات عقود إيثريوم الذكية ضمن ثلاثة أصناف تبعاً للمستوى الذي تقع فيه الثغرة، وأوضَحت أن كل الثغرات المذكورة جرى استغلالها من قبل المهاجمين لسرقة الأموال من العقود الذكية، فمثلاً يستغلّ هجوم DAO (الفقرة 2.2.7.2–) الثغرةَ الأولى في الجدول لسرقة الأموال.

كما اقترحت الدراسة [51] أداة تنفيذ رمزيّة (Symbolic) تدعى Oyente (الفقرة 3.3.7.2–) لإيجاد أربعة أنواع من العيوب (bugs) الأمنية المحتمَلة، واكتشفت الدراسة أن 8833 عقد إيثريوم ذكي مخترق من أصل 19366، يمكننا تلخيص تفاصيل العيوب الأربعة كالتالي:

1. الاعتماد على ترتيب المناقلة Transaction-Ordering Dependence TOD: يمكن للمناقلة الصالحة تغيير حالة سلسلة كتل الإيثريوم من σ إلى $\grave{o}$ (المنقول Transpose)، يقترح كل منقِّب كتلةً خاصة به لتحديث سلسلة الكتل في كل epoch[6]، حيث يمكن أن تتغير حالة سلسلة الكتل (σ) أكثر من مرة خلال الـ epoch. عندما تحتوي كتلة جديدة على مناقلتين T_i، T_j تابعتين لنفس العقد الذكي، فمن الممكن تمكين تلك الثغرة (TOD). يعتمد ترتيب تنفيذ المناقلات بشكل كامل على المنقِّبين. لذا، فإن ترتيب تنفيذ T_i و T_j يؤثر على الحالة النهائية σ للكتلة، حيث أن تنفيذ العقد الذكي مرتبط بحالة سلسلة الكتل مما يجعل عقود TOD عرضة للخطر.
2. الاعتماد على البصمة الزمنية Timestamp dependence: قلنا سابقاً أن كل كتلة في سلسلة الكتل لديها بصمتها الزمنية الخاصة التي يضعها المنقِّب وفقاً لنظامه الزمني المحلي (الجدول 2-1)، وهنالك بعض العقود الذكية التي تعتمد شروطُ تشغيلها على بصمة زمنية معينة، إن استطاع المهاجم تعديلَ البصمة الزمنية فستكون هذه الأنواع من العقود الذكية عرضةً للخطر.
3. Mishandled exceptions: يحدث هذا النوع من نقاط الضعف عندما يجري استدعاء عقود ذكية من عقود ذكية أخرى، فإذا لم يعمل العقد المستدعى بشكل صحيح فإنه سيعطي في خرجه قيمة خاطئة، وإذا لم يتحقق العقد المستدعي من قيمة خرج العقد المستدعَى بشكل صحيح قد تحدث هذه الثغرة.
4. ثغرة Reentrancy: تتغير الحالة الحالية لحساب العقد الذكي بعد استدعائه، وبالتالي يمكن للمهاجم استغلال الحالة الوسيطة لإجراء استدعاءات متكررة للعقد الذكي مما يؤدي أحياناً إلى سرقة عملات الإيثريوم المحتواة في العقد.

2.7.2- الهجمات الأمنية الشائعة لسلسلة الكتل

سنتحدث في هذا القسم عن الهجمات الأمنية الحقيقية على سلسلة الكتل، ونقوم بتحليل الثغرات التي ساعدت على تلك الهجمات.

1.2.7.2- هجوم التّنقيب الأناني Selfish Mining Attack

يجري تنفيذ هذا الهجوم من قبل المنقِّبين الأنانيين بغرض الحصول على مكافآت ليسوا بحاجة لها أو لهدر الطاقة الحسابية للمنقِّبين القانونيين، يحتفظ المهاجم سرياً بالكتلة المكتشَفة ثم يحاول إنشاء **سلسلة خاصة** متفرعة عن السلسلة

[6] كل مجموعة جديدة من الكتل (30000 كتلة) تدعى epoch ويستخدم بها نفس الـ DAG من أجل التنقيب.

الأساسية (العامة)، يقوم المنقِّبون الأنانيون بعدها بالتنقيب في السلسلة المتفرّعة (الشكل 2-9) مع محاولة جعلها أطول من **السلسلة العامة** كونهم يمتلكون عدد أكبر من الكتل المكتشَفة حديثاً، يقوم المنقِّبون القانونيون على التوازي بمواصلة التّنقيب على السلسلة العامة إلى أن يجري الكشف عن الكتل الجديدة المنقَّب عنها من قبل المهاجمين عندما تتقارب السلسلتان بالطول، عندها يكون المنقِّبون القانونين قد هدروا طاقة حسابية دون أيّة مكافأة بسبب تنقيب تلك الكتل من قبل المهاجمين أولاً، وسيُجبر المنقِّبون القانونيون بالانضمام إلى السلسلة الخاصة. يؤثّر هذا الهجوم على الطبيعة اللامركزية لسلسلة الكتل من خلال دمج طاقة التنقيب لصالح المهاجم.

اقترحت الدراسة [59] استراتيجية هجوم تدعى التّنقيب الأناني (Selfish-Mine) التي بإمكانها إجبار المنقِّبين القانونيين على القيام بعمليات حسابية دون جدوى على الفرع العام المهمَل. تكون السلسلتان العامة والخاصة في التّنقيب الأناني متقاربتان في الطول بدايةً، ويشمل ذلك التنقيب الحالات الثلاث التالية:

1. السلسلة العامة أطول من السلسلة الخاصة: سيقوم المنقِّبون الانانيون في هذه الحالة بتحديث السلسلة الخاصة بناءً على السلسلة العامة لأنهم قد لا يتغلبون على المنقِّبين القانونيين بالطاقة الحسابية، ولا يحصلون في هذا السيناريو على أيّة مكافأة.
2. وجدَ المنقِّبون الأنانيّون والقانونيّون أولَ كتلة جديدة بأوقات متقاربة: سيقوم المنقِّبون الأنانيّون في هذه الحالة بنشر الكتلة المكتشَفة حديثاً، وستحوي السلسلة على فرعين متزامنين وبنفس الطول، سيقوم المنقِّبون القانونيون بالتّنقيب على أحد الفرعين بينما يستمر الأنانيون بالتّنقيب على السلسلة الخاصة، سيكون لدينا ثلاث حالات:
   - إذا وجد المنقِّبون الأنانيون الكتلةَ الثانية أولاً، سيقومون بنشرها مباشرةً وسيحصلون بالتالي على مكافآت الكتلتين معاً لأن السلسلة الخاصة أطول من العامة في هذه الحالة وهي السلسلة الصالحة النهائية.
   - إذا وجد المنقِّبون القانونيون الكتلة الثانية أولاً وجرت إضافتها إلى السلسلة الخاصة، فسيربح الأنانيون مكافأة الكتلة الأولى، وسيربح القانونيون مكافأة الكتلة الثانية.
   - إذا وجد المنقِّبون القانونيون الكتلة الثانية وجرت إضافتها إلى السلسلة العامة، سيجنون مكافأتي الكتلتين الأولى والثانية ولن يحصل المنقِّبون الانانيون على أية مكافأة.
3. حصل المنقِّبون الأنانيون على ثاني كتلة جديدة بعد حصولهم على الأولى مباشرةً: سيقومون في هذه الحالة بالاحتفاظ بتلك الكتلتين سرياً، وسيواصلون التنقيب عن كتل جديدة على السلسلة الخاصة. عندما يكتشف المنقِّبون القانونيون أول كتلة جديدة، سيقوم الأنانيون بنشر الكتلة الأولى التي لديهم، وسيجري نفس

السيناريو بالنسبة لثاني كتلة جديدة، وهكذا إلى أن تصبح السلسلة العامة أطول بكتلة واحدة من الخاصة، عندها سينشر الأنانيون آخر كتلة جديدة قبل أن يكتشفها القانونيون، وبالتالي تصبح السلسلة الخاصة هي الصالحة ويكتسب الأنانيون مكافآت كل الكتل المكتشَفة.

2.2.7.2- هجوم DAO

يعتبَر DAO عقداً ذكياً جرى نشره في 28 أيار عام 2016 في إيثريوم، وجرت مهاجمته بعد نشره بـ 20 يوماً فقط، جمعت تلك العقود $150 قبل وقوع الهجوم وهو أكبر تمويل جماعي على الإطلاق. سرق المهاجمون وقتها $60 من خلال استغلال ثغرة Reentrancy (الفقرة 2.2.1.7.2-).

3.2.7.2- هجوم خطف بروتوكول BGP Hijacking Attack BGP

BGP هو بروتوكول توجيه ينظم كيفية إرسال الأطر الشبكية إلى وجهتها الصحيحة، يتلاعب به المهاجمون لاعتراض تدفق المرور الشبكي لسلسلة الكتل. يتطلب اختطاف BGP عادةً التحكمَ بمشغّلي الشبكات لاستغلالها في تأخير الرسائل الشبكية، قامت الدراسة [60] بتحليل شامل لتأثير هجمات التوجيه على مستويي الشبكة والعقد في بتكوين، وأظهرت أن عدد الهجمات الناجحة يعتمد على آلية توزيع طاقة التّنقيب، حيث توجد مركزية عالية في بعض أحواض تنقيب البتكوين، مما يسبّب تأثيراً كبيراً في حال اختطاف BGP بسبب قدرة المهاجمين على تقسيم شبكة البتكوين بشكل فعال أو تأخير سرعة انتشار الكتلة.

يقوم المهاجمون بهجوم خطف BGP لاعتراض الاتصالات بين منقِّبي البتكوين ومخدِّم حوض التّنقيب، وإعادة توجيه كثافة تدفق البيانات إلى حوض تنقيب خاضع لسيطرتهم بغرض سرقة العملة الرقمية المعمّاة من الضحية، حيث جمع هذا الهجوم ما يقارب $83000 من العملة الرقمية في مدّة شهرين. يجب على مشغّلي الشبكات الاعتماد على أنظمة المراقبة التي تقوم بالإبلاغ عن الإعلانات الخبيثة (مثل BGPMon) لأن توسيعات أمن BGP لا يجري نشرها على نطاق واسع. لكن حتى وإن جرى اكتشاف الهجوم، فإن حلّ عملية الاختطاف قد يستغرق ساعات لأنه عملية مُقادة بشرياً تشمل إما تغيير الإعدادات أو فصل المهاجم، فقد استغرقت YouTube على سبيل المثال ما يقارب ثلاث ساعات لحل مشكلة اختطاف البادئات (Prefixes) من قبل مزود خدمة انترنت باكستاني [61].

4.2.7.2- هجوم الكسوف Eclipse Attack

يتمكّن المهاجم من خلال هذا الهجوم من احتكار جميع اتصالات الضحية الواردة والصّادرة، مما يعزلها عن أندادها (Peers) في الشبكة، يستطيع المهاجم بعدها ترشيح معاينة (View) الضحية لسلسلة الكتل، أو ترك الضحية تخسر طاقة حسابية دون جدوى على معاينات مهملة للسلسلة، أو استغلال الطاقة الحسابية للضحية للقيام بأعمال خبيثة.

صنّفت الدراسة [62] هجوم الكسوف على شبكة الند للند في بتكوين إلى نوعين هما هجوم botnet وهجوم البنية التحتية (infrastructure)، حيث جرى إطلاق هجوم botnet بواسطة bots لها مجالات عناوين IP متنوعة، بينما ينمذِج هجوم البنية التحتية الخطر الناتج عن مزود الخدمة ISP، الشركة، أو الدولة التي لها عناوين IP متجاورة. يعتبَر هذه الهجوم أساساً مفيداً لهجمات أخرى كما يبيّن الجدول 2-4، كما يسبّب اضطراباً في شبكة البتكوين إضافةً إلى ترشيح معاينة الضحية لسلسلة الكتل.

الجدول 2-4 بعض الهجمات الناتجة عن هجوم الكسوف.

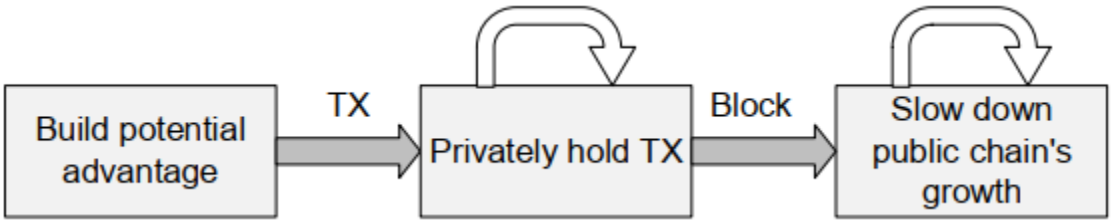
الهجوم	الأذى
سباقات كتلة الهندسة Engineering Block Races	إضاعة طاقة التنقيب على كتل يتيمة
تقسيم طاقة التنقيب splitting Mining Power	تحريض ثغرة 51%
التنقيب الأناني Selfish Mining	حصول المهاجم على مكافآت تنقيب أكثر من الحد الطبيعي
الإنفاق المزدوج دون تأكيد 0-confirmation double spend	عدم حصول البائع على مكافآت مقابل خدمته.
الإنفاق المزدوج بـ N تأكيد N-confirmation double spend	

5.2.7.2- هجوم Liveness

اقترحت الدراسة [63] هجوم liveness القادر على تأخير زمن تأكيد المناقلة قدر الإمكان، وطرحَت مثالين لهذا الهجوم على بتكوين وإيثريوم، يتألّف هذا الهجوم من ثلاث مراحل هي مرحلة التحضير للهجوم، مرحلة رفض المناقلة، ومرحلة تأخير سلسلة الكتل كما يوضّح الشكل 2-16 كالتالي:

1. مرحلة التحضير للهجوم: يجني المهاجم أرباحه اعتماداً على المنقِّبين القانونيين (مثل التّنقيب الأناني، الفقرة 1.2.7.2-) بطريقةٍ ما قبل نشر المناقلة المستهدَفة TX إلى السلسلة العامة، حيث يعمل المهاجم على بناء السلسلة الخاصة التي تعدّ أطول من العامة.
2. مرحلة رفض المناقلة: يحتفظ المهاجم سرياً بالكتلة التي تحوي المناقلة TX لمنع كتابتها في السلسلة العامة.
3. مرحلة تأخير سلسلة الكتل: لن يستطيع المهاجم في زمن معين من عملية بناء السلسلة العامة الإبقاءَ على المناقلة TX لديه بشكل سري، لذا، سيقوم بنشر الكتلة التي تحتويها. يجري في بعض أنظمة سلسلة الكتل

اعتبار TX **صالحة** إذا كان عمق الكتلة التي تحتويها أكبر من طول ثابت، وبالتالي، سيستمرّ المهاجم في بناء السلسلة الخاصة للحصول على فوائد على حساب السلسلة العامة، ثم سيقوم بنشر الكتل التي لديه في السلسلة العامة في الوقت المناسب لإبطاء معدّل نمو السلسلة العامة، وينتهي هجوم liveness عندما يجري التحقق من صحة TX في السلسلة العامة.



الشكل 2-16 مراحل عمل هجوم **Liveness**.

6.2.7.2- هجوم التوازن Balance Attack

يحدث هذا الهجوم ضد سلسلة الكتل القائمة على خوارزمية POW، ويقوم فيه المهاجمون ذوو طاقة التنقيب المنخفضة بتعطيل الاتصالات بين المجموعات الجزئية التي تتمتع بطاقة تنقيب متكافئة [64]. يقوم المهاجم بعد حدوث تأخير بين المجموعات الجزئية المتكافئة بإصدار مناقلات في إحدى تلك المجموعات (تدعى مجموعة الجزئية للمناقلة) والتنقيب عن الكتل في مجموعة جزئية أخرى (تدعى مجموعة جزئية للكتلة)، حتى يضمن تفوّق مجموعة الكتلة على مجموعة المناقلة مما يمكّنه من إعادة توليد الكتل ذات الاحتمال الأكبر أو من القيام بالإنفاق المزدوج.

3.7.2- التحسينات الأمنية في سلسلة الكتل

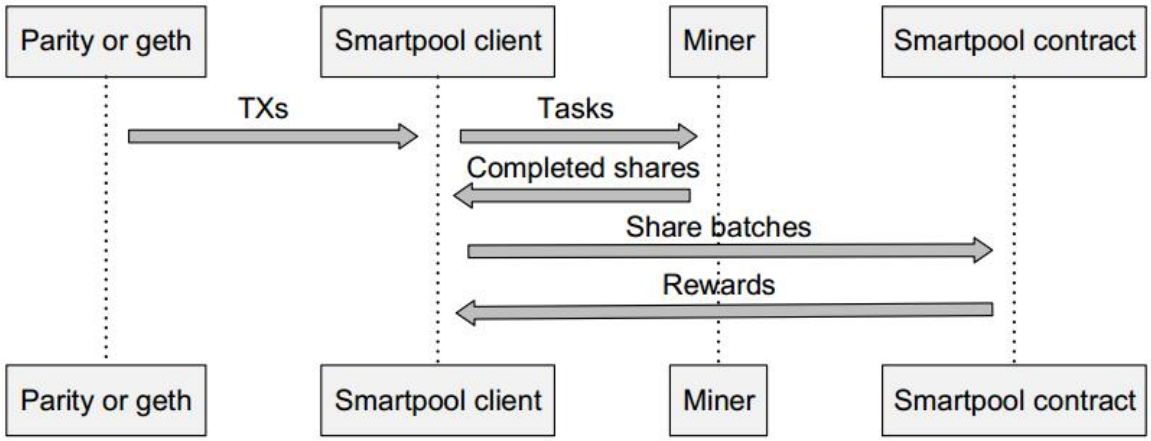
سنلخّص في هذا القسم التحسينات الأمنية لأنظمة سلسلة الكتل، والتي يمكن استخدامها في تطوير تلك الأنظمة.

1.3.7.2- الحوض الذكي SmartPool

قد تتمتّع إحدى أحواض التّنقيب بطاقة تنقيب أكثر من 40% من الطاقة الحسابية الإجمالية لسلسلة الكتل (الفقرة 1.1.1.7.2-)، مما يشكّل تهديداً خطيراً للطبيعة اللامركزية لسلسلة الكتل ويجعلها عرضةً للعديد من الهجمات. اقترحت الدراسة [65] نظاماً جديداً لحوض التنقيب يدعى SmartPool، يوضّح الشكل 2-17 آلية سير عمل ذلك النظام حيث يحصل الحوض الذكي على المناقلات من زبائن (Clients) عقدة الإيثريوم (مثل زبون Parity وزبون geth) التي تحوي على معلومات مهام التّنقيب، ثم يقوم المنقِّب بعمليات التهشير بناءً على تلك المهام ويعيد النتائج المكتمِلة (تدعى Shares) إلى زبون الحوض الذكي ويجري تجميعها إلى أن تصل إلى عدد معين من النتائج ثم

يجري تثبيتها في عقد الحوض الذكي القائم على بيئة إيثريوم، يقوم العقد الذكي بعد ذلك بالتحقق من تلك النتائج ثم يعطي مكافآت للزبون. يتمتّع الحوض الذكي بالخصائص التالية مقارنةً بحوض الند للند التقليدي:

- اللّامركزية: جرى تنجيز نواة (Core) الحوض الذكي بهيئة عقد ذكي قائم على تقنية سلسلة الكتل، يحتاج المنقِّبون أولاً إلى الاتصال بإثريوم من خلال الزبون، وبالتالي، يمكن أن يعتمد حوض التّنقيب في عمله على آلية التوافق الخاصة بالإثريوم مما يضمن الطبيعة اللامركزية لمنقِّبي الحوض، كما يضمن إدارة حوض التّنقيب من قبل الإثريوم دون الحاجة إلى مشغّل للحوض.
- الفعالية: يستطيع المنقِّبون إرسال الـ shares المكتمِلة إلى عقد الحوض الذكي على دفعات (batches)، كما يستطيعون إرسال جزء من الـ shares للتحقق وليس جميعها، مما يجعل الحوض الذكي أكثر فعاليةً من حوض الند للند.
- الأمن: يستخدم الحوض الذكي بنيةَ بياناتٍ جديدة يمكن أن تمنع المهاجم من إعادة تجميع الـ shares في دفعات مختلفة، كما تضمن آلية التحقق المتَّبعة أن يحصل المنقِّبون القانونيون على المكافآت المتوقَّعة حتى مع وجود منقِّبين خبيثين في حوض التّنقيب.

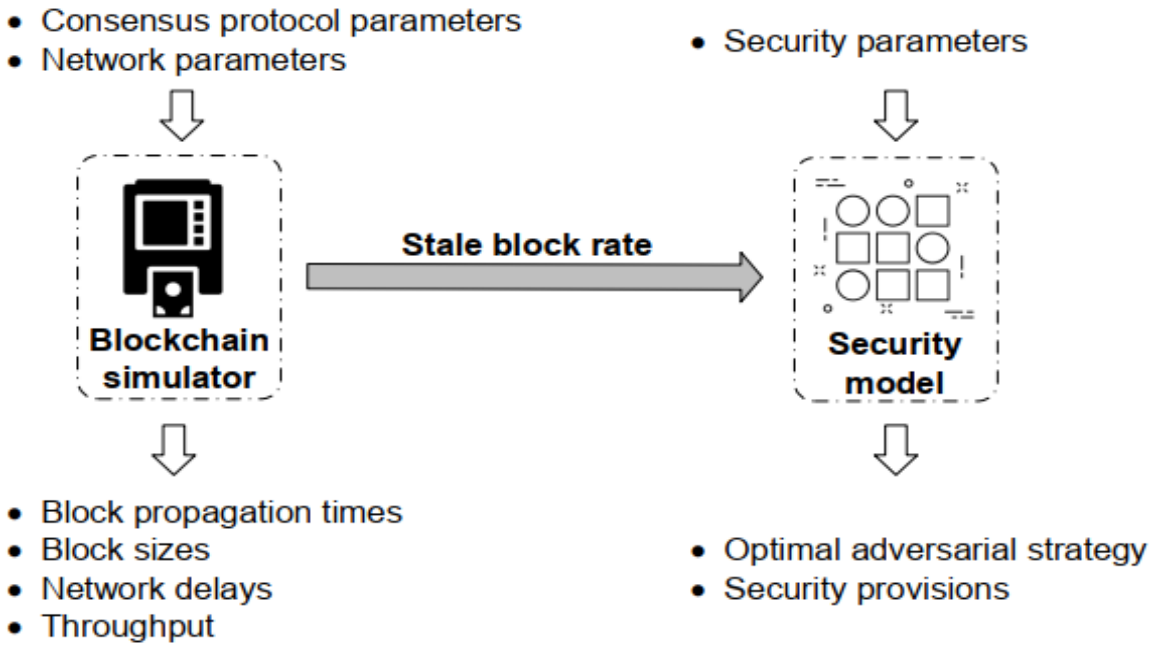


الشكل 2-17 نظرة عامة على إجرائية تنفيذ الحوض الذكي.

