

# **Defense Against Integrity and Privacy Attacks**

**in**

## **The Internet of Things**

A thesis submitted in fulfillment  
of the requirements for the degree of

**Doctor of Philosophy**

by

**Imran Makhdoom**

School of Electrical and Data Engineering  
Faculty of Engineering and Information Technology  
University of Technology Sydney  
NSW 2007, Australia

August 2020



# ABSTRACT

The world is resorting to the Internet of Things for ease of control and monitoring of smart devices. The ubiquitous use of the Internet of Things ranges from Industrial Control Systems to e-Health, e-Commerce, smart cities, supply chain management, smart cars, and a lot more. Such reliance on the Internet of Things is resulting in a significant amount of data to be generated, collected, processed, and analyzed. The big data analytics is no doubt beneficial for business development. However, at the same time, numerous threats such as attacks on message and device integrity, the vulnerability of end-devices to malware attacks, physical compromise of devices, and threats to user data security and privacy pose a great danger to the sustenance of Internet of Things. Therefore, it is the need of the hour to develop a security mechanism for the Internet of Things systems to ensure the integrity and privacy of data being processed by these systems.

This study thus endeavors to highlight most of the known threats at various layers of the Internet of Things architecture with a focus on the anatomy of some of the significant attacks. The research also construes a detailed attack methodology adopted by some of the most successful malware attacks on the Internet of Things, including Industrial Control Systems and Cyber Physical Systems. The study further infers an attack strategy of a Distributed Denial of Service attack through the Internet of Things botnet followed by requisite security measures. The illustration of attack methodologies is followed by a composite guideline for the development of an Internet of Things security framework based on industry best practices.

Sequel to the Internet of Things threat modeling, this research investigates the use of blockchain technology to protect the Internet of Things against data integrity and privacy attacks. Hence, to arrive at intelligible conclusions, a systematic study of the peculiarities of the Internet of Things environment, including its security and performance requirements and progression in blockchain technologies, is carried out. Moreover, this thesis also identifies unique challenges to blockchain's adoption in the Internet of Things and recommends a possible way forward.

Based on a systematic and analytical review of blockchain technology, this study proposes a privacy-preserving and secure data sharing framework for smart cities. The proposed scheme preserves user data privacy by dividing the blockchain network into various channels, where every channel comprises a finite number of authorized organizations and processes a specific type of data such as health, smart car, smart energy, or financial details. Moreover, access to users' data within a channel is controlled by embedding access control rules in the smart contracts. The

devised solution also conforms to some of the essential requirements outlined in the European Union General Data Protection Regulation.

Another important contribution of this work is the conception and design of a novel Internet of Things centric consensus protocol with the Internet of Things focused transaction validation rules. The proposed Proof-of-Honesty consensus protocol not only reduces the possibility of Byzantine behavior by block proposers (validator/mining nodes) during the consensus process but is also scalable with low communication complexity. It is believed that the proposed consensus protocol will prove to be a governing factor for the Internet of Things systems considering to adopt blockchain technology.

Correspondingly, the main conclusion of this research and evaluation is that a sensibly selected and carefully designed blockchain-based IoT application can provide some assurance to the users concerning the security and privacy of their data. In this context, the focus should be on developing an IoT-centric consensus protocol with an intelligent misbehavior detection mechanism to detect and identify malicious miner/validator nodes. Moreover, validation of IoT devices' integrity is also an open challenge that requires due attention.

# STATEMENT OF ORIGINAL AUTHORSHIP

I, Imran Makhdoom, declare that this thesis is submitted in fulfillment of the requirements for the award of the degree of Doctor of Philosophy in the School of Electrical and Data Engineering, Faculty of Engineering and Information Technology, at the University of Technology Sydney.

This thesis is wholly my work unless otherwise referenced or acknowledged. In addition, I certify that all information sources and literature used are indicated in the thesis.

This document has not been submitted for qualifications at any other academic institution.

This research is supported by the Australian Government Research Training Program.

This research was also [partially] supported by funding from Food Agility CRC Ltd, funded under the Commonwealth Government CRC Program. The CRC Program supports industry-led collaboration between industry, researchers, and the community.

Signed:

Production Note:

Signature removed prior to publication.

---

Imran Makhdoom

3 August 2020



# STATEMENT OF THE TYPE OF THESIS

The thesis is structured as a single manuscript comprising a combination of chapters. Whereas, the chapters other than the Introduction Chapter, are the compilation of published/publishable work.





# ACKNOWLEDGEMENTS

I express my profound gratitude to my supervisors, A/Prof Mehran Abolhasan (Principal Supervisor), A/Prof Justin Lipman (Co-Supervisor), and Dr. Wei Ni (External Supervisor) for their fruitful guidance and support throughout my Ph.D. candidature. Their encouragement and regular interactive meetings made my experience very productive. I am especially thankful to Dr. Mehran for his kind support that enabled me to focus on my research. He was also very supportive in terms of providing assistance to me to attend international conferences.

I am also thankful to the University of Technology Sydney for giving me the opportunity to pursue my Ph.D. studies by granting me scholarships to cover my tuition fee and living expenses. I also acknowledge the handwork put in by the School of Electrical and Data Engineering staff to provide efficient admin and academic support to the research students.

In the end, I would like to extend my gratitude to my parents for their kind prayers, my lovely wife for taking care of me and the kids, and also for bearing with me during hard times.



# LIST OF PUBLICATIONS

## Journal Papers

- J-1. I. Makhdoom, M. Abolhasan, J. Lipman, R. P. Liu and W. Ni, "Anatomy of Threats to the Internet of Things," in IEEE Communications Surveys & Tutorials, vol. 21, no. 2, pp. 1636-1675, Secondquarter 2019. **Research Question 1**
- J-2. I. Makhdoom, M. Abolhasan, H. Abbas and W. Ni, "Blockchain's Adoption in IoT: The Challenges, and a Way Forward," Journal of Network and Computer Applications, vol. 125, pp. 251–279, 2018. **Research Question 2**
- J-3. I. Makhdoom, I. Zhou, M. Abolhasan, J. Lipman and W. Ni, "PrivySharing: A Blockchain-Based Framework for Privacy-Preserving and Secure