2.3.7.2- المنصّة الكمّية Quantitative Framework

اقترحت الدراسة [66] منصةً كمّية لاستخدامها في تحليل أداء تنفيذ سلسلة الكتل القائمة على خوارزمية POW، تحوي المنصة مكوّنين أساسيين كما يوضّح الشكل 2-18 هما محاكي سلسلة الكتل ونموذج أمني. يقوم المحاكي بتقليد عملية تنفيذ وتشغيل سلسلة الكتل ويأخذ محدّدات بروتوكول التوافق والشبكة كدخلٍ له، ويعطي في خرجه إحصائيات أداءٍ لسلسلة الكتل المستهدَفة بما فيها أزمنة انتشار الكتلة، أحجام الكتل، التأخيرات الشبكي، معدّل الكتل البالية (stale) ومعدّل الإنتاجيّة (throughput) الخ. تشير الكتل البالية إلى الكتل التي جرى التنقيب عنها لكنها لم تُكتَب

على السلسلة العامة، بينما يعبّر معدّل الإنتاجية عن عدد المناقلات التي يمكن لسلسلة الكتل التعامل معها خلال ثانية واحدة، ويجري إدخال معدّل الكتل البالية إلى النموذج الأمني القائم على إجرائيات ماركوف لاتخاذ القرار (MDP) لتجنّب هجومَي الإنفاق المزدوج والتّنقيب الأناني. نستنتج أخيراً أن المنصّة المصمّمة حصينة ضد الهجمات الأمنية وتسهّل بناء القواعد الأمنية لسلسلة الكتل حيث يوجد تفاضل مستمر بين أداء سلسلة الكتل والمتطلبات الأمنية.



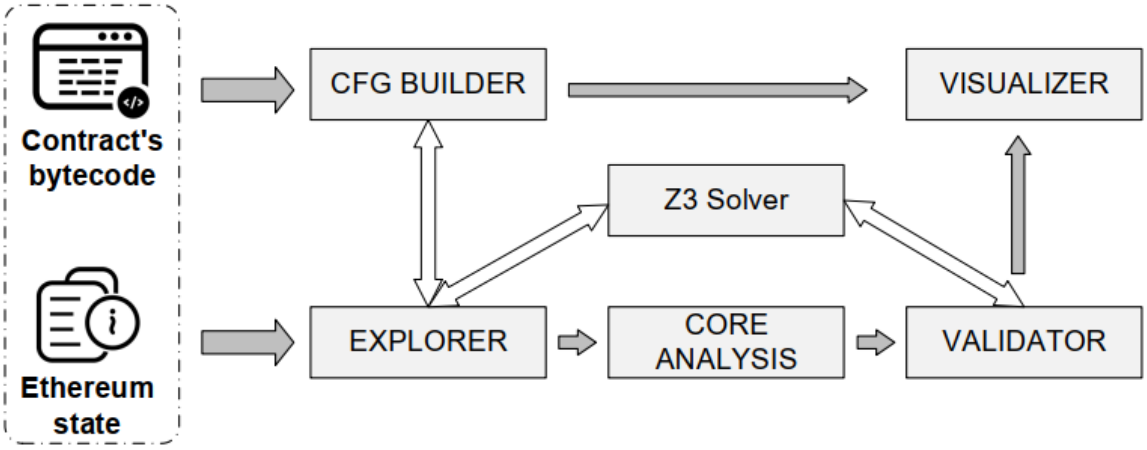
الشكل 2-18 مكوّنات المنصّة الذكية.

Oyente -3.3.7.2

اقترحت الدراسة [51] الأداةَ Oyente مفتوحة المصدر للكشف عن عيوب عقود إثريوم الذكية، تُجري تلك الأداة تنفيذ رمزيّ (Symbolic) لتحليل الرّماز الثماني (Bytecode) للعقود الذكية وتتّبع نموذج التنفيذ الخاص بـ EVM، كما تستطيع كشف العيوب في العقود المنشورة (deployed) نظراً لأن إثريوم تخزن الرماز الثماني للعقود الذكية في سلسلة الكتل الخاصة بها. يوضّح الشكل 2-19 بنية الأداة المقترَحة وإجرائية تنفيذها، حيث تأخذ في دخلها الرمازَ الثماني للعقد الذكي والحالة العالمية للإثريوم (Ethereum Global State)[7]، يقوم أولاً باني CFG ببناء الـ CFG الخاص بالعقد الذكي، ثم يقوم المستكشِف (EXPLORER) بمحاكاة تنفيذ العقد الذكي بناءً على حالة الإثريوم ومعلومات الـ CFG وبالاستفادة من التنفيذ الرمزي. تستخدِم وحدة CORE ANALYSIS خوارزميات التحليل

[7] Global or world state: تعبر عن مقابلة (mapping) بين العناوين (الحسابات) وحالات الحساب، وهي لا تخزَّن في سلسلة الكتل وإنما في ملف تعريفي tier يُحدَّث عند كل تنفيذ للمناقلة، ويحوي كل المعلومات عن حسابات إثريوم [85].

المختصّة لكشف أربعة أنواع من الثغرات (كما ذكرنا في الفقرة 2.2.1.7.2-)، وتقوم وحدة VALIDATOR بالتحقق من الثغرات المكتشَفة والمسارات غير الآمنة، يجري في النهاية تحويل الثغرات الأمنية المؤكَّدة ومعلومات CFG إلى وحدة VISUALIZER التي يستفيد منها المستخدمون في تصحيح الأخطاء وتحليل البرامج.



الشكل 2-19 بنية وسير عمل منصة **Oyente**.

4.3.7.2- الصّقر Hawk

يمثِّل تسرُّب الخصوصية تهديداً خطيراً لسلسلة الكتل (كما وضّحنا في الفقرة 5.1.1.7.2-)، فمثلاً لا تقتصر العلنيّة في سلسلة الكتل 2.0 على المناقلات فحسب، وإنما على المعلومات المتعلقة بالعقود مثل الرّماز الثماني للعقود الخ ..

اقترحت الدراسة [67] منصة جديدة تدعى Hawk لتطوير عقود ذكية للحفاظ على الخصوصية، يستطيع المطوّرون باستخدام تلك المنصة كتابةَ عقود ذكية خاصة دون الحاجة إلى تعمية الرماز (code) أو استخدام تقنيات التشويش، كما لن يجري تخزين معلومات المناقلات المالية بوضوح في سلسلة الكتل. يمكن تقسيم العقد إلى قسمين أثناء تطويره برمجياً: الجزء الخاص والجزء العام، حيث يحتوي الجزء الخاص على المعلومات السرية الخاصة والرّمازات البرمجية المتعلقة بالتوابع المالية، بينما تجري كتابة الرمازات البرمجية التي لا تحوي معلومات خاصة في الجزء العام. يجري تصريف (compile) عقد Hawk في ثلاثة أجزاء:

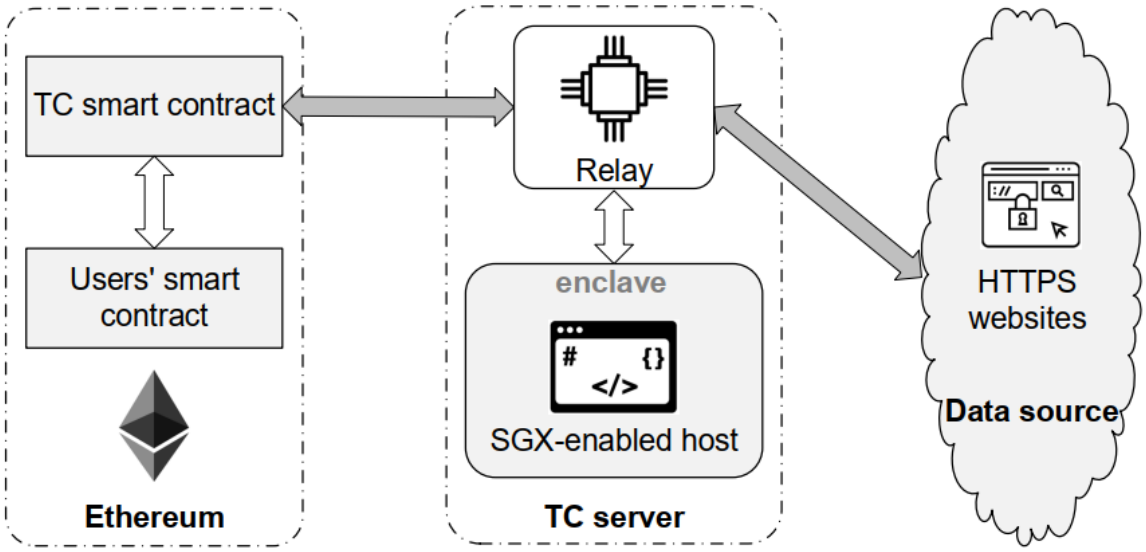
1. البرنامج الذي سيجري تنفيذه في جميع الآلات الافتراضية (VMs) للعقد، بشكل مشابه للعقود الذكية في إثريوم.
2. البرنامج الذي سيجري تنفيذه فقط من قبل مستخدمي العقود الذكية.
3. البرنامج الذي سيجري تنفيذه من قبل المدير (Manager)، وهو طرف خاص موثوق في Hawk، يجري تنفيذه في بيئة تشغيل إنتل SGX (الفقرة 1.2.1.7.2-)، ويمكنه الاطلاع على المعلومات الخصوصية

للعقد دون الإشهار بها، وإذا ألغى المدير بروتوكول Hawk فستجري معاقبته مالياً بشكل أوتوماتيكي إضافةً إلى تعويض المستخدمين.

تستطيع المنصة المذكورة (Hawk) حماية الخصوصية بين عقود Hawk المختلفة ايضاً، إضافةً إلى حماية الخصوصية أمام العموم، فهي بالتالي تستطيع حماية خصوصية المستخدمين إلى حدٍّ كبير عند استخدامهم لسلسلة الكتل.

5.3.7.2- مؤذّن البلدة Town Crier TC

يتطلّب العقد الذكي غالباً التفاعل مع مصدر بيانات يقع خارج سلسلة الكتل، ولا تستطيع تلك العقود الحصول على البيانات عبر بروتوكول HTTPS نظراً لأن تلك العقود منشورة (deployed) في سلسلة الكتل. لذا، جرى اقتراح نظام TC [68]، وهو نظام تغذية بيانات مصادَق (authenticated) مخصّص لإجرائية تفاعل البيانات، يعمل كجسر بين مصدر البيانات القائم على بروتوكول HTTPS والعقود الذكية كما يوضح الشكل 2-20.



الشكل 2-20 البنية الأساسية لنظام **TC**.

كما يظهِر الشكل 2-20 أيضاً البنيةَ الأساسية للنظام المقترَح، يمثِّل عقد TC الطرفَ الأمامي (Front End) لنظام TC، ويعمل ذلك العقد كواجهة برمجية للتطبيقات API بين عقود المستخدمين ومخدِّم TC. يجري تشغيل برنامج النواة لـ TC في بيئة تشغيل إنتل SGX (الفقرة 1.2.1.7.2-)، وتتمثّل الوظيفة الرئيسية لمخدِّم TC في الحصول على طلبات البيانات (data requests) من عقود المستخدمين، والحصول على البيانات من الواقع الالكترونية المستهدَفة التي تدعم HTTPS، ويعيد في النهاية برقية معطيات (datagram) إلى عقود المستخدمين بصيغة رسائل موقعة رقمياً لسلسلة كتل.

8.2- خاتمة

قدّمنا في هذا الفصل دراسةً نظرية عن تقنية سلسلة الكتل التي بدأت في العملة الرقمية بتكوين وتستخدَم حالياً في العقود الذكية، كما تحدّثنا عن بنيتها وأنواعها وآلية عملها واستخدامها في العديد من مجالات الحياة. تطرّقنا أيضاً إلى بعض الأساسيات التي تستخدِمها تلك الكتلة مثل توابع التهشير. ثم انتقلنا إلى أمن وخصوصية سلسلة الكتل، حيث تطرّقنا إلى بعض الأخطار والهجمات الأمنية التي تهدّدها وأرفقنا ذلك بآخِر وأحدث الحلول الأمنية في الأدبيات، لننتقل في الفصل التالي إلى أحد أهم تطبيقات سلسلة الكتل وهو استخدامها في تحسين أمن وخصوصية انترنت الأشياء وإمكانية تكامل هذه التقنية مع أنظمة انترنت الأشياء والتحديات التي تواجهها.

الفصل الثالث

الدراسة المرجعية

نبين في هذا الفصل أحدث وأهم الدراسات التي اعتمدت على سلسلة الكتل في تأمين انترنت الأشياء، كما سنعرض أهم التحديات الموافقة لذلك التكامل بين سلسلة الكتل وانترنت الأشياء.

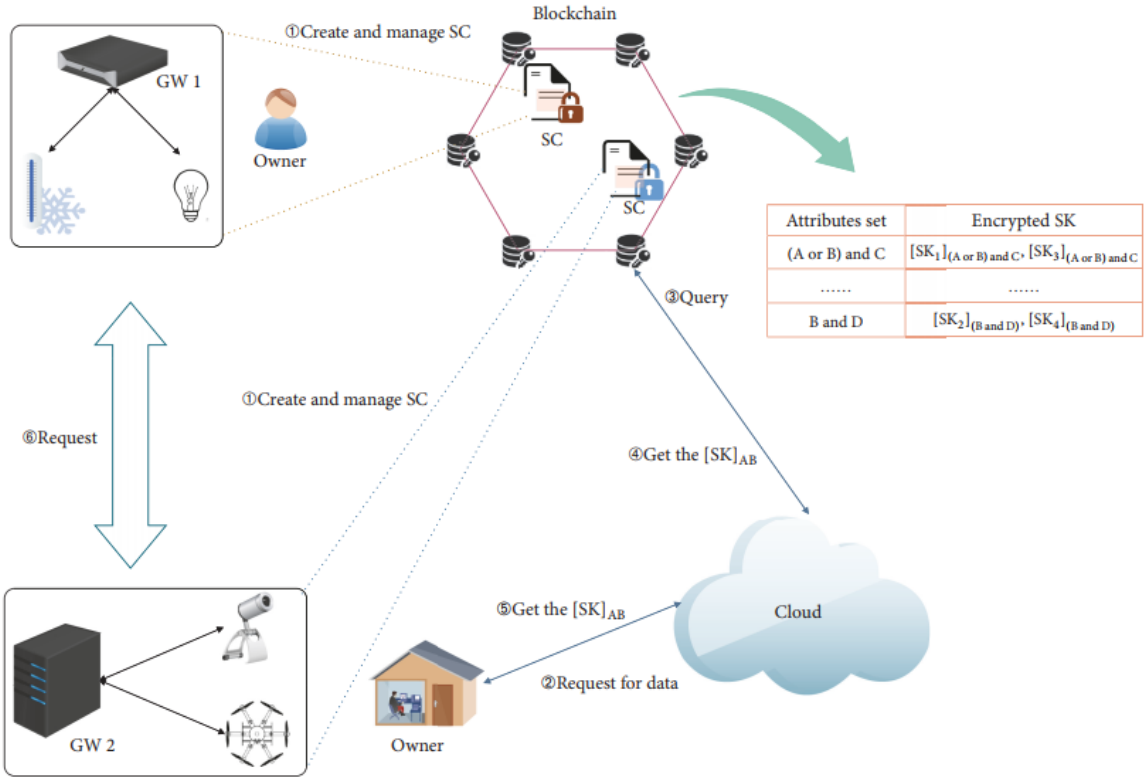
1.3- مقدمة

يتزايد عدد تجهيزات انترنت الأشياء بشكل دائم مما يزيد من كمية بياناتها المنتشِرة عبر الانترنت، قد تحوي تلك البيانات على معلومات حساسة بالنسبة للمستخدمين، وستصبح عرضة للهجمات الالكترونية. كما أن عقد انترنت الأشياء محدودة الطاقة والقدرة الحسابية (كما رأينا في الفقرة 1.6.1-) ويجب أن توجّه معظم طاقتها للقيام بالوظائف الأساسية المطلوبة منها، لا أن تهدرها في حماية نفسها وبياناتها من الهجمات، لذا، فإن الحلول الأمنية التقليدية غير ملائمة في أنظمة انترنت الأشياء فضلاً عن كون معظم تلك الحلول مصمّمة للشبكات المركزية بينما تعتبَر أنظمة انترنت الأشياء لا مركزية. مما دفع الباحثين إلى التفكير في استخدام تقنية سلسلة الكتل التي تتمتع بصفات وميزات رأيناها في الفقرة (2.2-) تجعلها قادرة على توفير حلول الأمن والخصوصية لإنترنت الأشياء، كما تساعِد تقنية سلسلة الكتل على تطبيق مستويات مختلفة من التحكم بالوصول لتقييد العمليات غير المخوّلة بالوصول إلى بيانات أجهزة انترنت الأشياء. سنقدّم فيما يلي آخر وأهم الدراسات البحثية التي استخدمت سلسلة الكتل لتأمين انترنت الأشياء وسنقوم بمناقشتها ثم سنتحدّث عن أهم التحديات التي تترافق مع تكامل تقنية سلسلة الكتل مع أنظمة انترنت الأشياء.

2.3- أحدث الدراسات التي استخدمت سلسلة الكتل في انترنت الأشياء

بعد أن ظهرت مشكلات الأمن والخصوصية في انترنت الأشياء بسبب نموّها العالمي والزيادة المستمرّة في البيانات الناتجة عن العقد، بدأ العديد من الباحثين في الأوساط الأكاديمية والصناعية بإظهار فعالية سلسلة الكتل في حماية أمن وخصوصية انترنت الأشياء، سنعرض فيما يلي أبرز الدراسات المنجَزة التي يلخّصها الجدول 3-1:

- طرح المؤلّفون في [69] بنية آمنة (BaDS) لمشاركة بيانات انترنت الأشياء في السحابة مع نظام تحكم بالوصول قائم على الواصفات، يتألف نموذج الشبكة المقترَح من أربعة مكونات أساسية هي أجهزة انترنت الأشياء، مالك البيانات، شبكة سلسلة الكتل ومنصة الحوسبة السحابية (الشكل 3-1). يجري في تلك البنية اعتماد نموذج سلسلة الكتل المعرَّف بالصلاحيات لإدارة مناقلات انترنت الأشياء والتحكم بالطلبات التي تتلقّاها السحابة للوصول إلى الأجهزة، بينما تراقب السحابةُ شبكةَ سلسلة الكتل بدقة. أظهرَت النتائج قدرةَ البنية المقترَحة على حماية الخصوصية، التحكم الذاتي للمستخدم بالوصول إلى البيانات المشاركة، واللامركزية من خلال استخدام سلسلة الكتل والعديد من الأنظمة المعمّاة (cryptosystem)، وفّر استخدام التوقيع القائم على الواصفات (ABS) واستخدام CP-ABE القدرةَ على التحكم بالوصول، كما جرى تحليل أداء تلك البنية من حيث متطلبات الأمن الأساسية (السرية، السلامة والتوافرية) ومن حيث تقليل العمليات الحسابية.



الشكل 3-1 مشارَكة بيانات **IoT** من خلال بنية **BaDS**.

- اقترحت الدراسة [70] نموذجاً جمع بين تقنية سلسلة الكتل والتعمية القائمة على الواصفات، وجرى تطبيقه لحماية الخصوصية في أنظمة انترنت الأشياء البيولوجية (ecosystem)، يتكوّن النموذج من أربعة أطراف هي مدير العنقود (Cluster Head CH)، منفّذي سلسلة الكتل (blockchain miners)، سلطات

الواصفات (attribute authorities)، ودفتر الحسابات الموزّع (distributed ledger). حيث يستخدِم CH خوارزميةَ ABE لتعمية البيانات لكي يتمكّن المستخدمون ذوو الواصفات المحدّدة من الوصول إلى تلك البيانات، وتقوم سلطات الواصفات بإصدار credentials للمنقّبين والمستخدمين، لكن لاتزال مشكلة ABE موجودة وهي عدم القدرة على الإلغاء التلقائي لواصفات ومفاتيح المستخدمين.

- ناقشت الدراسة [71] مقارباتٍ لا مركزية لأمن وخصوصية انترنت الأشياء في المنزل الذكي، حيث اقترح المؤلّفون منصّة LSB قائمة على تقنية سلسلة الكتل المعدّلة من قبلهم، وجرى تحليل أداء تلك المنصة من حيث متطلبات الأمن الأساسية، كما أظهرت نتائج المحاكاة فعالية النموذج المقترح في حالة المنزل الذكي.
- جرى في الدراسة [72] اقتراح نموذج شبكة آمنة متعدّدة المستويات قائم على تقنية سلسلة الكتل، قام النموذج المقترح بتقليل التعقيد والعمليات الحسابية لاستخدام تقنية سلسلة الكتل في أنظمة انترنت الأشياء من خلال تقسيمها إلى شبكة لا مركزية متعددة المستويات.
- قام المؤلّفون في [73] بالتحقيق والبحث في إمكانيّة سلسلة الكتل في توزيع معلومات أنظمة انترنت الأشياء، جرى في الدراسة تسليط الضوء على متطلّبات الأمن الأساسية وكيف يمكن لسلسلة الكتل أن تساعد في معالجة تلك المتطلّبات، كما جرى طرح تصميم لتوزيع المعلومات في أنظمة انترنت الأشياء وتحليل كيفية جعل مخططات الأمن الحالية أكثر قوة باستخدام تقنية سلسلة الكتل.
- سلَّط المؤلفون في [74] الضّوءَ على العديد من القضايا الأمنية مثل السلامة، إخفاء الهوية، والتكيّف (adaptability) لإدارة البيانات في أنظمة انترنت الأشياء، وقاموا بمناقشة العديد من حالات استخدام تقنية سلسلة الكتل لمعالجة تلك القضايا، وجرت الإشارة إلى العديد من المشكلات البحثية المفتوحة لتلك القضايا.
- عرضَت الدّراسة [75] لمحة موجزة عن استخدام تقنية سلسلة الكتل في أنظمة انترنت الأشياء، وناقشت إمكانية تقنية سلسلة الكتل في معالجة التحديات المختلفة المرتبطة بأنظمة انترنت الأشياء بما في ذلك التكلفة، قابلية التوسع، البنية الضعيفة، وتوافرية المخدّمات السحابية، وجرى التأكيد على قدرة سلسلة الكتل في تحسين الأمن العام لأنظمة انترنت الأشياء.
- قامت الدّراسة [76] بتصميم نظام تتبّع لسلسلة الإمداد الغذائي استناداً إلى تحليل المخاطر ونقط التحكم الحرجة (HACCP)، سلسلة الكتل وانترنت الأشياء، بهدف توفير منصة لأعضاء سلسلة الإمداد بشكل آمن وشفاف وموثوق، كما جرى تقديم فكرة جديدة للأنظمة اللامركزية واسعة النطاق تسمى BigchainDB، إضافةً إلى مناقشة التحدّيات المرتبطة بالاستخدام المستقبلي لتقنية سلسلة الكتل في نظام التتبّع المتقدّم لسلسلة الإمداد الغذائي.

- اقترحت الدراسة [77] نموذجَ انترنت الأشياء الذكية (IoST) عن طريق إضافة ميّزات تستند إلى الذكاء الصنعي، حيث تستخدمُ IoST بروتوكولَ سلسلة الكتل القائم على الصلاحيات (permission-based) الذي يدعى Multichain للاتصال الآمن بين الأشياء الذكية وذلك بسبب انخفاض تكلفة الاتصال في ذلك البروتوكول.
- اقترحَت الدراسة [78] بنية خفيفة قائمة على تقنية سلسلة الكتل من أجل أنظمة انترنت الأشياء، يمكن أن تقلّل البنية المقترَحة من الحمل الزائد لمخططات سلسلة الكتل التقليدية مع توفير نفس المستوى من الأمن والخصوصية، قامت الدراسة بالتحقق من صلاحية البنية المقترَحة في بيئة المنزل الذكي لتسليط الضوء على فعاليتها، فتبيّن من نتائج المحاكاة أن الحل المقترح يمكن أن يؤدي إلى انخفاض كبير في الحمل الزائد للطرود والمعالجة مقارنةً مع الحلول التقليدية لسلسلة الكتل.

الجدول 3-1 أحدث الدراسات التي استخدمت سلسلة الكتل لتأمين IoT.

المرجع	العام	الهدف	الحل المقترح	ملاحظات
[69]	2018	حماية خصوصية بيانات انترنت الأشياء المشارَكة على السحابة	تقديم نموذج آمن لمشاركة البيانات في السحابة باستخدام التعمية القائمة على الواصفات وسلسلة الكتل يدعى BaDS، لحفظ خصوصية البيانات وضمان تحكّم المستخدم بالوصول إلى بياناته المشارَكة	أحدثَ التكامل بين انترنت الأشياء وسلسلة الكتل إطاراً أمنياً شاملاً للحفاظ على خصوصية البيانات وملكيتها ومشاركتِها بشكل آمن.
[70]	2017	حماية السرية والخصوصية في الأنظمة البيولوجية لإنترنت الأشياء	تقديم نموذج لحماية الخصوصية اعتماداً على سلسلة الكتل والتعمية القائمة على الواصفات	جرى تقديم بنية جديدة لسلسلة الكتل لحماية خصوصية المناقلات باستخدام التعمية

				القائمة على الواصفات، وجرى تحليل أمن وخصوصية النموذج المقترح تجاه عدد من الهجمات الأمنية المعروفة، كما جرى استنتاج فعالية استخدام سلسلة الكتل في انترنت الأشياء والاستفادة من التعمية القائمة على الواصفات لتخفيف التعقيدات الحسابية.
[71]	2017	توفير نموذج موزّع للأمن والخصوصية في المنازل الذكية	مخطط سلسلة كتل معدَّل للمنازل الذكية	جرى تحليل المخطط المقترَح من حيث المتطلبات الأمنية الأساسية (السرية، السلامة، التوافرية)
[72]	2017	تقليل التعقيد الحسابي لاستخدام سلسلة الكتل في انترنت الأشياء	قسّم المؤلّفون أنظمة انترنت الأشياء إلى شبكة لا مركزية متعدّدة المستويات تعتمد على تقنية سلسلة الكتل	تعتبَر الشبكة المقترَحة حلّاً ملائماً لتأمين انترنت الأشياء
[73]	2017	البحث في إمكانية سلسلة الكتل لتوزيع	تقديم تصميم لتحليل إمكانية جعل نماذج	ناقش المؤلفون كيف يمكن تلبية متطلبات

		المعلومات في أنظمة انترنت الأشياء	الأمن الحالية أكثر قوةً مع استخدام تقنية سلسلة الكتل	الأمن الرئيسية من خلال استخدام تقنية سلسلة الكتل
[74]	2017	توفير مراجعة أدبية بحثية لاستخدام سلسلة الكتل في انترنت الأشياء	جرى مناقشة العديد من حالات استخدام سلسلة الكتل لمعالجة أهم القضايا الأمنية والقضايا البحثية المفتوحة في انترنت الأشياء	جرى أخذ ثلاث معاملات بعين الاعتبار وهي: السلامة، إخفاء الهوية، ولتكيّف (adaptability)
[75]	2017	دراسة جدوى استخدام سلسلة الكتل في انترنت الأشياء	جرى تسليط الضوء على التحدّيات المختلفة في انترنت الأشياء وتقديم حلول لتلك التحديات باستخدام تقنية سلسلة الكتل	جرى التأكيد بشكل عام على قدرة سلسلة الكتل على تحسين الأمن في انترنت الأشياء
[76]	2017	تصميم وتطوير نظام تتبّع سلسلة توريد غذائي، لتوفير منصة آمنة وموثوقة لأعضاء تلك السلسلة	اقترح المؤلفون نظام تتبّع سلسلة الإمداد الغذائي القائم على HACCP، سلسلة الكتل وانترنت الأشياء	جرت مناقشة التحديات المرتبطة بالاستخدام المستقبلي لتقنية سلسلة الكتل في نظام التتبع المتقدّم لسلسلة الإمداد الغذائية
[77]	2017	تصميم وتطوير انترنت الأشياء الذكية	استخدم المؤلفون سلسلة الكتل القائمة	يوفّر بروتوكول Multichain تكلفة

		(IoST)، واستخدام تقنية سلسلة الكتل لتأمين الاتصال	على الصلاحية (permission-based) والتي تدعى Multichain لتأمين الاتصال بين الأشياء الذكية	اتصال منخفضة وهو اختيار مناسب لحلول انترنت الأشياء
[78]	2017	تطوير بنية خفيفة قائمة على تقنية سلسلة الكتل من أجل أنظمة انترنت الأشياء	جرى التحقق من صلاحية البنية المقترحة لحالة استخدام المنزل الذكي	توفّر البنية المقترحة حمل أقل من حيث الطرود والمعالجة

3.3- التحدّيات الموافقة لاستخدام سلسلة الكتل في أنظمة IoT:

تتزامن الميّزات الجديدة التي توفّرها سلسلة الكتل لإنترنت الأشياء مع بعض التحديات التي تتعلّق إما بالنّشر (deployment) الآمن لإنترنت الأشياء أو بالتوافق بين سلسلة الكتل وانترنت الأشياء، حيث تشمل بعض التحديات المتعلّقة بالنشر الآمن لإنترنت الأشياء ما يلي:

- تأمين عقد IoT المنتشِرة.
- أنظمة انترنت الأشياء مجزّأة (fragmented) بشكل كبير، ومؤلّفة من مجموعة كبيرة من البروتوكولات وتقنيات الاتصال، مما يزيد صعوبة تحديات الأمن والخصوصية كما يزيد الحاجة إلى التوحيد المعياري بين كل تلك البروتوكولات والتقنيات للحصول على توافق بينها مما سيقلّل بالتأكيد من تعقيد أنظمة انترنت الأشياء.
- يمكن الوصول بشكل فيزيائي إلى عقد IoT في بعض التطبيقات مما يجعلها عرضة للهجمات الفيزيائية.
- يمكن لعقد IoT الانضمام إلى الشبكة أو مغادرتها حسب التطبيق، مما يتطلّب بروتوكول مصادقة خفيف وآمن لتأمين الاتصال.
- يجب ضمان حد أدنى من الأمن والخصوصية من أجل النشر العالمي لأنظمة انترنت الأشياء.

بينما تشمل التحديات المتعلّقة باستخدام تقنية سلسلة الكتل في أنظمة انترنت الأشياء ما يلي:

- قابليّة التوسّع: من المهم اختبار التنجيزات الحالية لسلسلة الكتل وتصميم تنجيزات جديدة لأنظمة IoT المتوسّعة بشكل دائم.
- بُنى ومخططات خفيفة: تصميم وتطوير بنى خفيفة قائمة على سلسلة الكتل من أجل أنظمة انترنت الأشياء مهم جداً لتقليص الحمل الزائد المرافق لتقنيات سلسلة الكتل التقليدية مع ضمان الحصول على نفس المستوى من الأمن والخصوصية.
- الطاقة الحسابية: تتنوّع أنظمة انترنت الأشياء وتنتشر بشكل واسع مع عدد كبير من العقد، مما يصعِّب عملياً القيام بآليات التعمية من قبل جميع العقد، لذا، لابد من ابتكار آليات جديدة وخفيفة للقيام بالتعمية من قبل مجموعة محدّدة من العقد.
- التخزين: تحتاج عقد IoT إلى تخزين بياناتها المتزايدة مع مرور الزمن وهي غير قادرة على تخزين كميات كبيرة من البيانات، لذا تستفيد أنظمة IoT من البنية الموزّعة لسلسلة الكتل من أجل تخزين بياناتها.
- التصميم الأمثلي: يجب تصميم نظام IoT أمثلي يعتمد على خصائص الأمن والخصوصية التي توفرها تقنية انترنت الأشياء.
- القضايا التشريعية: تختلف معايير الأمن والخصوصية تبعاً للبلد والمنطقة، مما يشكِّل تحدّياً كبيراً للتكيّف الناجح لتقنية سلسلة الكتل في أنظمة انترنت الأشياء، وهذا يستدعي منصة معيارية يستخدمها المصنّعون لتوفير حلول الأمن والخصوصية.

4.3- خاتمة

قدّمنا في هذا الفصل مناقشة واسعة للدراسات التي عملت على توظيف تقنية سلسلة الكتل في تحسين أمن وخصوصية أنظمة انترنت الأشياء، حيث يمثّل الأمن والخصوصية قضايا هامة جداً لنجاح تلك الأنظمة. كما قمنا بتعريف التحدّيات الرئيسية المتعلّقة بنشر انترنت الأشياء واعتمادها عالمياً، إضافةً إلى التحديات المرتبطة باستخدام سلسلة الكتل في انترنت الأشياء، واستنتجنا وجود العديد من القضايا التي مازالت تحتاج إلى البحث والتطوير على الرغم من كثافة الأبحاث حول هذا الموضوع في العامين الماضيين مثل الحاجة إلى استخدام مخططات خفيفة من سلسلة الكتل لتتناسب مع الصفات المميّزة لإنترنت الأشياء (الجدول 3-1).

الفصل الرابع

النموذج المقترح

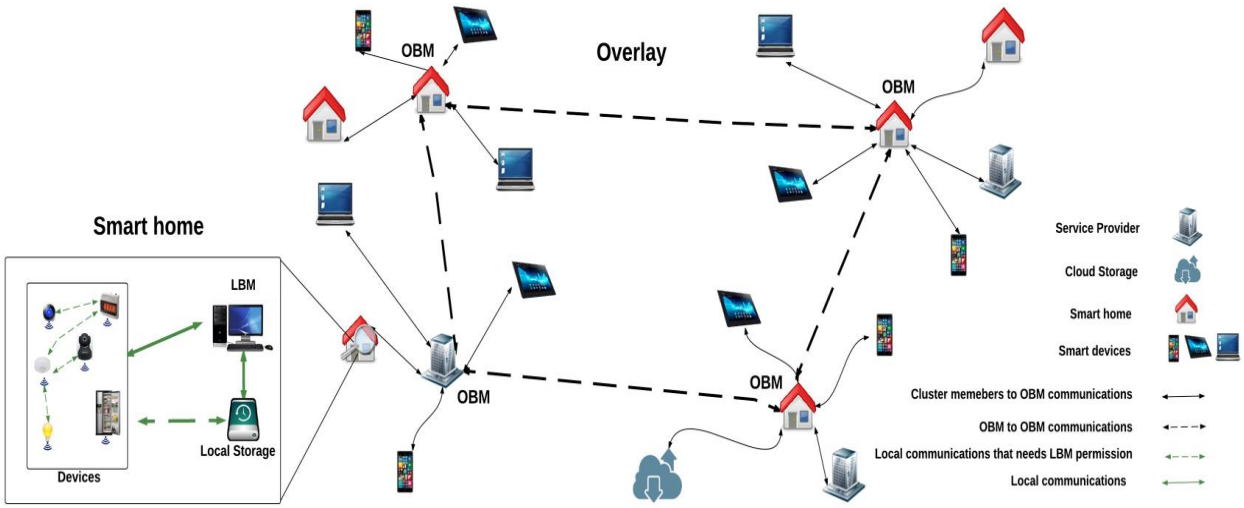
نعرض في هذا الفصل النموذج المقترح لسلسلة الكتل في انترنت الأشياء، محققاً للسرية والخصوصية، وسنستخدم حالة المنزل الذكي كمثال على تحقيق هذا النموذج.

1.4- مقدمة

قبل البدء بالمحاكاة، يجدر بنا أولاً توضيح النموذج المقترح والحديث عن أجزائه ووظائفه المختلفة. نستخدم في توصيف النموذج المقترح منصة LSB المعرّفة في [71] ونضيف إليها التحسينات التي سنقوم بتعريفها لاحقاً من أجل ضمان الوصول إلى شبكة آمنة محققةً لخدمات السرية والخصوصية باستخدام سلسلة الكتل، يتألف النموذج المقترح من عدّة أجزاء رئيسية أهمّها التخزين السحابي، الشبكة الغطاء (overlay)، والمنزل الذكي كما يوضّح الشكل 4-1 والتي سنتحدّث عنها بالتفصيل.

نعرّف بدايةً بعض المفاهيم الأساسية في النموذج:

- المناقلة: هي وحدة الاتصال الأساسية بين العقد.
- مدير الكتلة Block Manager BM: هو كيان مسؤول عن إدارة سلسلة الكتل، بما في ذلك الإنشاء، التحقق، التخزين للمناقلات ولكتل المناقلات.



الشكل 4-1 النموذج المقترح وأجزاؤه.

ثم سننتقل إلى أجزاء النموذج فيما يلي:

2.4- الشبكة الغطاء Overlay Network

هي الشبكة التي تُبنى فوق شبكة المنزل، وتحقق التواصل بين عقد المنزل والعقد الأخرى الخارجية للتخزين بطريقة سرية. تتألف هذه الشبكة من عدد كبير من العقد تسمى عقد overlay، بما فيها عقدة المنزل الذكي LBM، عقدة الهاتف الذكي، وعقدة مزود الخدمة SP.

1.2.4- بناء الشبكة:

نفترض أن مجموعة جزئية من هذه العقد مسؤولة عن إدارة سلسلة الكتل العامة وذلك لضمان قابلية التوسع (scalability)، كما نفترض أن يجري تجميع العقد في عناقيد بخوارزمية عنقدة كالموجودة في [79]، يجري في كل عنقود (cluster) انتخاب Cluster Head (CH) أو "Overlay Block Manager (OBM)" الذي يعتبر بمثابة مدير كتلة على مستوى الـ overlay وهو مسؤول عن إدارة سلسلة الكتل العامة مع أقرانه من الـ OBMs. كما يعتبَر OBM مسؤولاً عن معالجة كل المناقلات الصادرة والواردة من وإلى العنقود الخاص به، ويجب أن يتمتع بموارد عالية وأن يبقى متصلاً لفترات زمنية طويلة.

نستخدم العقدة CH كمولِّد للمفاتيح، وهي أيضاً تمثل السلطة المركزية CA في الشبكة. نحتاج هذه العقدة في اقتراحنا فقط من أجل التحقق من العقد الموجودة في البداية، ولتوليد المفاتيح المطلوبة خلال هذه المرحلة، ثم يمكننا الاستغناء عنها.

تقوم العقدة CH خلال مرحلة التعريف باختيار كثيري حدود بشكل عشوائي $F,G \in \mathbb{R}$ ثم تقوم بحساب المفتاح العام بالشكل:

$$K_{ch+} = f_q^{-1} \times g \pmod q \qquad (1\text{-}4)$$

تستخدم العقدة A رقماً مميزاً يمثل الرقم التعريفي لها ID_A للتسجيل عند العقدة CH.

تقوم CH الآن بحساب المفتاح العام والخاص للعقدة A بالشكل:

$$K_{A+} = f_{A,q}^{-1} \times g \pmod q$$
$$K_{A-} = \left(f_A, f_{A,q}^{-1}, f_{A,p}^{-1}, g\right)$$

ومن ثم تختار كثير حدود عشوائي $k_A \in L_k$ وتقوم بحساب القيم التالية (وهي القيم المميزة لكل عقدة):

$$X_A = k_A \times K_{ch+} \pmod q$$
$$HID_A = H\left(K_{A+} \| ID_A\right)$$
$$S_A = HID_A \times K_{A+} + k_A \pmod q$$

حيث يمثل التابع H تابع التهشير و || هي علاقة الضم بين المتحولات.

يجب على العقد المشاركة في كل عنقود أن تتحقق من بعضها البعض. لذلك تقوم العقدة A بطلب الشهادة الموثقة من العقدة CH، فترسل لها الشهادة المفصّلة التالية:

$$CH \to A : cert_A = \left[IP_A, K_{A+}, t, e\right] K_{CH-}$$

والموقعة بالمفتاح الخاص للعقدة CH.

تحوي هذه الشهادة عنوان العقدة A وهو IP الخاص بها، والمفتاح العام لها، وقيمة زمنية تمثل تاريخ صدور الشهادة وتاريخ نهايتها.

بعد نهاية مرحلة التعريف تكون كل العقد قد عرفت المفتاح العام للعقدة CH، والمفاتيح الخاصة بها، والقيم المميزة لها X_M, HID_M, S_M . عندئذ تكون مهمة CH قد انتهت.

وللتعامل مع حالات فشل CH أو OBM عند انضمام أجهزة IoT جديدة أو مغادرة أجهزة موجودة، نستخدم التعمية العتبية (Threshold Cryptograghy) لتوزيع السر المشترك بين العقد دون الحاجة إلى وجود العقدة المركزية CH. حيث تقوم مجموعة العقد الموجودة ضمن العنقود بتجميع المفتاح وإعطائه للعقدة الجديدة بعد التحقق منها.

1.1.2.4- المناقلات

هي المناقلات التي يكون مولّدها (requester) ومستقبلها (requestee) وهما عقدتا overlay. وتحوي شبكة overlay المناقلات الأساسية التالية:

- Genesis: يجب أولاً على كل عقدة في شبكة overlay إنشاء هذه المناقلة التي تمثّل نقطة البداية لسجلّها (ledger) في سلسلة الكتل العامة.
- Store: تنشئ عقدة ما هذه المناقلة لتخزين البيانات في السحابة.
- Access: يجري توليدها من قبل عقدة overlay لطلب البيانات المخزّنة من قبل أحد التجهيزات، كأن يطلب أحد مزودات الخدمة (requester) جميع البيانات المخزّنة من قبل أحد التجهيزات (requestee) لفترة معينة من الزمن.
- Monitor: كأن يطلب مزود خدمة معلومات في الزمن الحقيقي عن احد التجهيزات.

تجري حماية هذه المناقلات باستخدام التعمية غير المتناظرة، والتوقيع الرقمي الحلقي (كما سنرى لاحقاً في الفقرة 3.3.4-)، وتوابع التهشير.

يمكن تصنيف المناقلات إلى:

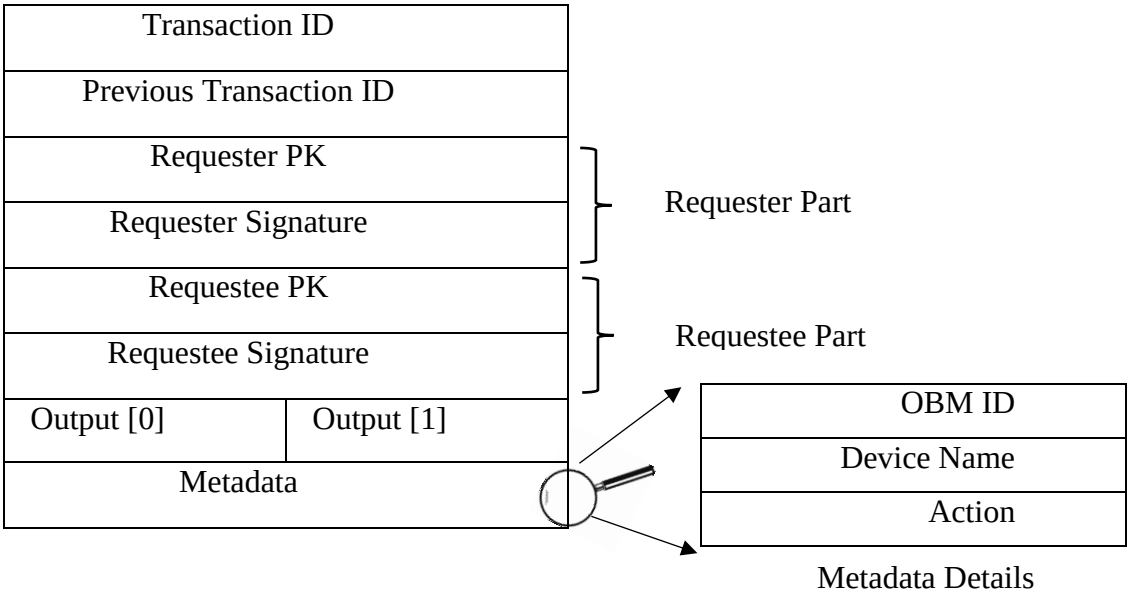
- مناقلات وحيدة التوقيع Single Signature: تحوي فقط توقيع منشئ (مولّد) المناقلة.
- مناقلات متعددة التواقيع Multisig: يجري توقيعها من قبل مولّد المناقلة (requester) ومستقبلها (requestee).

يوضّح الشكل 4-2 بنية المناقلات متعدّدة التواقيع التي تتألف من 8 حقول أساسية، يعبّر الحقل الأول عن معرّف المناقلة، بينما يمثِّل الحقل الثاني مؤشراً على المناقلة السابقة لنفس العقدة المولّدة للمناقلة (requester)، مما يربط جميع المناقلات المولّدة من نفس العقدة معاً. ثم تأتي أربعة حقول تمثّل المفتاح العام والتوقيع لكل من المرسل والمستقبِل للمناقلة، مع ملاحظة أن توقيع المستقبل (requestee) يضاف إلى المناقلة عند استلامها من قبله. يمثّل الحقلُ السابع في بنية المناقلة خرجَ المناقلة وهو مقسَّم إلى خانتين يضع المرسِل قيمها:

- Output [0]: العدد الكلي للمناقلات المنشأة من قبل الrequester والموافَق عليها من الـ requestee.
- Output [1]: العدد الكلي من المناقلات المرفوضة من قبل الـ requestee.

تؤمّن هاتين الخانتين معلومات تاريخية ضرورية لحساب سمعة الrequester ، التي تستخدَم في خوارزمية الثقة الموزعة (الفقرة 3.1.2.4-). أما الحقل الثامن من بنية المناقلة (Metadata) فهو يحوي معلوماتٍ عن النشاط (action) المرغوب، وأحد تجهيزات المنزل الذكي المقصود بذلك النشاط.

تتشابه المناقلة وحيدة التوقيع مع المناقلة المتعددة التواقيع من حيث البنية، ماعدا توقيع ومفتاح الrequestee العام والبيانات الموجودة، والخرجين الأول والثاني من الحقل السابع كون تلك المناقلة محصورة في عقدة overlay واحدة. يجري تنظيم الصنفين السابقين من المناقلات في كتل منفصلة بسبب اختلاف المخرجات لها.



الشكل 4-2 بنية المناقلة متعدّدة التواقيع.

ودائماً ما يجري فصل مسار البيانات عن مسار المناقلات، أي في حالة الاستجابة لمناقلات access أو monitor، يقوم الجهاز المقصود (requestee) بإرسال البيانات إلى الrequester في مسار رزم (Packets) البيانات منفصل عن مسار المناقلة بعد التأكد من تخويله للوصول إلى البيانات، وكذلك الأمر بالنسبة لمناقلة التخزين. وبالتالي نجد أن المناقلات يجري بثّها إلى جميع العقد بينما يجري توجيه البيانات إلى الوجهة المحددة باستخدام أحد بروتوكولات التوجيه (مثل OSPF).

يجري تخزين مناقلات overlay في سلسلة الكتل العامة المدارة من قبل OBMs، وتتكون كل كتلة في السلسلة العامة من جزأين أساسين هما المناقلات وترويسة الكتلة (كما ذكرنا سابقاً في الفقرة 4.2-)، بينما تتكون ترويسة الكتلة من قيمة تهشير الكتلة السابقة، معرّف (ID) مولّد الكتلة، وتواقيع العقد المتحقّقة من الكتلة. تضمن قيمة تهشير

الكتلة السابقة ثبات الكتلة وعدم التلاعب بها (immutability)، فإن حاول المهاجم تغيير معلومات مناقلة سابقة، سيؤثر ذلك التغيير على قيمة تهشير الكتلة الحاوية لتلك المناقلة، وبالتالي على جميع الكتل اللاحقة وسيجري كشف الهجوم بسهولة. يجري تجميع عدد معين من المناقلات في كتلة واحدة (كما في البتكوين)، حيث تستطيع الكتلة تخزين عدد T_{max} من المناقلات كحدّ أعظمي، يؤثر ذلك العدد على إنتاجية (throughput) سلسلة الكتل حيث يزداد عدد المناقلات الممكن تخزينها في كتلة واحد بازدياد T_{max}.

يحوي كل OBM على قائمة مفاتيح تشبه قائمة مبسّطة للتحكم بالوصول (ACL) تحوي زوج المفاتيح العامة لمنشئ ومستقبل المناقلة التي تدل على إمكانية المنشئ بإرسال مناقلة معينة إلى أحد المستقبِلين، ويجري تحديث تلك القائمة من قبل عقد العنقود لإعطاء الصلاحيات إلى عقد overlay الأخرى بإرسال المناقلات لها، ويمكن للعقدة وضع قيمة "broadcast" بدلاً من مفتاح المنشئ (requester) أي أنها ستستقبل جميع المناقلات التي تحوي عنوانها كَrequestee. عندما يستقبل OBM مناقلة Y، يتأكد أولاً من وجود الrequestee المقصود بها في عنقوده، فإذا تطابق معطيات المناقلة Y (مفاتيح المنشئ والمستقبل) مع أحد أسطر القائمة، سيقوم الOBM بإرسال المناقلة إلى المستقبِل الموجود معه في نفس العنقود، وإذا لم يكن المستقبل موجوداً في عنقوده، فسيقوم ببثّ المناقلة إلى جميع الـ OBMs الأخرى. يجري تخزين كل المناقلات المنتظِرة (pending) في حوض (Pool) مناقلات حتى يصل حجم الحوض إلى T_{max}، عندها يبدأ OBM بعملية توليد كتلة جديدة باستخدام خوارزمية التوافق.

2.1.2.4- خوارزمية التوافق Consensus algorithm

تستخدِم التنجيزات الحالية لسلسلة الكتل خوارزميات توافق مثل POW أو POS وغيرها التي تتطلب موارد حسابية عالية لا تتناسب مع أجهزة انترنت الأشياء محدودة الموارد. لذا، سنقوم باقتراح خوارزمية توافق خفيفة قائمة على الزمن ومتناسبة مع الأجهزة مقيدة الموارد. يجب على خوارزمية التوافق ضمان العشوائية في اختيار العقدة المولّدة للكتلة وأن تكون العقدة مقيدة بعدد الكتل التي تولِّدها. تفترِض الخوارزمية المقترحة لضمان العشوائية في اختيار العقدة المنقِّبة أن يقوم كل OBM بالانتظار زمن عشوائي يدعى (waiting-period) قبل إنشاء كتلة جديدة. تختلف قيم الأزمنة العشوائية من OBM لآخر، وبالتالي ربما يستقبل أحد الـ OBMs كتلة جديدة مولَّدة من قبل OBM آخر وتحوي بعض أو كل المناقلات الموجودة حالياً في حوض المناقلات الخاص به، لذا يجب عليه حذف تلك المناقلات لأنه لا يجوز إضافتها أكثر من مرة إلى سلسلة الكتل. يساعد الانتظار لزمن عشوائي أيضاً في إنقاص عدد الكتل المكرّرة المحتمل إنشاؤها بنفس الوقت. القيمة العظمى لزمن الانتظار العشوائي تساوي ضعفي القيمة العظمى للتأخير من النهاية إلى النهاية في شبكة overlay، لضمان بثّ الكتل المولّدة حديثاً إلى جميع العقد.

لحماية شبكة overlay من الOBMs الخبيثة التي من الممكن أن تولّد عدد كبير من الكتل بمناقلات مزيفة (وهذا ما يسمى appending attack)، تفرِض الخوارزمية على العقد ألا تقوم بتوليد أكثر من كتلة واحدة في مجال زمني

محدد يدعى دور التوافق (consensus-period) الذي يجري ضبط قيمته من خلال إدارة الإنتاجية الموزّعة (DTM)، القيمة الافتراضية (والعظمى) لدور التوافق هي 10 ثواني التي تساوي قيمة مجال التنقيب في بتكوين، أما القيمة الصغرى فتساوي ضعفي القيمة العظمى للتأخير من النهاية إلى النهاية في شبكة overlay لضمان وجود زمن كافٍ لنشر الكتل الجديدة المولّدة من قبل الآخرين في الشبكة. يراقب كل OBM تردد توليد الكتل من قبل الآخرين ويجري إهمال أي كتلة مخالفة لخوارزمية التوافق مع إنقاص السمعة للعقدة المولدة لها كما سنوضح في الفقرة التالية. لمنع أحد الـ OBMs من الاستحواذ الدائم على قيم صغيرة لِـ waiting-period يقوم البقية بمراقبته أيضاً وإذا تجاوز عتبة معينة يجري إهمال الكتل المولَّدة من قبله.

3.1.2.4- خوارزمية الثقة الموزّعة

إن التحقق من كل المناقلات والكتل مكلف حسابياً، وخصوصاً عندما يزداد عدد العقد في شبكة overlay مما يسبب مشاكل متعلقة بقابلية التوسع في انترنت الأشياء. لذا، نقوم باقتراح خوارزمية الثقة الموزّعة التي تنقِص تدريجياً عدد المناقلات الواجب التحقق منها في كل كتلة جديدة من خلال قيام كل OBM في الشبكة ببناء جدول ثقة عن الآخرين. تقدِّم خوارزمية الثقة الموزّعة انطباعاً عن أدلة مباشرة وغير مباشرة كالتالي:

- الدليل المباشر Direct evidence: تمتلك عقدة (OBM) دليلاً مباشر عن عقدة أخرى إذا كانت قد تحققت من مناقلة واحدة على الأقل من تلك العقدة.
- الدليل غير المباشر Indirect evidence: إذا لم تملك عقدة أولى دليلاً مباشراً عن عقدة ثانية، لكن عقدة ثالثة أخرى قد تحققت مسبقاً من أحد مناقلات العقدة الثانية، بالتالي فإن العقدة الأولى تملك دليلاً غير مباشر عن العقدة الثانية.

يحتفظ كل OBM بجدول للأدلّة المباشرة يسجّل فيه عدد الكتل المتحقق منها لكل الـOBMs الأخرى، رأينا في الفقرة السابقة أنه يمكن لأحد العقد توليد كتل غير متلائمة مع خوارزمية التوافق. لذا، عندما تستلم العقد الأخرى كتلةً غير متلائمة تقوم بإهمالها وإنقاص الثقة المباشرة للعقدة المسؤولة بمقدار واحد مما يستدعي زيادة عدد المناقلات الواجب التحقق منها لتلك العقدة من قبل باقي العقد. أما بالنسبة للأدلّة غير المباشرة، تقوم العقدة المستقبِلة للكتلة بفحص عدد العقد التي تحققت من كتلة لنفس المولِّد. تكمن الفكرة الأساسية من خوارزمية الثقة الموزّعة أنه كلما زادت قوة الأدلة لعقدة معينة كلما نقص عدد المناقلات التي يجب التحقق منها للتأكد من صلاحية الكتلة، يظهِر الجدول 4-1 مثالاً عن جدول الثقة الموزّعة التي تحتفظ به العقدة (OBM) عن العقد البقية.

الجدول 4-1 الثقة الموزّعة.

الدليل المباشر	عدد الكتل المتحقق منها سابقاً	10	20	30	40	50
	بحاجة للتحقق	%80	%60	%40	%30	%20
الدليل غير المباشر	النسبة المئوية لعدد OBMs التي وقعت الكتلة	%20	%40	%60	%80	%100
	بحاجة للتحقق	%80	%75	%70	%60	%40

للأدلّة المباشرة أولوية على الأدلة غير المباشرة، مع ملاحظة أنه يجب التحقق من نسبة معينة من المناقلات حتى بوجود أدلة مباشرة قوية وذلك للحماية من الOBMs الخبيثة، وإن لم يكن هنالك أية أدلة، فيجب التحقق من جميع مناقلات الكتلة.

4.1.2.4- إدارة الإنتاجية الموزّعة Distributed Throughput Management DTM

نعرّف الإنتاجية (Throughput) على أنها عدد المناقلات المخزَّنة في سلسلة الكتل بالثانية. تحدّ خوارزميات التوافق التقليدية المستخدَمة في سلسلة الكتل من إنتاجية تلك السلسلة، حيث يتطلب حلّ اللّغز المعمّى (cryptographic puzzle) موارد حسابية عالية جداً، فمثلاً تحدّ خوارزمية التوافق POW المستخدمة في سلسلة كتل البتكوين إنتاجيةَ تلك السلسلة إلى 7 مناقلات في الثانية. نجد مما سبق أن تلك المحدودية غير مقبولة في انترنت الأشياء حيث يوجد الكثير من التفاعلات والمناقلات بين العقد المختلفة، لذا نقترح آليةَ إدارة الإنتاجية الموزّعة DTM الموضّحة في الخوارزمية 4-1 للمراقبة الفعّالة لإنتاجية سلسلة الكتل وإجراء التعديلات المناسبة لإبقائها ضمن مجال مقبول.

الخوارزمية 4-1 إدارة الإنتاجية الموزّعة.

Input α

while true **do**
  If ($\alpha > \alpha_{max}$) **then**
    compute consensus_period$_{new}$ from Equation (2-4) with $\alpha = \frac{\alpha_{min} + \alpha_{max}}{2}$
    If (consensus_$period_{min} \leq$ consensus_$period_{new}$) **then**
      update consensus_period to consensus_period$_{new}$
    else
      reset consensus_period to default value
      compute M from Equation (2-4) with $\alpha = \frac{\alpha_{min} + \alpha_{max}}{2}$
      recluster overlay
    end if
  end if
  If ($\alpha < \alpha_{min}$) **then**
    compute consensus_period$_{new}$ from Equation (2-4) with $\alpha = \frac{\alpha_{min} + \alpha_{max}}{2}$
    If (consensus_$period_{new} \leq$ consensus_$period_{max}$) **then**
      update consensus_period to consensus_period$_{new}$
    else
      reset consensus_period to default value
      compute M from Equation (2-4) with $\alpha = \frac{\alpha_{min} + \alpha_{max}}{2}$
      recluster overlay
    end if
  end if
end while

يقوم كل OBM في نهاية كل دور توافق بحساب المردود (utilization) α الذي يساوي نسبة العدد الكلي للمناقلات المولّدة إلى العدد الكلي للمناقلات المضافة إلى سلسلة الكتل منذ آخر حساب لـ α، ينبغي أن تكون قيمة α متقاربة

عند جميع العقد لأن كل المناقلات والكتل الجديدة يجري نشرها في الشبكة إلى جميع العقد، وتعمل خوارزمية الإنتاجية الموزّعة على الحفاظ على قيمة α ضمن مجال مقبول $(\alpha_{min}, \alpha_{max})$.

نفترض شبكة مكوّنة من N عقدة، مع عدد M من الOBMs ، ونفترض R المعدّل الوسطي لإنتاج عدد من المناقلات في الثانية من قبل عقدة (يمكن تقدير قيمة R من العدد الكلي للمناقلات المولَّدة في consensus-period)، يمكننا حساب قيمة α من المعادلة التالية:

$$\alpha = \frac{N * R * Consensus - period}{T_{max} * M} \qquad (2\text{-}4)$$

تقترح المعادلة السابقة أن هنالك طريقتين لضبط قيمة المردود هما:

- تغيير قيمة دور التوافق (consensus-period) الذي يعبر عن تردد إضافة الكتل إلى السلسلة.
- تغيير قيمة M حيث يمكن لكل OBM توليد كتلة واحدة خلال دور التوافق، لكن هذه الطريقة تسبّب زيادة الحمل على الشبكة بشكل كبير حيث تتطلّب إعادة تهيئة (reconfiguration) شبكة overlay بالكامل (كما رأينا في الفقرة 1.2.4-).

لدينا حالتين لعمل خوارزمية إدارة الإنتاجية الموزّعة:

1. إذا تجاوزت قيمة α القيمة α_{max}: تقوم الخوارزمية أولاً بالتحقق من إمكانية إنقاص دور التوافق، فإن أمكن ذلك، يجري حساب قيمة جديدة للدور من المعادلة (2-4) مع إعطاء قيمة لـ α هي

$$\alpha = \frac{\alpha_{max} + \alpha_{min}}{2}$$

وهي منتصف المجال المسموح مما يضمن نقطة عمل مستقرة للشبكة (السطرين 2 و3 من الخوارزمية 4-1). وإن لم يكن بالإمكان إنقاص قيمة دور التوافق، فيجب إعادة عنقدة الشبكة بحساب قيمة جديدة لـ M (السطر 4 من الخوارزمية 4-1)، يجري حساب M أيضاً من المعادلة (4-2) مع نفس القيمة السابقة لـ α أي منتصف المجال المرغوب، ومع وضع القيمة الافتراضية لدور التوافق (وهي القيمة العظمى كما رأينا في الفقرة 2.1.2.4-) وذلك لكي لا تبقى على العتبة الدنيا بشكل دائم مما سيضطرنا إلى إعادة تهيئة الشبكة من جديد، تسمح هذه الميزة للشبكة بالتّوسّع (scale) بشكل جيد حيث تزداد الانتاجية بازدياد عدد العقد المشاركة.

2. $\alpha < \alpha_{min}$ بعكس الحالة السابقة، تحاول الخوارزمية أولاً زيادة قيمة دور التوافق، وإلّا فسوف تنقِص قيمة M (الأسطر 7 – 9 من الخوارزمية 4-1).

لضمان انسجام جميع العقد مع القرار المتّخَذ (تغيير قيمة دور التوافق أو M)، ينتظِر كل OBM لزمن عشوائي ثم يبثّ القرار الذي يؤيده لكل أقرانه، ويقوم كل من استلم الرسالة إما بتوقيعها وإعادة إرسالها في حالة التوافق مع القرار، أو ينشئ رسالة جديدة بقراره المخالف ويبثّها، وبالتالي يجري العمل بالقرار الذي وافق عليه أكثر من نصف العقد (OBMs). قد يحدث في بعض الأحيان عدم توافق في حساب قيمة المناقلات المولّدة بين العقد بسبب فقد الرزم (Packet Loss) أو بسبب التأخير في الشبكة مما يعطي اختلافات في حساب قيمة دور التوافق أو M.

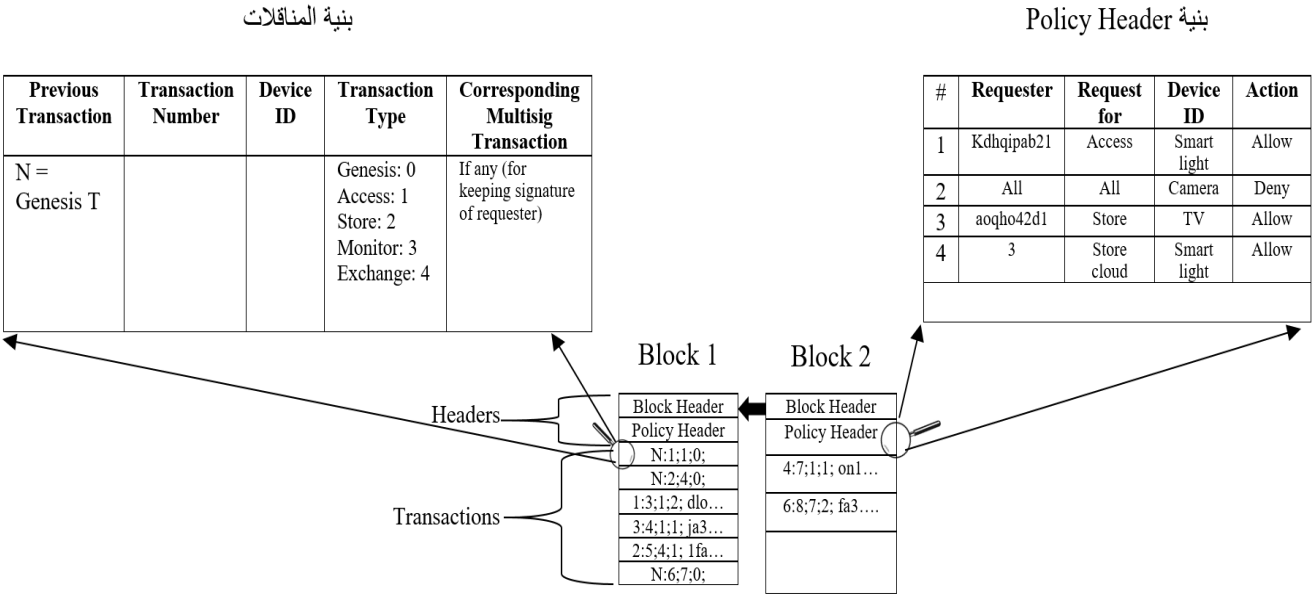
3.4- المنزل الذكي

يتكوّن المنزل الذكي من عدد من تجهيزات انترنت الأشياء التي يديرها مدير محلي (Local Block Manager LBM)، تتميز معظم تلك التجهيزات بمحدودية مواردها مما يستدعي استخدام تعمية متناظرة خفيفة (الفقرة 2.3.4–) للمناقلات المحلية (داخل المنزل الذكي)، واستخدام تابع تهشير خفيف مثل Spongent المستخدَم في [80]، يُدير LBM مركزياً سجلاً ثابتاً محلياً (Immutable Ledger IL) الذي يشبه ببنيته سلسلة الكتل، ويعالج المناقلات المحلية ومناقلات overlay الصادرة أو الواردة من وإلى المنزل الذكي. يستخدِم LBM خوارزمية Diffie-Hellman (الملحق آ) المعمّمة لتوليد وتوزيع المفاتيح المشتركة بين أي مكوّنين محلّيين يريدان الاتصال فيما بينهما لتبادل البيانات حسب الصلاحيات الموجودة في Policy Header المخزَّن في IL والذي سنناقشه فيما يلي.

يبيّن الشكل 4-3 بنية السجل الثابت المحلي، حيث تتكون كل كتلة فيه من block header وpolicy header، تحوي ترويسة الكتلة (block header) قيمة تهشير الكتلة السابقة لضمان الثبات وعدم التغيير (immutability) كما في سلسلة الكتل العامة، بينما يُعتبَر policy header بمثابة قائمة تحكم بالوصول ACL التي تعرّف قواعد التعامل مع المناقلات المحلية ومناقلات overlay. يوضّح الجزء اليميني من الشكل بنية policy header التي تتكون من 4 محدّدات:

- Requester: هي معرّف ID العقدة التي قامت بتوليد المناقلة، حيث تكون المفتاح العام للعقدة المولّدة بالنسبة للمناقلات الواردة من شبكة overlay (مناقلة متعددة التواقيع) ، بينما تدلّ على جهاز معين بالنسبة للمناقلات المحلية (كما هو موضح في الشكل).
- Request for: تدلّ على النشاط المسموح (موجود في البيانات المترفّعة من المناقلة كما رأينا في الشكل 4-2)، الذي يمكن أن يكون store locally، store cloud، access، monitor، و periodic monitor.
- Device ID: الجهاز المقصود بالنشاط السابق.

- Action: الصلاحية التي تسمح أو ترفض النشاط المرغوب.



الشكل 4-3 بنية **IL** المحلّي.

ويجري تخزين كل المناقلات في الجزء المخصص لها في IL لأغراض المراقبة (auditing)، حيث يُخزَّن 5 حقول لكل مناقلة كما يوضّح الجزء اليساري من الشكل السابق، الحقل الأول هو مؤشر على المناقلة السابقة لنفس العقدة المولِّدة لسلسلة من المناقلات المستهدِفة لجهاز معيّن وتستخدِم LBM هذا الحقل لأغراض المراقبة والمصادقة، بينما يمثّل الحقل الثاني معرّف للمناقلة. أما الحقل الثالث فهو معرّف للجهاز المولّد للمناقلة بالنسبة للمناقلات المحلية، ومعرّف للجهاز المقصود بالمناقلة بالنسبة لمناقلات overlay ويجري استخلاصه من حقل البيانات المترفّعة للمناقلة المستقبَلة من overlay (الشكل 4-2). يعبّر الحقل الرابع عن نوع المناقلة (والذي سنتحدث عنه في الفقرة التالية (4.3.1-))، يُستخدَم الحقل الخامس في حالة مناقلة مستقبَلة من شبكة overlay لتخزين قيمة تهشير المناقلة (transaction ID) لاستخدامه كعنوان للوصول إلى المناقلة في سلسلة الكتل العامة.

يجري تزويد كل منزل ذكي بجهاز تخزين محلّي (Local storage) لتخزين بيانات التجهيزات المحلية، يمكن لهذا الجهاز أن يكون مندمجاً مع LBM أو أن يكون منفصلاً، يُولِّد LBM مفتاحاً مشترك تستخدِمه التجهيزات للمصادقة مع جهاز التخزين المحلي وفق الصلاحيات الموجودة في policy header.

1.3.4- المناقلات المحلية

هي المناقلات المتبادلة بين العقد التي تنتمي لنفس المنزل الذكي، يجري تشفيرها بمفتاح مشترك بين الجهازين المتبادِلين لها. يقوم LBM بتوليد مفاتيح مشتركة للأجهزة باستخدام خوارزمية Diffie-Hellman المعمّمة وذلك بعد الحصول على موافقة مالك المنزل الذكي، وتبقى تلك المفاتيح صالحة حتى يرسل LBM رسائل تحكم تفيد بانتهاء صلاحيتها. المناقلات المحلية الأساسية هي:

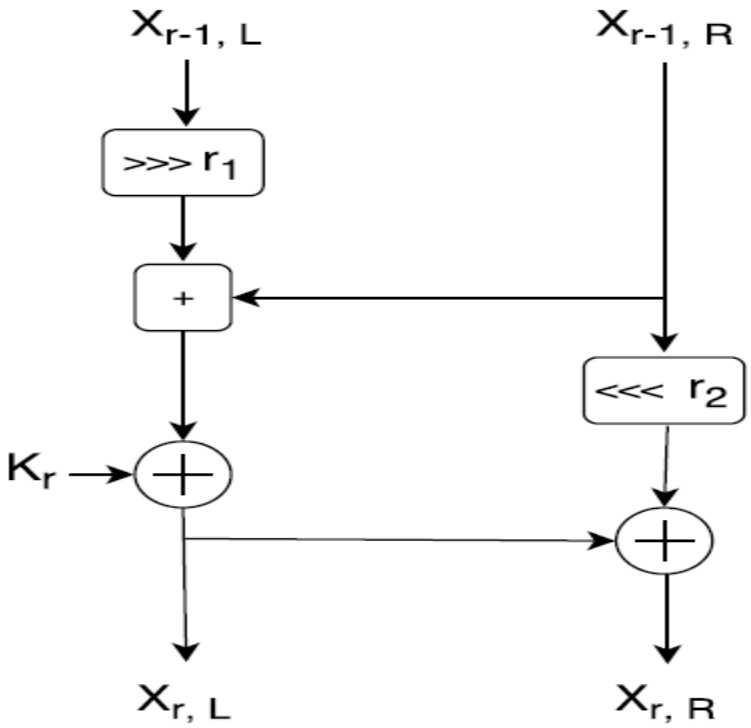
- مناقلة Genesis: هي أول مناقلة مخزّنة في IL المحلي لكل جهاز من المنزل الذكي، يولّد LBM مفتاحاً مشترك لتعمية الاتصالات بينه وبين الجهاز ويقوم بتخزين ذلك المفتاح في مناقلة genesis الخاصة بالجهاز.
- مناقلة store locally: يقوم أولاً الجهاز الذي يرغب بتخزين البيانات في جهاز التخزين المحلّي بإرسال طلب إلى LBM، ثم يقوم LBM بتوليد وتوزيع مفتاح مشترك بين جهاز التخزين المحلي والجهاز الذي يرغب بالتخزين، يستخدِم جهاز التخزين المحلي المفتاحَ المشترك في المصادقة، ويسري مفعول ذلك المفتاح من أجل طلبات التخزين اللّاحقة بشكل مباشر دون الرجوع إلى LBM إلى أن يقرر مالك المنزل بعدم السماح للجهاز بالتخزين فتنتهي صلاحية المفتاح.
- مناقلة Data exchange: قد يحتاج أي جهاز في المنزل الذكي أن يطلب بيانات من جهاز محلي آخر لتقديم خدمة معينة، فمثلاً يمكن أن يحتاج حساس الإضاءة إلى بيانات حساس كشف الحركة بقصد إنارة المنزل عند دخول أحدهم إليه. لفرض سيطرة المالك على المنزل، يجب على أي جهازين يريدان الاتصال أولاً الحصول على المفتاح المشترك من LBM ويبقى المفتاح صالحاً حتى يأتي القرار من المالك بإلغائه.

تجري حماية المناقلات المحلية كما المناقلات في الـ overlay باستخدام تقنيات التوقيع الرقمي الحلقي، ونستخدم التعمية المتناظرة من أجل التعمية وذلك لمحدودية الأجهزة الموجودة.

2.3.4- خوارزمية التعمية المتناظرة ARX

نستخدم في نموذجنا فرعًا معينًا من تعمية المفتاح المتماثل، يسمى ARXخوارزميات لتعمية البيانات لسلسة الكتل blockchain. تتميز هذه الخوارزمية بعمليات حسابية بسيطة كالجمع، التدوير وXOR ويدعم تعمية خفيفة للأجهزة الصغيرة محدودة الموارد.

جرى استخدام هذه الخوارزمية في أمثلة قليلة معروفة، آخرها وأهمّها عائلة SPECK[8] [81]، وهي عائلة تضمّ مجموعة من خوارزميات التعمية الكتلية الخفيفة، حيث يجري تقسيم كل كتلة إلى فرعين، ويجري تعديل كلا الفرعين في كل مرحلة (round)، يظهِر الشكل 4-4 وظيفة المرحلة الواحدة في عائلة SPECK، حيث يجري فيها تقسيم كل كتلة إلى نصفين: يميني ويساري.



الشكل 4-4 وظيفة المرحلة الواحدة في **SPECK**.

حيث تستخدِم SPECK في كل مرحلة ثلاث عمليات أساسية على كلمة مؤلّفة من n بت:

- $\oplus$: عملية XOR على مستوى البت.
- $\boxplus$: الجمع بالمقياس 2^n.
- انزياح دائري يميني ويساري بمقدار r_2 و r_1 بت على التوالي.

[8] عائلة SPECK هي مجموعة من خوارزميات التعمية الكتلية الخفيفة، جرى طرحها من قبل وكالة الأمن القومي الأمريكية (NSA) عام 2013.

تدلّ (X_{r-1}, L) على النصف الأيسر من الكلمة (n بت)، بينما تعبّر (X_{r-1}, R) عن النصف الأيمن، بينما تدلّ القيمة k_r على المفتاح المطبّق على الكلمة (n بت) في الدورة رقم r، أما كلمات خرج الدورة r فهي $X_{r,L}$ و $X_{r,R}$ ويجري حسابهما كالتالي:

$$X_{r,L} = \left((X_{r-1,L} >\!\!>\!\!> r_1) \boxplus X_{r-1,R} \right) \oplus k_r \qquad (3\text{-}4)$$

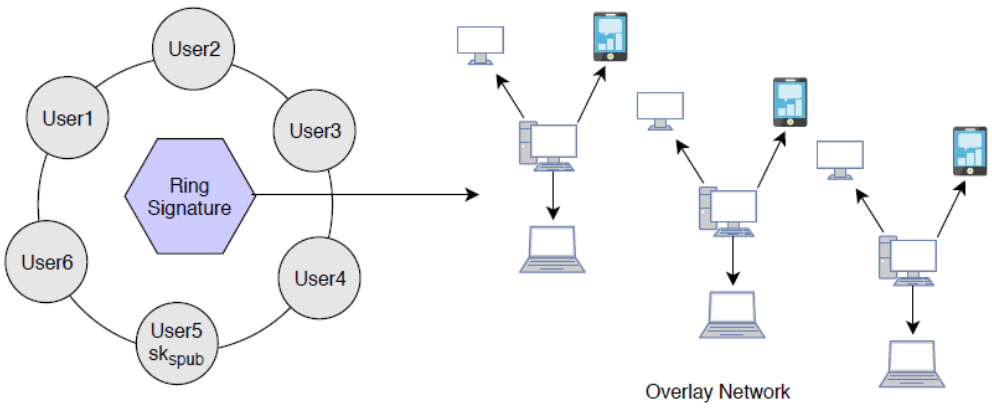
$$X_{r,R} = ((X_{r-1,R} <\!\!<\!\!< r_2) \oplus X_{r,L}) \qquad (4\text{-}4)$$

جرى استخدام أطوال مفاتيح مختلفة في تنجيزات عائلة SPECK، ويعتمد العدد الكلي للمراحل (rounds) على key size، وجرى تعيين قيم ثوابت التدوير (rotation) كالتالي:

إما $r_1 = 7, r_2 = 2$ أو $r_1 = 8, r_2 = 3$ في التطبيقات المختلفة لتلك العائلة.

3.3.4- التوقيع الرقمي الحلقي Digital Ring Signature

ستخدم التوقيع الحلقي الرقمي [82] الذي يسمح للموقّع بتوقيع البيانات بطريقة تخفي هويته (anonymous) كما هو موضَّح في الشكل 4-5، حيث يجري فيها مزج التوقيع مع مجموعات أخرى (هي الحلقة) ولا أحد من تلك المجموعة يعرف الموقّع الحقيقي إلّا صاحب التوقيع.



الشكل 4-5 التوقيع الرقمي الحلقي.

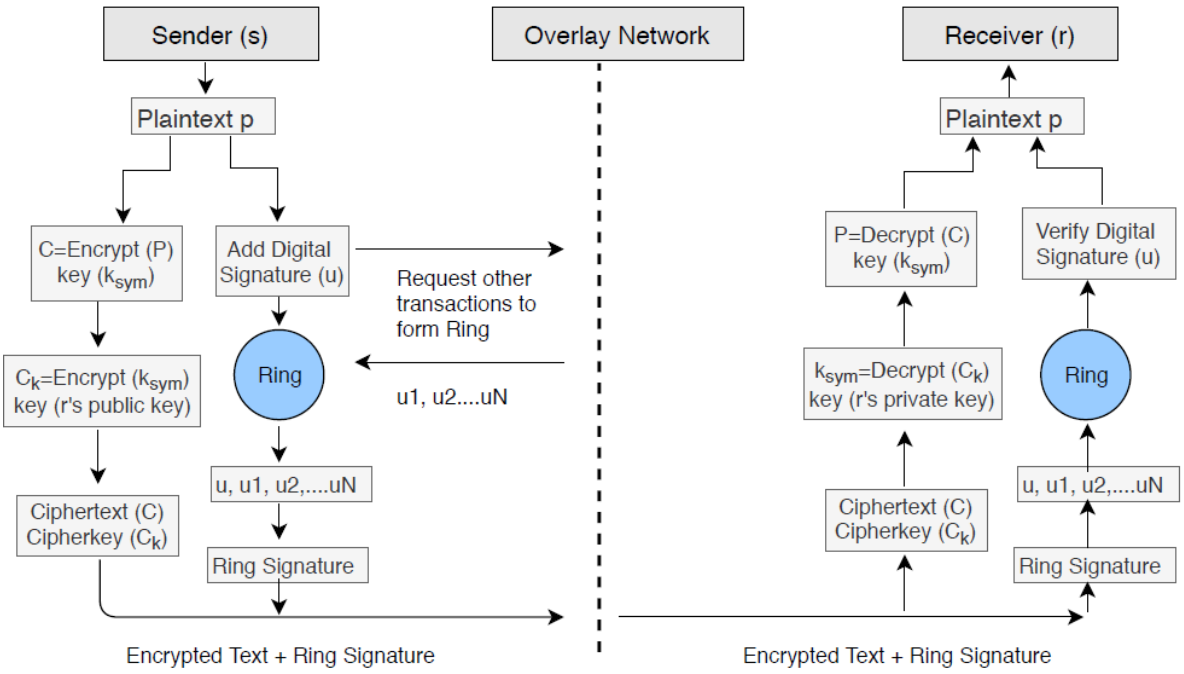
جرى طرح التوقيع الحلقي للمرة الأولى من قبل Rivest في عام 2001 [83]، حيث يقوم المستخدِم الذي يرغب بمزج مناقلته بإرسال طلب يحتوي على مفتاحه العام الخاص بالتوقيع $(sk_{s_{pub}})$ إلى شبكة سلسلة الكتل، ثم تقوم الشبكة

بإرسال كمية معيّنة من المفاتيح العامة $sk1_{s_{pub}}$، $sk2_{s_{pub}}$، ……، $skN_{s_{pub}}$ التي جرى جمعها من المستخدمين (u1, u2, …, uN) بما فيها المفتاح العام للمرسِل ($sk_{s_{pub}}$) كما يوضّح الشكل 4-6.

يجدر بنا الإشارة إلى أن زوج المفاتيح التي يستخدمها المرسل للتوقيع الرقمي مختلفة عن الزوج التي يستخدمها لتعمية البيانات.

يفيدنا استخدام التوقيع الحلقي في تحقيق خاصتين أمنيّتين هامّتين وهما:

- صلاحية التوقيع (Signature Correctness): يجري بشكل دائم قبول التوقيع الصالح ورفض التوقيع الغير صالح.
- إخفاء هوية الموقّع (Signers Anonymity): يجري توليد التوقيع من قبل أحد عناصر مجموعة حاملي المفاتيح العامة، لذا لا يمكن لأحد معرفة الهوية الحقيقية لصاحب التوقيع كونها مخفية ضمن الشبكة.



الشكل 4-6 مراحل تنفيذ خوارزمية التعمية والتوقيع الحلقي وتبادل المفاتيح.

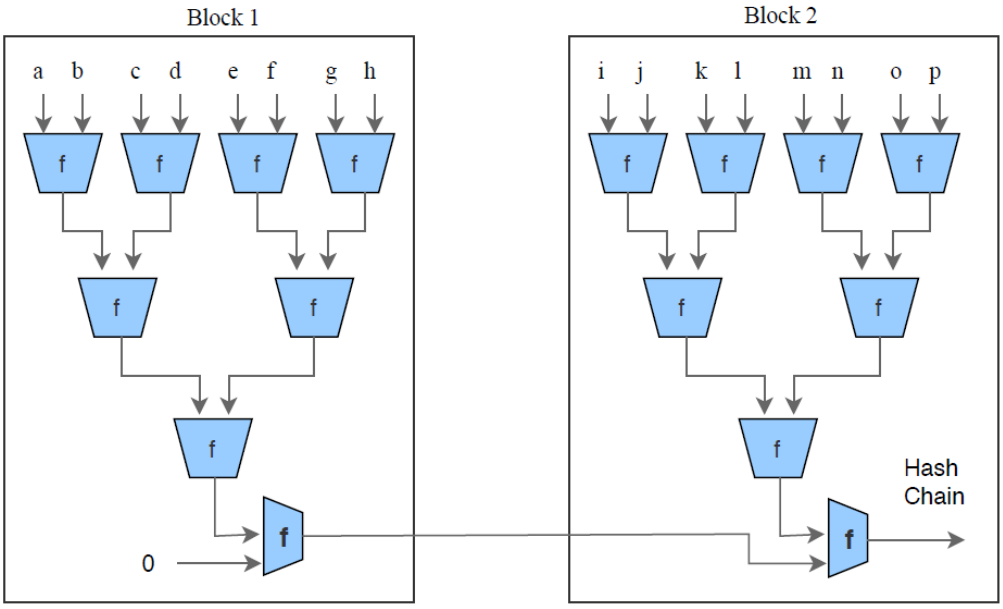
يبيّن الشكل السابق (الشكل 4-6) مراحل تنفيذ خوارزمية التعمية والتوقيع الرقمي الحلقي والموصفة بالخوارزمية التالية:

الخوارزمية 4-2 خوارزمية التعمية والتوقيع الحلقي وتبادل المفاتيح.

1: **Function** SIGNATURE ($data\_file$)
2: **If** user chose anonymity over blockchain **then**
3: Generate an asymmetric public-private key pair $sk_{s_{pub}}, sk_{s_{priv}}$
4: $hash_p \leftarrow$ calculate hash of the $data\_file$
5: Create the digital signature using $hash_p$ and signers private key ($sk_{s_{priv}}$).
6: Share the public key ($sk_{s_{pub}}$) to the receiver using Diffie-Hellman key exchange
7: Mix the signature with another network group to form a ring
8: **end if**
9: **end function**

4.4- التخزين السحابي

بدلاً من حفظ البيانات لانترنت الاشياء IoT عبر سلسلة الكتل blockchain، نستخدم مخدمات التخزين السحابي لحفظ بيانات المنزل. يقوم التخزين السحابي بتجميع بيانات المستخدم في كتل مماثلة مرتبطة مع رقم كتلة فريدة من نوعها. ترتبط هذه الغيوم بشبكات overlay، يرسل المخدِّم السحابي قيمة تهشير كتل البيانات إلى شبكة overlay. ويجري احتساب التهشير من البيانات في كتلة واحدة باستخدام شجرة ميركل كما في الشكل 4-7. تقوم الشبكة بتهشير الجذر للكتلة الجديدة، وتضيف قيمة التهشير الجديدة مع قيمة التهشير السابقة ويولد قيمة تهشير جديدة للسلسلة (كما رأينا في الفقرة 3.2-). وفي هذه الحالة لسنا بحاجة إلى أي طرف ثالث موثوق لأن أي تغييرات في البيانات يمكن تتبعها بسهولة.



الشكل 4-7 شجرة ميركل في سلسلة الكتل.

5.4- خاتمة

قمنا في هذا الفصل بتوضيح نموذجنا الأمني المقترح المكوّن من ثلاث طبقات، وتحدثنا عن كل طبقة وميزاتها بالتفصيل، إضافةً إلى الآليات المستخدَمة للتوافق والثقة والإنتاجية الموزّعة. لننتقل في الفصل التالي إلى محاكاة هذا النموذج وتوضيح نتائج تنفيذه عملياً.

الفصل الخامس

المحاكاة والتنفذ العملي

نعرض في هذا الفصل نتائج محاكاة النموذج المقترح في الفصل السابق، باستخدام الأداة Cooja في نظام التشغيل Contiki.

1.5- مقدمة

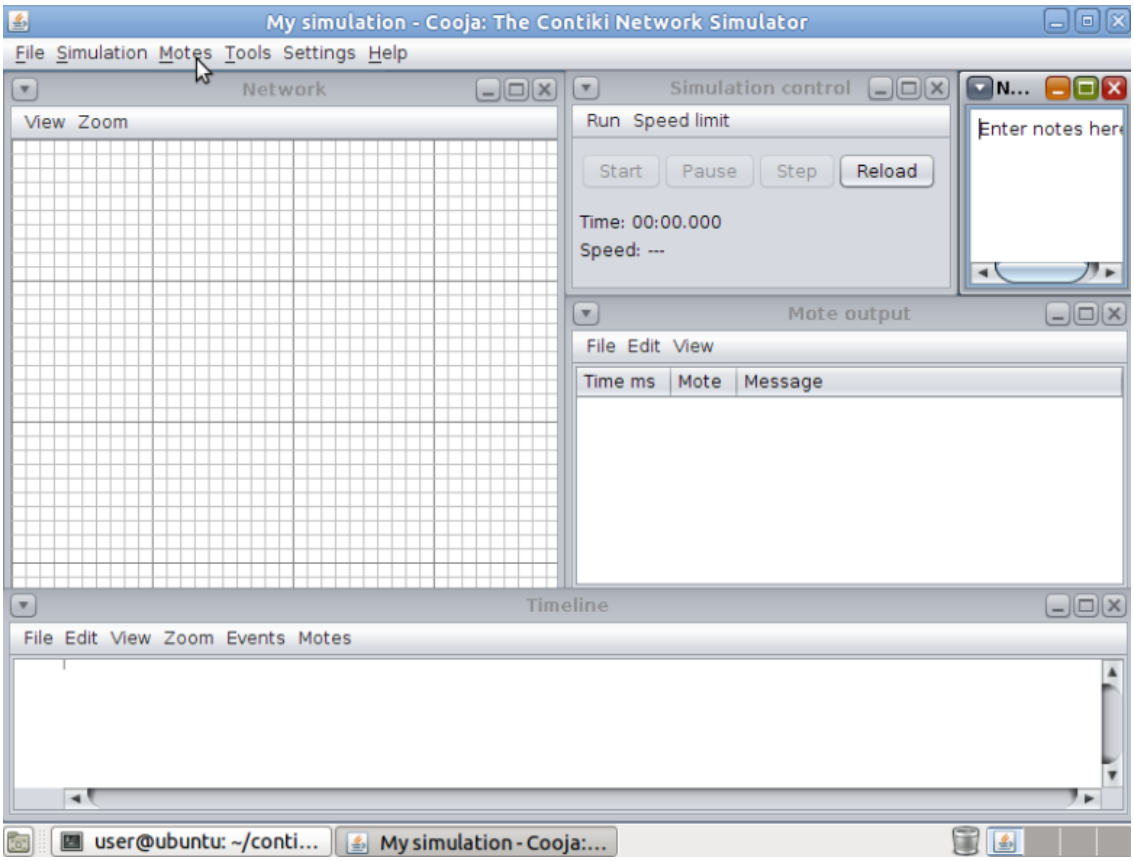
سنقوم بدايةً بالتعريف بالأدوات المستخدمة في المحاكاة قبل البدء بها، ثم سنتعرّف إلى أداة المحاكاة المستخدَمة (Cooja)، ثم تنفيذ المحاكاة لعدّة سيناريوهات وتقييم أداء النموذج المقترح باستخدام عدّة معايير، وعرض النتائج التي تدعم قدرة هذا النموذج في حماية أمن وخصوصية انترنت الأشياء باستخدام سلسلة الكتل.

2.5- الأداة Cooja

تعتبَر أداةً مثالية لمحاكاة شبكات الحساسات اللّاسلكية، لما تتمتع به من مواصفات قادرة على تمثيل الأجهزة محدودة الموارد، ولقدرتها على محاكاة بروتوكول الانترنت ipv6 ببساطة. تُستخدم هذه الأداة في نظام التشغيل Contiki، والذي صُمم خصيصاً لمحاكاة الأنظمة الشبكية التي تستعمل عقداً محدودة الموارد [84]، بالتحديد أجهزة انترنت الأشياء ذات الاستطاعة المنخفضة والذاكرة المحدودة. وتشمل الاستخدامات العديدة لنظام Contiki أنظمة المراقبة الذكية للمنزل، وأنظمة الإنارة في المدن الذكية وأجهزة الإنذار... الخ. كما يعتبر مفتوح المصدر تحت رخصة BSD.

جرى إنشاء هذا النظام من قبل Adam Dunkels في عام 2002، ثم جرى تطويره من قبل العديد من أشهر الجامعات والشركات مثل Texas Instrments، Atmel، Cisco، Oxford University، .....

يبيّن الشكل 5-1 الواجهة الرئيسية للأداة Cooja.

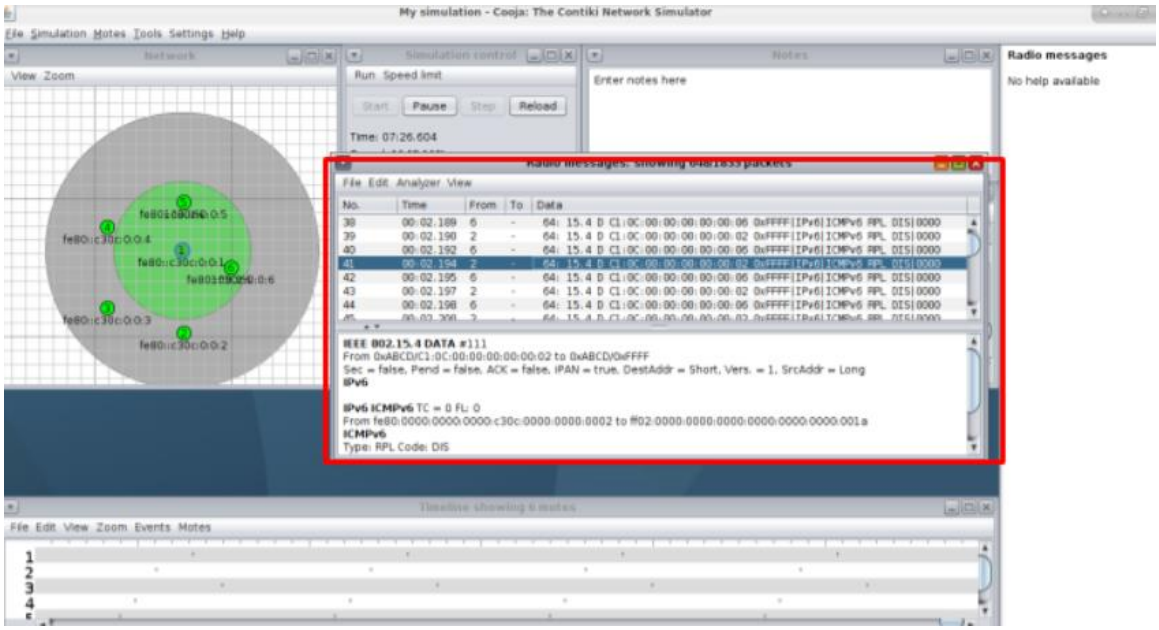


الشكل 5-1 واجهة **Cooja** الرئيسية.

1.2.5- ميزات الأداة Cooja

- محاكاة بيئة فيزيائية بنصف قطر 10 متر: وتمكننا هذه الميزة من تحديد تموضع العقد بناء على قوة الإشارة اللاسلكية القادمة.
- عرض المخطط الزمني للأحداث: حيث تعرض النافذة الزمنية المبينة في الشكل 5-2 الجدول الزمني للأحداث التي تمر في عقدة محدّدة.
- التقاط الحزم المتحركة ضمن الشبكة وإمكانية عرضها باستخدام wireshark: حيث يمكن تخزين المعلومات الموجودة في الحزم بملف pcap للاستفادة منه لاحقاً في تحليل المعلومات الموجودة ونمذجتها.
- إمكانية التواصل مع العقد الموجودة ضمن المحاكاة من الجهاز المضيف: باستخدام تطبيقات الويب الموجودة في Contiki، يمكننا التواصل بسهولة من الجهاز المضيف مع العقد المعرفة في المحاكاة، وبالتالي إمكانية تحديد الآثار الممكن حدوثها عند المحاكاة باستخدام مكونات عتادية حقيقية للعقد. وهذا ما يجعل أداة COOJA أكثر من محاكي للشبكات فقط.

- إمكانية المحاكاة لعدد كبير من العقد: وهذا يعتمد على الإمكانيات الفيزيائية للجهاز المضيف.
- إمكانية محاكاة أجهزة انترنت الأشياء محدودة الموارد.



الشكل 5-2 المخطط الزمني للأحداث في **Cooja**.

3.5- المحاكاة

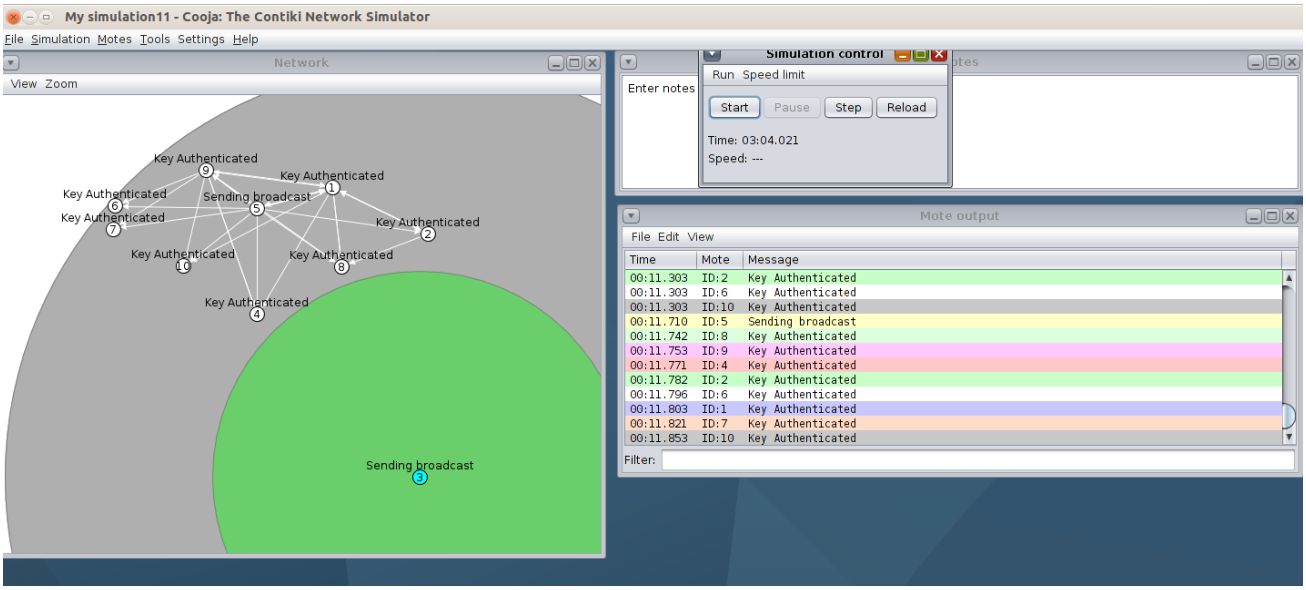
1.3.5- السيناريو الأول

نبدأ بالسيناريو الأول الذي يمثّل السيناريو الطبيعي، وذلك بتهيئة شبكة مكوّنة من مجموعة عقد في طبقة الغطاء.

للقيام بمحاكاة الشبكة كاملاً ودراسة أدائها، يجب أن نقوم بمحاكاة وتقييم أداء كل جزء فيها، وطالما أن الأجزاء في الشبكة مستقلة، فيمكننا الاكتفاء بمحاكاة طبقة overlay وتقييم أدائها، لأنها ستمثل الأداء العام للشبكة، باعتبارها الجزء الأكبر والرئيسي في الشبكة.

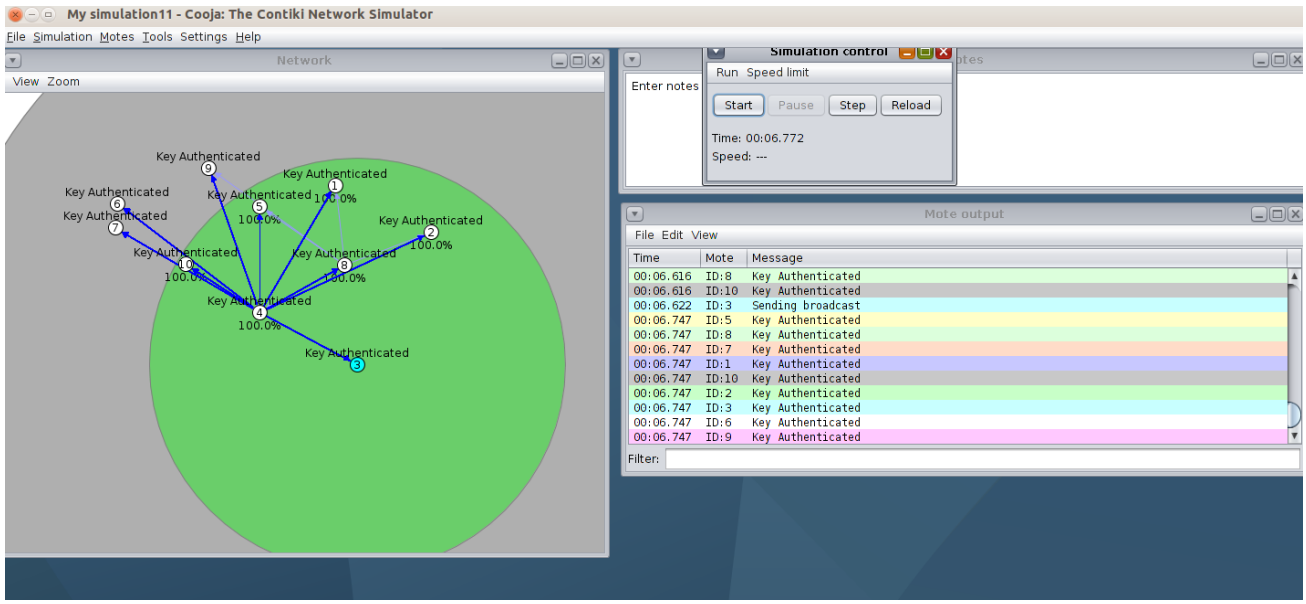
لابد بداية من إعادة تعريف العقدة داخل البرنامج لتتضمن التحسينات التي قمنا باقتراحها، وهي التعديل على الرماز المصدري الخاص بالعقدة باستخدام لغة البرمجة C. حيث قمنا بدايةً بإضافة تقنيات التعمية التي سنحتاجها وهي: التعمية المتناظرة ARX، والتعمية غير المتناظرة RSA، بالإضافة لتقنية التهشير SHA. بالإضافة إلى مجموعة التوابع المساعدة لتأمين عملية تحويل البنى البرمجية بما يتوافق مع دخل كل عملية من عمليات الحل المقترح، وملاءمة الخرج النهائي ليتوافق مع عمل العقد ضمن الشبكة.

نقوم بداية ببناء شبكة مكونة من 10 عقد سليمة، تتواصل فيما بينها بعد تهيئة وبناء الشبكة كما يوضّح الشكل 5-3.



الشكل 5-3 محاولة انضمام عقدة سليمة إلى الشبكة.

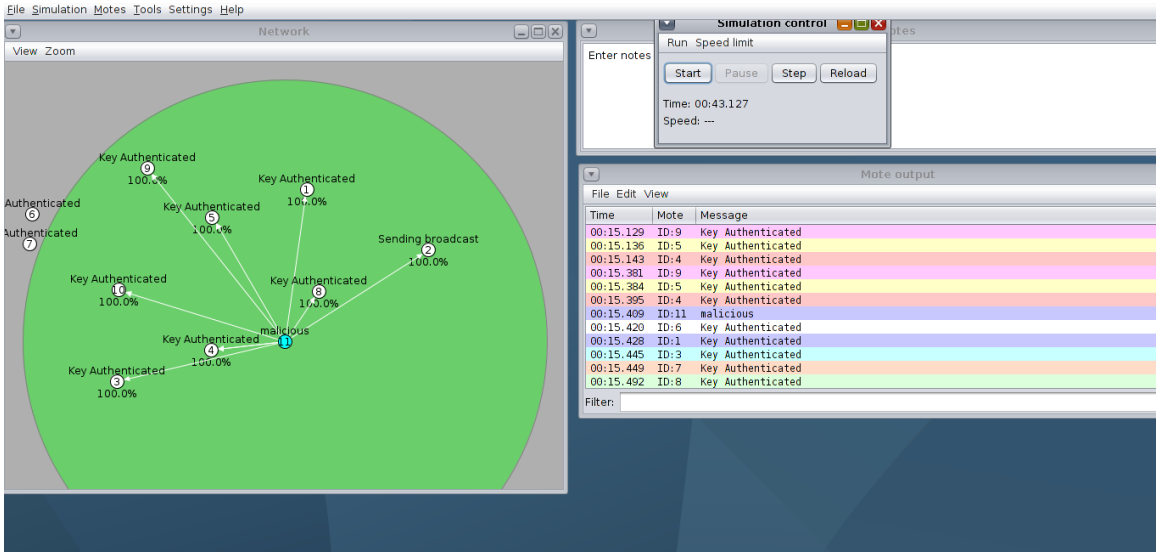
لإضافة عقدة جديدة إلى الشبكة، لاحاجة لوجود عقدة مركزية CA، بل يكفي أن تتعرف إليها العقد الأخرى الموجودة في الشبكة كما نلاحظ في الشكل 5-4، حيث تقوم العقد الموجودة بتجميع السر المشترك فيما بينها، وإرساله إلى العقدة الجديدة، وذلك بعد التأكد من هويتها.



الشكل 5-4 نجاح العقدة السليمة في الانضمام إلى الشبكة.

2.3.5- السيناريو الثاني

يعبّر هذا السيناريو عن محاولة دخول عقدة خبيثة إلى الشبكة كما يوضّح الشكل 5-5.



الشكل 5-5 محاولة انضمام عقدة خبيثة إلى الشبكة.

نلاحظ عدم قدرة العقدة الخبيثة على الحصول على السر المشترك (الشكل 5-6)، وبالتالي لن تحصل على المفتاح، ولن تستطيع دخول الشبكة، نتيجة تطبيق خوارزميات التعمية التي تحدثنا عنها سابقاً.

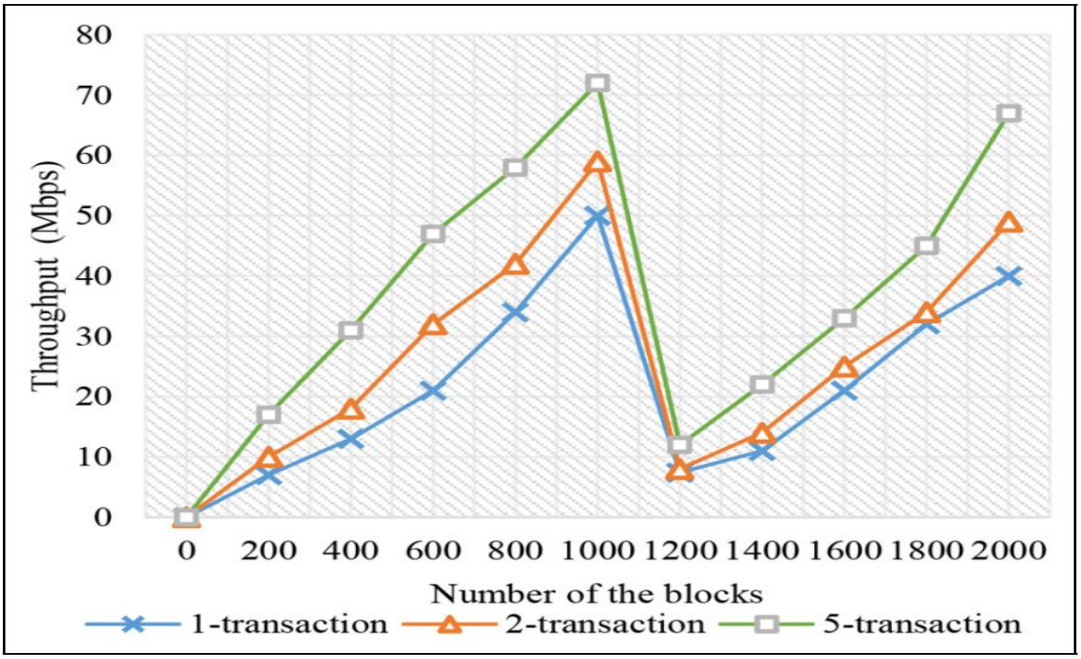
الشكل 5-6 فشل العقدة الخبيثة في الانضمام إلى الشبكة.

4.5- النتائج

نستنتج مما سبق أن الحل المقترح الذي قمنا بإضافته إلى سلسلة الكتل قد أعطى نتائج فعالة في بناء الشبكة وحمايتها من العقد الخبيثة الدّخيلة. وبذلك يمكننا القول أن هذا النموذج المقترح قد أعطى السرية والخصوصية التي كانت الهدف الأساسي في بحثنا.

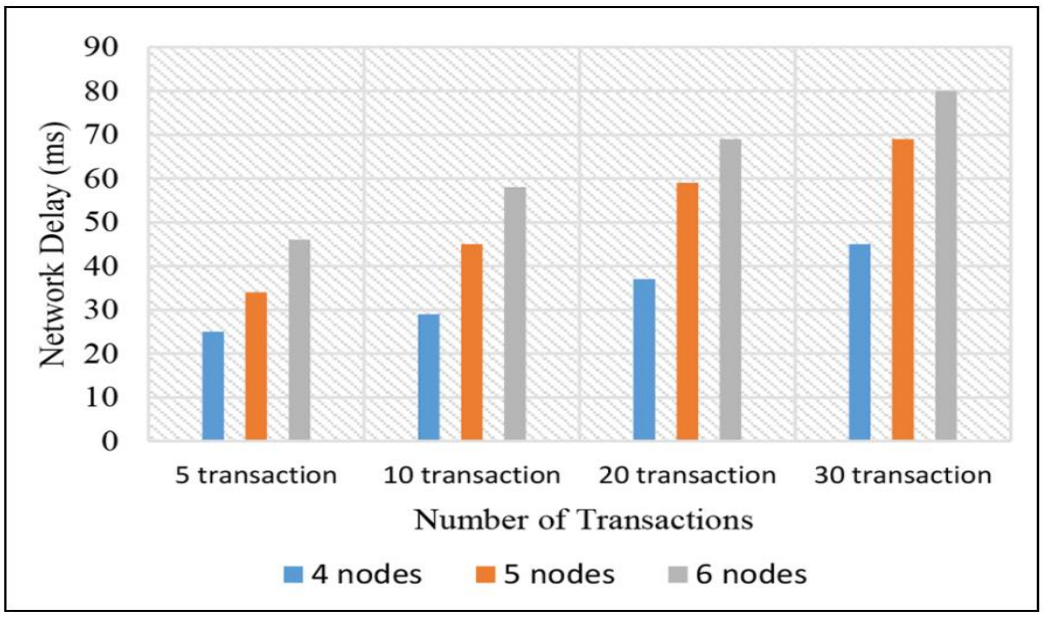
من المهم أيضاً أن نضمن أنّ إضافة هذا الحل لن يؤثر على الأداء العام للشبكة، ولدراسة أداء الشبكة يجب أن ندرس عدداً من العوامل التي تساهم في تقدير أداء النظام. وهذه العوامل هي مقدار التأخير في وصول الرزم delay، ومقدار الإنتاجية في الشبكة throughput، بالإضافة إلى نسبة التحميل الزائد التي يضيفها هذا الحل إلى الشبكة، وذلك للتأكد من أن الحل المقترح لم يؤثر على أداء الشبكة بشكل عام.

يمثّل الشكل 5-7 مقدار الإنتاجية في النموذج المقترح وعلاقته بعدد الكتل الموجودة في السلسلة.



الشكل 5-7 علاقة الإنتاجية بعدد الكتل وعدد المناقلات.

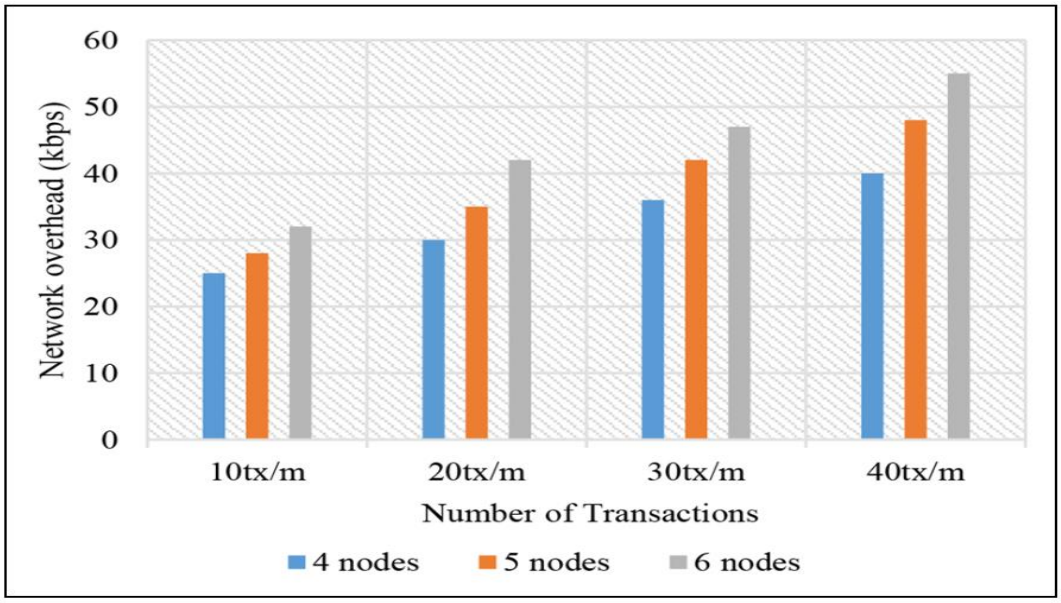
نلاحظ في الحالة الطبيعية أن مقدار الإنتاجية يزداد مع ازدياد عدد الكتل وزيادة عدد المناقلات. ونلاحظ أنه وفي لحظة ما يبدأ هجوم الفيضان (flooding) على تلك الشبكة، مما يسبب بتناقص كبير في الإنتاجية بسبب زيادة الازدحام وزيادة عدد المعالجات للرزم القادمة. ولكن بعد زمن قصير نسبياً نلاحظ عودة الإنتاجية إلى الازدياد تدريجياً وذلك بسبب نجاح الحل المقترح في صد هذا الهجوم والتعامل معه.



الشكل 5-8 علاقة التأخير الزمني بعدد العقد وعدد المناقلات.

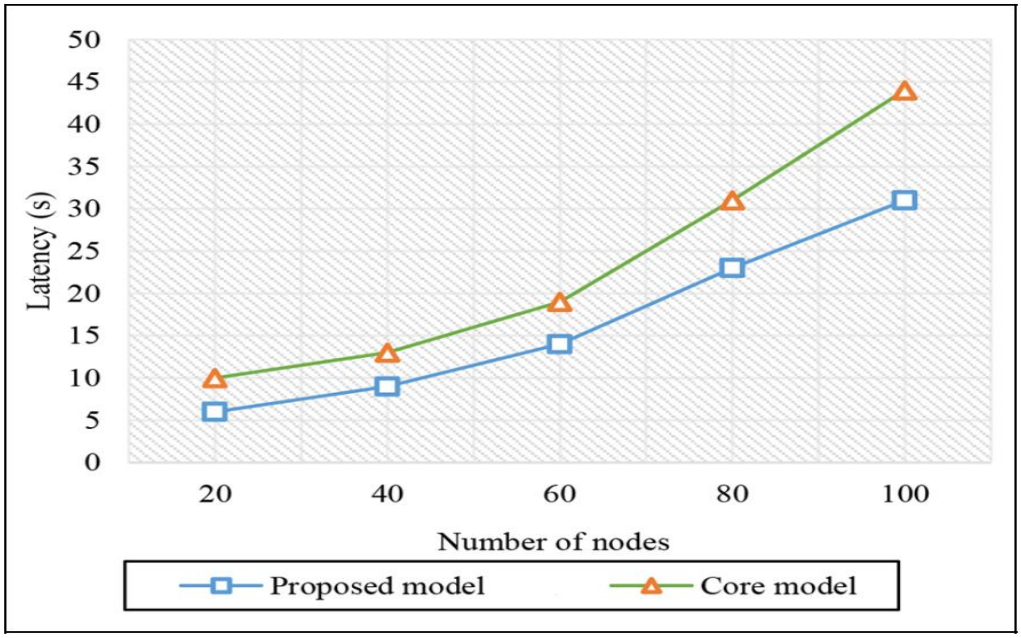
يمثل الشكل 5-8 مقدار التأخير الزمني للرّزم العابرة في الشبكة، ونلاحظ أن هذا التأخير يزداد بازدياد عدد المناقلات، وأيضاً بزيادة عدد العقد المكونة للشبكة.

بينما يمثّل الشكل 5-9 مقدار الأعباء المحملة على العقد، حيث نلاحظ أن الحمل يزداد بزيادة عدد العقد في الشبكة، كما يزداد بزيادة عدد المناقلات في الشبكة.



الشكل 5-9 علاقة الأعباء المحمَّلة بعدد العقد وعدد المناقلات.

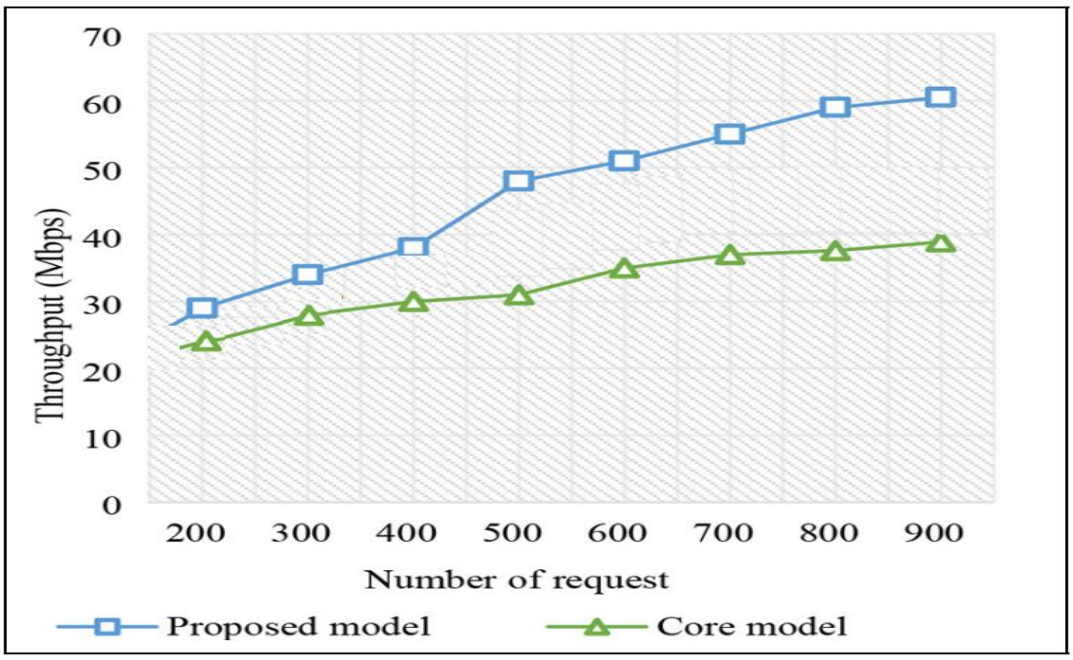
ويمثل الشكل 5-10 زمن الاستجابة للشبكة باستخدام حلنا المقترح ومقارنته مع نموذج أساسي core model والذي يمثل التخزين السحابي لانترنت الأشياء باستخدام سلسلة الكتل دون استخدام خوارزميات التحسين.



الشكل 5-10 مقارنة زمن الاستجابة في النموذج المقترح مع نموذج أساسي.

نلاحظ من الشكل 5-10 أن زمن الاستجابة في حالة نموذجنا المقترح أقل من الزمن في الحالة الاساسية، ويزداد بزيادة عدد العقد الموجودة.

بينما يمثل الشكل 5-11 مقارنة مقدار الإنتاجية بين حلنا المقترح وبين النموذج الاساسي الموجود دون خوارزميات التحسين. ونلاحظ منه أن الإنتاجية قد تحسنت بالفعل نتيجة استخدامنا للنموذج المقترح.



الشكل 5-11 مقارنة الإنتاجية في النموذج المقترح مع النموذج الأساسي.

5.5- تحليل النموذج المقترح

نناقش الآن المسائل الأمنية والخصوصية للنموذج المقترح، حيث يمكن أن تكون العقدة الخبيثة (أو مجموعة متعاونة من العقد الخبيثة) هي OBM أو أحد أجهزة المنزل الذكي أو عقدة في overlay، أو التخزين السحابي. يمكن لتلك العقد التنصت على الاتصالات، إلغاء المناقلات، توليد مناقلات وكتل خاطئة، تغيير وحذف بيانات من التخزين، أو تحليل العديد من المناقلات في محاولة إفشاء هوية العقدة وتوقيع مناقلات مزيّفة للتغطية على العقد الخبيثة.

1.5.5- الأمن

يلخِّص الجدول 5-1 الآليات المختلفة التي تسمح لحلنا المقترح بتلبية المتطلبات الأساسية للأمن.

الجدول 5-1 مناقشة المتطلّبات الأمنية للنموذج المقترَح.

متطلبات الأمن	الطريقة المستخدَمة
السرية	استخدام التعمية (متناظرة وغير متناظرة) لكل المناقلات
السلامة	تحوي كل مناقلة على قيمة تهشير لكل حقولها
التوافرية	يعالج LBM كل المناقلات الواردة ويتحكم بالوصول إلى كل أجهزة المنزل الذكي.

	يرسل OBM المناقلة إلى عناصر عنقوده فقط إذا توافق المفتاح الموجود فيها مع أحد قيم المفاتيح في قائمة المفاتيح المحفوظة لديه مما يضمن استلام عناصر العنقود للمناقلات من عقد مخولة فقط.
المصادقة	يولّد LBM في المنزل الذكي مفتاحاً مشتركاً بين كل جهازين يتصلان ببعضهما، ويستخدَم ذلك المفتاح أيضاً للمصادقة. ينبغي على كل عقدة في overlay أن تحوي مناقلةَ genesis مخزّنة في سلسلة الكتل العامة لتجري مصادقتها من خلال امتلاكها للمفتاح الخاص المتوافق مع المفتاح العام الموجود في المناقلة المخزنة في سلسلة الكتل كون تلك المناقلات مرتبطة مع مناقلة genesis.
عدم الإنكار	يجري توقيع مناقلات overlay من قبل مولِّديها لضمان عدم الإنكار، إضافةً إلى تخزين كل تلك المناقلات في سلسلة الكتل العامة مما يمنع مولّد ومستقبل المناقلة من إنكار اشتراكه بها

بينما نلخّص في الجدول 5-2 عدداً من الهجومات التي يمكن أن تستهدِف شبكات انترنت الأشياء وسلسلة الكتل، ونوضّح آلية حماية الحل المقترح من تلك الهجمات.

الجدول 5-2 مناقشة بعض الهجمات الأمنية على النموذج.

الهجوم	تعريفه	آلية الحماية
Appending Attack	يقوم المهاجم بإنشاء كتل مع مناقلات وهمية	يمكن لد OBM اكتشاف الكتلة الوهمية خلال مرحلة التحقق
Denial of Service Attack (DoS)	يقوم المهاجم بإغراق العقدة بعدد كبيرمن المناقلات	تقوم كل OBM بإرسال المناقلات لأعضاء العنقود فقط ، ويكون لكل عقدة حد أعلى من عدد المناقلات المسموح بها
Device injection attack	يقدم المهاجم أجهزة وهمية إلى المنزل الذكي للحصول على المعلومات	يجري عزل الجهاز نتيجة استخدام المفتاح المشترك عند كل LBM
False reputation	يقوم المهاجم بزيادة السمعة عن طريق زيادة output[0]	تستطيع OBM اكتشاف الزيادة الزائفة من خلال خوارزمية التوافق

2.5.5- الخصوصية

يستخدِم النموذج المقترح آليات إخفاء الهوية (anonymity) وتحكّم المستخدم (user control) لحماية خصوصية المستخدمين في المنزل الذكي وفي overlay وفي السحابة. يضمن استخدام المفاتيح العمومية المتغيرة كمعرّف لعقد overlay مستوىً مشابه من الخصوصية وإخفاء الهوية للأنظمة الأخرى القائمة على سلسلة الكتل (مثل البتكوين). تجري تعمية المناقلات المخزّنة في سلسلة الكتل العامة بالمفتاح العمومي لـ requestee لحماية خصوصية عقد overlay من المهاجمين الذين يحاولون قراءة بيانات في حقل البيانات للمناقلة متعددة التواقيع. كما يجري في المنزل الذكي فرض قواعد المالك من قبل LBM لضمان تحكّمه بالبيانات المتبادَلة وبالتالي حماية الخصوصية. يمكن للسحابة استخدام بيانات الأجهزة المختلفة لعقد overlay بغرض الحصول على الهوية الحقيقية، لذا تستخدِم تلك العقد حسابات (credits) متباينة لتخزين بيانات أجهزتها، مما يمنع السحابة من معرفة الأجهزة المختلفة العائدة لنفس عقدة overlay.

3.5.5- تقييم خوارزمية الثقة الموزّعة

يجري في سلاسل الكتل التقليدية التحقق من صحة جميع مناقلات الكتلة كي تعتبَر الكتلة صالحة، بينما نستخدِم في نموذجنا خوارزميةَ الثقة الموزّعة التي تساهم في التناقص التدريجي لعدد المناقلات الواجب التحقق من صحتها لاعتبار الكتلة صالحة حيث تبني الـ OBMs جداولَ ثقةٍ عن بعضها البعض.

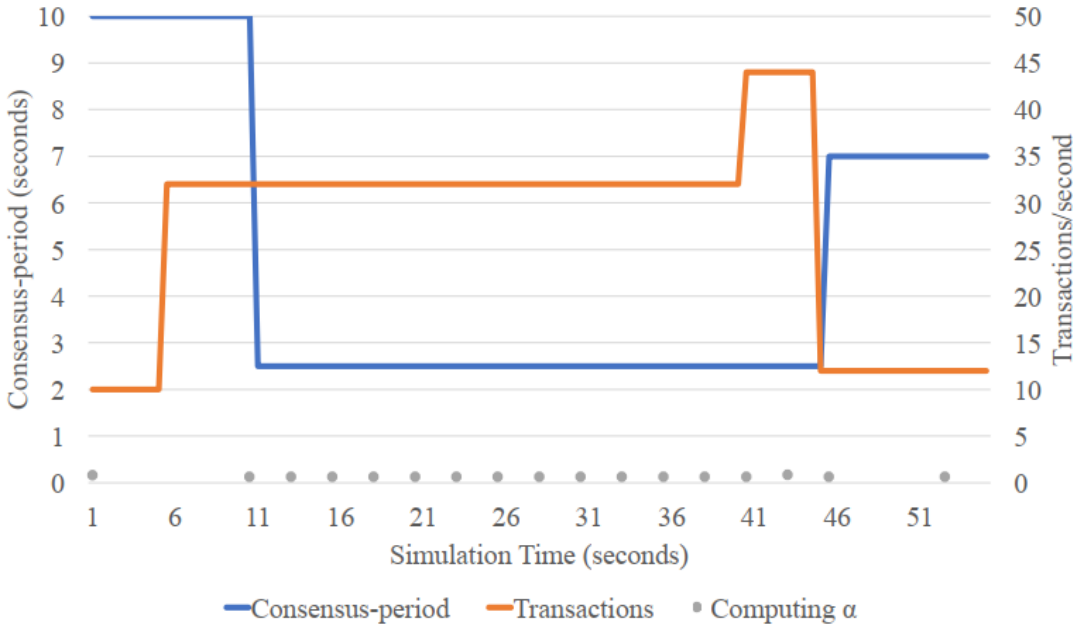
4.5.5- تقييم أداء DTM

تهدُف آلية DTM كما وضحنا سابقاً إلى ضبط مردود (utilization) الشبكة بشكل ديناميكي استناداً إلى الحمل الكلّي، أي عدد المعاملات التي يجري توليدها. ولتوضيح أداء DTM، قمنا بمحاكاة شبكة بإعدادات افتراضية بـ 13 عقدة تعمل كـ OBMs، قمنا بمحاكاة حالات يتغير فيها الطلب على الشبكة، فجرى في البداية توليد 10 مناقلات تراكمية، ثم زاد العدد إلى 32 مناقلة في الثانية في المجال الزمني من 5 إلى 40 ثانية، وإلى 44 مناقلة في الثانية في المجال من 40 إلى 45 ثانية ثم تناقص الحمل إلى 12 مناقلة في الثانية كما هو موضح في الشكل 5-12.

قمنا بضبط قيمة دور التوافق في البداية إلى 10 ثواني ، وافترضنا أن $\alpha_{min} = 0.25$، $\alpha_{max} = 1$. نلاحظ بعد أول دور توافق (أي بعد 10 ثواني) أن $\alpha = 2.4$ وهي أكبر من α_{max} وذلك بسبب الزيادة الحادة في حمل الشبكة عند الزمن 5 ثانية، لذا تقوم DTM بمحاولة إنقاص قيمة مردود الشبكة α من خلال إنقاص قيمة دور

التوافق إلى 2.5 ثانية باستخدام المعادلة (2-4) وباستخدام القيمة الوسطى لـ α وهي 0.62، ثم يبقى دور التوافق ثابتاً طالما الشبكة مستقرة أي حتى اللحظة 40 ثانية.

بعد هذه اللحظة يزداد حمل الشبكة، لذلك يجري بعد دور التوافق التالي (أي عند 43 ثانية) إعادة حساب α لتصبح 0.84 وهي ضمن المجال المرغوب فلا يُتّخَذ أي إجراء، مما يثبت فعالية اختيار α كنقطة وسطى للمجال $[\alpha_{min}, \alpha_{max}]$. ثم تنخفض قيمة α إلى 0.2 عند اللحظة 48 ثانية بسبب الانخفاض الحاد في عدد المناقلات عند اللحظة 45 ثانية، وبما أن قيمة α الجديدة هي أصغر من α_{min}، تقوم DTM بزيادة دور التوافق إلى قيمة جديدة وهي 7 ثواني.



الشكل 5-12 حساب دور التوافق اعتماداً على عدد المناقلات.

6.5- خاتمة

قمنا في هذا الفصل بالتعرف إلى أداة المحاكاة المستخدَمة (Cooja)، ثم تنفيذ المحاكاة لعدّة سيناريوهات وتقييم أداء النموذج المقترح باستخدام عدّة معايير، وعرضنا النتائج التي تدعم قدرة هذا النموذج في حماية أمن وخصوصية انترنت الأشياء باستخدام سلسلة الكتل.

الفصل السادس

الخاتمة والآفاق المستقبلية

نختم عملنا في هذا الفصل ونتحدّث عن آفاقه المستقبلية.

1.6- الخاتمة

قدمنا في هذا البحث عرضاً وافياً وتفصيلياً لتقنية سلسلة الكتل مع أحدث الدراسات المرجعية، وكذلك لتوصيف انترنت الاشياء، ومن ثم عرضنا التحديات الأمنية التي تواجه كل منهما وأحدث الدراسات التي قامت بالتعامل مع تلك التحديات.

ثم قدمنا توصيفاً وخوارزميات استخدام سلسلة الكتل في انترنت الأشياء، وبالتالي الاستفادة من مزايا سلاسل الكتل دون الوقوع في المشاكل الأمنية التي تصيب تلك الشبكات.

وقد توصلنا إلى اقتراح نموذج وحل لشبكة ذكية فعالة وآمنة تتميز بالخصوصية، وتعتمد على تقنية سلسلة الكتل. وقد بني هذا النموذج بجزئين رئيسيين:

- بناء الشبكة دون الحاجة إلى وجود سلطة مركزية.
- استخدام خوارزميات التعمية المتناظرة وغير المتناظرة لحماية المعلومات المتبادلة.

وقد أثبتت هذه التقنيات المستخدمة فعاليتها في تهيئة وبناء الشبكة في المرحلة الأولى، ومن ثم قدرتها على صد معظم الهجمات الأمنية التي يمكن أن تتعرض له هذه الشبكات. وبالتالي ضمان سرية وخصوصية هذا النوع من الشبكات دون الخسارة في أدائها أو التقليل من مواردها.

كما استطاع هذا الحل المقترح إضفاء العديد من الميزات على استخدام سلسلة الكتل في انترنت الاشياء، وأهمها:

- سهولة بناء الشبكة.

- سهولة إجراء المصادقة بين عقد الشبكة.
- سهولة التحقق من العقد الخبيثة التي تحاول الدخول أو التنصت.
- المناعة العالية ضد أغلب الهجمات الأمنية المحتملة.
- تأمين الخدمات الأمنية الاساسية: المصادقة، وسلامة المعطيات، وسريتها، وعدم الإنكار، بالإضافة إلى تحسين الخصوصية.

ولاننسى أن الحوسبة السحابية المستخدمة قد وسعت من آفاق استخدام البيئات الذكية، وبالتالي زيادة عدد المستخدمين لتلك التقنيات، وهذا يضعنا أمام تحديات عديدة، ما يجعل استخدام التعمية المتناظرة الخفيفة ARX وآلية حساب الثقة الموزعة فعالة جداً في هذا المجال.

2.6- الآفاق المستقبلية

- تطوير النموذج المقترَح لمحاكاته بشكل عملي باستخدام شبكات الحساسات أو الحساسات الفيزيائية في المنزل الذكي.
- متابعة العمل في الجزء السحابي من حيث تأمين المعلومات وتوزيعها بشكل سري وموثوق، والقدرة على استرجاعها بطريقة آمنة.
- زيادة سرية وخصوصية عقد overlay من خلال استخدام تقنيات التعمية لجداول التحكم الموجودة.
- محاولة الوصول إلى الحل الأمثلي من حيث الاستطاعة الصغرى والمجال الأصغري بالإضافة إلى السرعة الأعلى عند تطبيق هذا النموذج.
- محاولة تعميم النموذج المقترح لتطبيقه على بيئات ذكية أخرى كالمدن الذكية.

الملاحق

الملحق آ

خوارزمية Diffie-Hellman لتبادل المفاتيح

تسمح هذه الخوارزمية لمستخدمَين بالتبادل الآمن للمفتاح الخاص المشترَك [6]، والذي سيستخدَم فيما بعد لتعمية الرسائل بينهما. تعتمد هذه الخوارزمية في فعاليتها على صعوبة حساب اللوغاريتم المتقطّع الذي يمكننا اختصاره كالتالي:

1. نعرّف الجذر الأولي (Primitive Root) للعدد الأولي p باعتباره الجذر الذي نستطيع بحساب ناتج رفعه إلى قوى أن نحصل على الاعداد الصحيحة من 1 إلى p-1 كالتالي:

$$a \bmod p, a^2 \bmod p, \ldots., a^{p-1} \bmod p$$

2. من أجل أي عدد صحيح b أصغر من p، وبفرض a هو الجذر الأولي لـ p، يمكننا إيجاد أس وحيد i يحقق:

$$b = a^i \bmod p \qquad 0 \leq i \leq (p-1)$$

حيث نسمّي الأس i اللوغاريتم المتقطع (أو الدليل) للعدد b بالأساس a ونعبّر عن ذلك بالعلاقة:

$$i = dlog_{a,p}(b)^2$$

الخوارزمية:

يمكننا الآن تعريف الخوارزمية بعد أن أجرينا نظرة عامة على اللوغاريتم المتقطّع، يوضّح الجدول الملحق 1 تسلسل عمل تلك الخوارزمية [6]، لدينا رقمان معروفان هما:

- q: عدد أولي.
- α: هو عدد صحيح يمثّل جذر أولي للعدد q.

نفترض أن لدينا مستخدِمان A وB يريدان تبادل مفتاح خاص، تجري العملية كالتالي:

1. يختار المستخدِم A عدد صحيح X_A يحقق $X_A < q$، ثم يقوم بحساب $Y_A = \alpha^{X_A} \bmod q$، كما يختار المستخدم B عدد صحيح X_B يحقق $X_B < q$، ثم يقوم بحساب $Y_B = \alpha^{X_B} \bmod q$. يحتفظ كلا المستخدمَين بالقيمة X بشكل سرّي، بينما يجعل كل منهما القيمة Y متوفّرة للطرف الآخر.

2. يقوم المستخدِم A بحساب المفتاح $K = (Y_B)^{X_A} \bmod q$، بينما يحسُب المستخدِم B المفتاح:

$$K = (Y_A)^{X_B} \bmod q.$$

3. تعطي الحسابات في الخطوة السابقة نتيجة مماثلة لأن:

$$K = (Y_B)^{X_A} \bmod q$$
$$= (\alpha^{X_B} \bmod q)^{X_A} \bmod q$$
$$= (\alpha^{X_B})^{X_A} \bmod q$$
$$= \alpha^{X_B X_A} \bmod q$$
$$= (\alpha^{X_A})^{X_B} \bmod q$$
$$= (\alpha^{X_A} \bmod q)^{X_B} \bmod q$$
$$= (Y_A)^{X_B} \bmod q$$

الملحق 1 خوارزمية **Diffie_Hellman** لتبادل المفاتيح.

Global Public Elements	
q	Prime number
α	α < q and α is a primitive root of q
User "A" key generation	
Select Private X_A	$X_A < q$
Calculate public Y_A	$Y_A = \alpha^{X_A} \bmod q$
User "B" key generation	
Select Private X_B	$X_B < q$
Calculate public Y_B	$Y_B = \alpha^{X_B} \bmod q$
Generation of secret key by user "A"	
$K = (Y_B)^{X_A} \bmod q$	
Generation of secret key by user "B"	
$K = (Y_A)^{X_B} \bmod q$	

المراجع

[1] Statista, “IoT: Numberof Connected Devices Worldwide 2015-2025,” *Statista Research Department*, 2018. [Online]. Available: https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/.

[2] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao, “A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications,” *IEEE Internet Things J.*, 2017.

[3] W. Ejaz and A. Anpalagan, *Internet of Things for Smart Cities: Technologies, Big Data and Security*. Springer, 2019.

[4] A. Whitmore, A. Agarwal, and L. Da Xu, “The Internet of Things---A survey of topics and trends,” *Inf. Syst. Front.*, vol. 17, no. 2, pp. 261–274, Apr. 2015.

[5] L. Lilien, A. Al-Alawneh, and L. Ben Othmane, “The pervasive trust foundation for security in next generation networks,” in *Proceedings New Security Paradigms Workshop*, 2010.

[6] W. Stallings and B. Lawrie, *Computer security: principles and practice*. Pearson Education, Inc, 2018.

[7] L. Buttyan and J.-P. Hubaux, *Security and cooperation in wireless networks: thwarting malicious and selfish behavior in the age of ubiquitous computing*. Cambridge University Press, 2007.

[8] A. A. Yavuz, A. Mudgerikar, A. Singla, I. Papapanagiotou, and E. Bertino, “Real-Time Digital Signatures for Time-Critical Networks,” *IEEE Trans. Inf. Forensics Secur.*, vol. 12, no. 11, pp. 2627–2639, Nov. 2017.

[9] C. M. Medaglia and A. Serbanati, “An Overview of Privacy and Security Issues in the Internet of Things,” in *The Internet of Things*, 2010.

[10] D. Miorandi, S. Sicari, F. De Pellegrini, and I. Chlamtac, “Internet of things: Vision, applications and research challenges,” *Ad Hoc Networks*, vol. 10, no. 7, pp. 1497–1516, Sep. 2012.

[11] D. M. Mendez, I. Papapanagiotou, and B. Yang, “Internet of things: Survey on security and privacy,” *arXiv Prepr. arXiv1707.01879*, 2017.

[12] H. Suo, J. Wan, C. Zou, and J. Liu, “Security in the internet of things: A review,” in *Proceedings - 2012 International Conference on Computer Science and Electronics Engineering, ICCSEE 2012*, 2012.

[13] J. Lee and H. Kim, “Security and Privacy Challenges in the Internet of Things [Security and Privacy Matters],” *IEEE Consum. Electron. Mag.*, vol. 6, no. 3, pp. 134–136, Jul. 2017.

[14] A. R. Sadeghi, C. Wachsmann, and M. Waidner, “Security and privacy challenges

in industrial Internet of Things," in *Proceedings - Design Automation Conference*, 2015.

[15] P. Kasinathan, C. Pastrone, M. A. Spirito, and M. Vinkovits, "Denial-of-Service detection in 6LoWPAN based Internet of Things," in *International Conference on Wireless and Mobile Computing, Networking and Communications*, 2013.

[16] R. Roman, J. Zhou, and J. Lopez, "On the features and challenges of security and privacy in distributed internet of things," *Comput. Networks*, 2013.

[17] O. Vermesan and P. Friess, *Internet of things: converging technologies for smart environments and integrated ecosystems*. River publishers, 2013.

[18] J. A. Stankovic, "Research directions for the internet of things," *IEEE Internet Things J.*, 2014.

[19] R. H. Weber, "Internet of things: Privacy issues revisited," *Comput. Law Secur. Rev.*, vol. 31, no. 5, pp. 618–627, 2015.

[20] W. Trappe, R. Howard, and R. S. Moore, "Low-energy security: Limits and opportunities in the internet of things," *IEEE Secur. Priv.*, 2015.

[21] H. Shafagh, A. Hithnawi, A. Dröscher, S. Duquennoy, and W. Hu, "Poster: Towards encrypted query processing for the Internet of Things," in *Proceedings of the 21st annual international conference on mobile computing and networking*, 2015, pp. 251–253.

[22] R. Kotamsetty and M. Govindarasu, "Adaptive latency-aware query processing on encrypted data for the internet of things," in *2016 25th International Conference on Computer Communications and Networks, ICCCN 2016*, 2016.

[23] S. Al Salami, J. Baek, K. Salah, and E. Damiani, "Lightweight encryption for smart home," in *Proceedings - 2016 11th International Conference on Availability, Reliability and Security, ARES 2016*, 2016.

[24] M. A. Khan and K. Salah, "IoT security: Review, blockchain solutions, and open challenges," *Futur. Gener. Comput. Syst.*, vol. 82, pp. 395–411, May 2018.

[25] T. Pecorella, L. Brilli, and L. Mucchi, "The role of physical layer security in IoT: A novel perspective," *Inf.*, 2016.

[26] Owasp, "Top IoT Vulnerabilities." [Online]. Available: https://www.owasp.org/index.php/Top_IoT_Vulnerabilities.

[27] T. Bhattasali and R. Chaki, "A Survey of Recent Intrusion Detection Systems for Wireless Sensor Network," in *International conference on network security and applications*, 2011, pp. 268–280.

[28] H. Kim, "Protection Against Packet Fragmentation Attacks at 6LoWPAN Adaptation Layer," in *2008 International Conference on Convergence and Hybrid Information Technology*, 2008, pp. 796–801.

[29] R. Riaz, K. H. Kim, and H. F. Ahmed, "Security analysis survey and framework design for IP connected LoWPANs," in *Proceedings - 2009 International Symposium on Autonomous Decentralized Systems, ISADS 2009*, 2009.

[30] R. Hummen, J. Hiller, H. Wirtz, M. Henze, H. Shafagh, and K. Wehrle, "6LoWPAN fragmentation attacks and mitigation mechanisms," in *WiSec 2013 - Proceedings of the 6th ACM Conference on Security and Privacy in Wireless and Mobile Networks*, 2013.

[31] A. Dvir, T. Holczer, and L. Buttyan, "VeRA - Version number and rank authentication in RPL," in *Proceedings - 8th IEEE International Conference on Mobile Ad-hoc and Sensor Systems, MASS 2011*, 2011.

[32] K. Weekly and K. Pister, "Evaluating sinkhole defense techniques in RPL networks," in *Proceedings - International Conference on Network Protocols, ICNP*, 2012.

[33] A. A. Pirzada and C. McDonald, "Circumventing sinkholes and wormholes in wireless sensor networks," in *IWWAN'05: Proceedings of International Workshop on Wireless Ad-hoc Networks*, 2005, vol. 71.

[34] P. N. Mahalle, B. Anggorojati, N. R. Prasad, and R. Prasad, "Identity authentication and capability based access control (IACAC) for the internet of things," *J. Cyber Secur. Mobil.*, 2013.

[35] T. Kothmayr, C. Schmitt, W. Hu, M. Brünig, and G. Carle, "DTLS based security and two-way authentication for the Internet of Things," *Ad Hoc Networks*, 2013.

[36] J. M. Bohli, A. Skarmeta, M. Victoria Moreno, D. Garcia, and P. Langendorfer, "SMARTIE project: Secure IoT data management for smart cities," in *2015 International Conference on Recent Advances in Internet of Things, RIoT 2015*, 2015.

[37] G. Peretti, V. Lakkundi, and M. Zorzi, "BlinkToSCoAP: An end-to-end security framework for the Internet of Things," in *2015 7th International Conference on Communication Systems and Networks (COMSNETS)*, 2015, pp. 1–6.

[38] H. C. Pöhls *et al.*, "RERUM: Building a reliable IoT upon privacy- and security-enabled smart objects," in *2014 IEEE Wireless Communications and Networking Conference Workshops, WCNCW 2014*, 2014.

[39] S. Perez, J. A. Martinez, A. F. Skarmeta, M. Mateus, B. Almeida, and P. Malo, "ARMOUR: Large-scale experiments for IoT security & trust," in *2016 IEEE 3rd World Forum on Internet of Things, WF-IoT 2016*, 2017.

[40] S. Raza, T. Voigt, and V. Jutvik, "Lightweight IKEv2: a key management solution for both the compressed IPsec and the IEEE 802.15. 4 security," in *Proceedings of the IETF workshop on smart object security*, 2012, vol. 23.

[41] N. Park and N. Kang, "Mutual Authentication Scheme in Secure Internet of Things Technology for Comfortable Lifestyle," *Sensors*, vol. 16, no. 1, p. 20, Dec. 2016.

[42] M. H. Ibrahim, "Octopus: An Edge-fog Mutual Authentication Scheme.," *IJ Netw. Secur.*, vol. 18, no. 6, pp. 1089–1101, 2016.

[43] M. Brachmann, S. L. Keoh, O. G. Morchon, and S. S. Kumar, "End-to-end transport security in the IP-based internet of things," in *2012 21st International Conference on Computer Communications and Networks, ICCCN 2012 -*

Proceedings, 2012.

[44] M. Sethi, J. Arkko, and A. Keränen, “End-to-end security for sleepy smart object networks,” in *37th Annual IEEE Conference on Local Computer Networks-Workshops*, 2012, pp. 964–972.

[45] D. Conzon, T. Bolognesi, P. Brizzi, A. Lotito, R. Tomasi, and M. A. Spirito, “The VIRTUS middleware: An XMPP based architecture for secure IoT communications,” in *2012 21st International Conference on Computer Communications and Networks, ICCCN 2012 - Proceedings*, 2012.

[46] X. Li, P. Jiang, T. Chen, X. Luo, and Q. Wen, “A survey on the security of blockchain systems,” *Futur. Gener. Comput. Syst.*, no. Xiaoqi Li, pp. 1–25, 2017.

[47] A. Bahga and V. K. Madisetti, “Blockchain platform for industrial internet of things,” *J. Softw. Eng. Appl.*, vol. 9, no. 10, p. 533, 2016.

[48] I. C. Lin and T. C. Liao, “A survey of blockchain security issues and challenges,” *Int. J. Netw. Secur.*, 2017.

[49] A. M. Antonopoulos, *Mastering Bitcoin: unlocking digital cryptocurrencies*. “ O’Reilly Media, Inc.,” 2015.

[50] S. Nakamoto and others, “Bitcoin: a peer-to-peer electronic cash system (2008).” 2008.

[51] L. Luu, D. H. Chu, H. Olickel, P. Saxena, and A. Hobor, “Making smart contracts smarter,” in *Proceedings of the ACM Conference on Computer and Communications Security*, 2016.

[52] H. Mayer, “ECDSA Security in Bitcoin and Ethereum : a Research Survey,” *Blog.Coinfabrik*, 2016.

[53] A. Zaharia, “What You Need to Know About CTB Locker, a New Generation Ransomware [UPDATED],” *Heimdal Security*, 2019. [Online]. Available: https://heimdalsecurity.com/blog/ctb-locker-ransomware/.

[54] Z. Whittaker, “Two years after WannaCry, a million computers remain at risk,” *TechCrunch*, 2019. [Online]. Available: https://techcrunch.com/2019/05/12/wannacry-two-years-on/.

[55] G. O. Karame, E. Androulaki, and S. Čapkun, “Double-spending fast payments in Bitcoin,” in *Proceedings of the ACM Conference on Computer and Communications Security*, 2012.

[56] A. Miller *et al.*, “An Empirical Analysis of Linkability in the Monero Blockchain,” *CoRR*, 2017.

[57] A. Juels, A. Kosba, and E. Shi, “The ring of gyges: Investigating the future of criminal smart contracts,” in *Proceedings of the ACM Conference on Computer and Communications Security*, 2016.

[58] N. Atzei, M. Bartoletti, and T. Cimoli, “A survey of attacks on Ethereum smart contracts (SoK),” in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2017.

[59] I. Eyal and E. G. Sirer, “Majority Is Not Enough: Bitcoin mining is vulnerable,” *Commun. ACM*, 2018.

[60] M. Apostolaki, A. Zohar, and L. Vanbever, “Hijacking Bitcoin: Routing Attacks on Cryptocurrencies,” in *Proceedings - IEEE Symposium on Security and Privacy*, 2017.

[61] Dyn, “Pakistan hijacks YouTube: Dyn Blog,” *Dyn Guest Blogs*, 2018. [Online]. Available: https://dyn.com/blog/pakistan-hijacks-youtube-1/.

[62] E. Heilman, A. Kendler, A. Zohar, and S. Goldberg, “Eclipse Attacks on Bitcoin’s Peer-to-Peer Network,” *USENIX Secur. Symp.*, 2015.

[63] A. Kiayias and G. Panagiotakos, “On Trees, Chains and Fast Transactions in the Blockchain,” 2019.

[64] C. Natoli and V. Gramoli, “The balance attack against proof-of-work blockchains: The R3 testbed as an example,” *arXiv Prepr. arXiv1612.09426*, 2016.

[65] L. Luu, Y. Velner, J. Teutsch, and P. Saxena, “SMART POOL : Practical Decentralized Pooled Mining.,” *IACR Cryptol. ePrint Arch.*, 2017.

[66] A. Gervais, G. O. Karame, K. Wüst, V. Glykantzis, H. Ritzdorf, and S. Čapkun, “On the security and performance of Proof of Work blockchains,” in *Proceedings of the ACM Conference on Computer and Communications Security*, 2016.

[67] A. Kosba, A. Miller, E. Shi, Z. Wen, and C. Papamanthou, “Hawk: The Blockchain Model of Cryptography and Privacy-Preserving Smart Contracts,” in *Proceedings - 2016 IEEE Symposium on Security and Privacy, SP 2016*, 2016.

[68] F. Zhang, E. Cecchetti, K. Croman, A. Juels, and E. Shi, “Town crier: An authenticated data feed for smart contracts,” in *Proceedings of the ACM Conference on Computer and Communications Security*, 2016.

[69] Y. Zhang, D. He, and K. K. R. Choo, “BaDS: Blockchain-based architecture for data sharing with ABS and CP-ABE in IoT,” *Wirel. Commun. Mob. Comput.*, 2018.

[70] Y. Rahulamathavan, R. C. W. Phan, M. Rajarajan, S. Misra, and A. Kondoz, “Privacy-preserving blockchain based IoT ecosystem using attribute-based encryption,” in *11th IEEE International Conference on Advanced Networks and Telecommunications Systems, ANTS 2017*, 2018.

[71] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, “Lsb: A lightweight scalable blockchain for iot security and privacy,” *arXiv Prepr. arXiv1712.02969*, 2017.

[72] C. Li and L. J. Zhang, “A blockchain based new secure multi-layer network model for internet of things,” in *Proceedings - 2017 IEEE 2nd International Congress on Internet of Things, ICIOT 2017*, 2017.

[73] G. C. Polyzos and N. Fotiou, “Blockchain-assisted information distribution for the internet of things,” in *Proceedings - 2017 IEEE International Conference on Information Reuse and Integration, IRI 2017*, 2017.

[74] M. Conoscenti, A. Vetro, and J. C. De Martin, “Blockchain for the Internet of Things: A systematic literature review,” in *Proceedings of IEEE/ACS International Conference on Computer Systems and Applications, AICCSA*, 2017.

[75] N. Kshetri, “Can Blockchain Strengthen the Internet of Things?,” *IT Prof.*, 2017.

[76] F. Tian, “A supply chain traceability system for food safety based on HACCP, blockchain & Internet of things,” in *14th International Conference on Services Systems and Services Management, ICSSSM 2017 - Proceedings*, 2017.

[77] M. Samaniego and R. Deters, “Internet of Smart Things - IoST: Using Blockchain and CLIPS to Make Things Autonomous,” in *Proceedings - 2017 IEEE 1st International Conference on Cognitive Computing, ICCC 2017*, 2017.

[78] A. Dorri, S. S. Kanhere, and R. Jurdak, “Towards an optimized blockchain for IoT,” in *Proceedings - 2017 IEEE/ACM 2nd International Conference on Internet-of-Things Design and Implementation, IoTDI 2017 (part of CPS Week)*, 2017.

[79] A. Kousaridas, S. Falangitis, P. Magdalinos, N. Alonistioti, and M. Dillinger, “SYSTAS: Density-based algorithm for clusters discovery in wireless networks,” in *IEEE International Symposium on Personal, Indoor and Mobile Radio Communications, PIMRC*, 2015.

[80] A. Bogdanov, M. Knežević, G. Leander, D. Toz, K. Varici, and I. Verbauwhede, “Spongent: A lightweight hash function,” in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2011.

[81] R. Beaulieu, S. Treatman-Clark, D. Shors, B. Weeks, J. Smith, and L. Wingers, “The SIMON and SPECK lightweight block cIPhers,” in *Proceedings - Design Automation Conference*, 2015.

[82] L. Malina, J. Hajny, P. Dzurenda, and S. Ricci, “Lightweight Ring Signatures for Decentralized Privacy-preserving Transactions,” 2018.

[83] R. L. Rivest, A. Shamir, and Y. Tauman, “How to leak a secret,” in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2001.

[84] Cooja, “Contiki.” [Online]. Available: http://anrg.usc.edu/contiki/index.php/CoojaSimulator.

[85] G. Rubino, “Ethereum Explained: Merkle Trees, World State, Transactions, and More,” *PEGASYS.Tech*, 2018. [Online]. Available: https://pegasys.tech/ethereum-explained-merkle-trees-world-state-transactions-and-more/.

الملخص

وسّعَت أنظمة أنترنت الأشياء (IoT) مجالَ الشبكات إلى عشرات المليارات من الأجهزة المتّصلة، وأصبح من الصعب حماية أمنها وخصوصية بيانات مستخدميها بسبب عدم تجانس الأطراف المتّصلة وتمتّعها بخصائص مميّزة تجعل من الصعب تطبيق الحلول الأمنية التقليدية. لذا، نهدُف في هذه الأطروحة إلى إيجاد منصّة أمنية لحماية خصوصية أجهزة انترنت الأشياء في بيئة المنزل الذكي الذي يعتبَر من أهم تطبيقات IoT، وذلك اعتماداً على تقنية سلسلة الكتل (blockchain) التي حصدَت اهتماماً كبيراً من قبل الباحثين منذ نشأتها في العملة الرقمية بتكوين، نظراً لطبيعتها الثابتة وميزات الأمن والخصوصية التي تقدّمها، مما يكسبها القدرة للتغلّب على التحديات الأمنية لأنظمة انترنت الأشياء. لكن تعتبَر تقنية سلسلة الكتل مكلفة من حيث العمليات الحسابية، قابلية التوسّع، والتأخير الزمني، وهذا يشكّل تحدّياً في تطبيقها في أنظمة انترنت الأشياء التي يجب أن تكون ديناميكية في انضمام أو مغادرة الأجهزة المتّصلة وتقدِّم غالب خدماتها في الزمن الحقيقي.

يتكوّن النموذج المطروح من عدّة طبقات مصمّمة لتناسب إمكانيات أجهزة انترنت الأشياء، ويجري تطبيقه في المنزل الذكي الذي يحوي تجهيزات وحساسات محدودة الموارد بالمجمل.

يحقّق النموذج المطروح اللّامركزية من خلال استخدام الشبكة الغطاء (overlay) والتي تتكون من أجهزة عالية الموارد تتشارك معاً في إدارة سلسلة كتل عامة (Public BC) تضمن تحقيق الأمن والخصوصية لكافة أطراف الاتصال، يجري تقسيم شبكة الغطاء إلى عناقيد ولكل عنقود مدير هو الذي يمثل عنقوده في المشاركة بإدارة سلسلة الكتل مع المدراء الآخرين. يتضمّن النموذج العديد من التحسينات مثل خوارزمية التوافق الخفيفة وآلية الثقة الموزعة وخوارزميات التعمية المتناظرة وغير المتناظرة من أجل تحقيق السرية والخصوصية للأجهزة الموجودة. وذلك لمحاولة الوصول إلى حل أمثلي غير مكلف حسابياً، وقابل للتوسع الديناميكي، وبتأخير زمني أقل مايمكن.

هذه التحسينات التي سنقوم بها ستساهم في إعطاء العديد من الميزات وأهمها سهولة بناء الشبكة، وكذلك سهولة التحقق من العقد الخبيثة التي تحاول الدخول أو التنصت على الشبكة، وبالتالي المناعة العالية ضد أغلب الهجمات الأمنية المحتملة. أي أن النموذج المقترح قد ساهم في تأمين الخدمات الأمنية الأساسية: المصادقة، سلامة المعطيات، سريتها، عدم الإنكار، بالإضافة إلى تحسين الخصوصية.

سنقوم بتنجيز النموذج باستخدام أداة المحاكاة Cooja، والتي تعمل ضمن نظام التشغيل Contiki، واختباره أمنياً، من خلال منع محاولات دخول أي عقدة خبيثة إلى الشبكة.

Abstract

Internet of Things (IoT) systems have expanded any network to billions of connected devices. However, privacy and security for those networks have become main issues because of the heterogeneity of the parties involved, and the features that make it difficult to implement traditional security solutions. Therefore, the main aim of this study is to create a security platform to protect the privacy of IoT devices in the smart home environment, which is considered one of the most important applications of IoT, based on blockchain technology, which has gained more researchers' interest since the invention of digital currency. Blockchain technology have the ability to overcome the security challenges of IoT systems.

Blockchain technology is heavily costed, less scalability, and much time delay. Those challenges make it very difficult to dynamically join or leave connected devices in real time environment.

Our proposed solution tries to achieve decentralization through using of overlay, which is a network consists of high-resource devices that joint to manage a public blockchain to ensure the security and privacy of all network parties. Overlay is divided into clusters and each cluster has cluster head to participate in the management of the chain blocks with others.

Our solution includes many enhanced algorithms, such as light consensus algorithm, distributed trust mechanism, symmetric and asymmetric encryption algorithms, to achieve the confidentiality and privacy of existing devices. Also, find better solution that is inexpensively, dynamically scalable and less time delay.

These improvements will contribute to give many features in the network, as building network easily, as well as do the verification of malicious nodes that try to eavesdrop. Therefor, giving the network high immunity against most potential security attacks. This means that the proposed model has contributed in provision of basic security services, as well as improving privacy.

We will implement the proposed solution using Cooja emulation tool, which runs within Contici OS, and test its security by blocking any malicious node that attempts to enter the network.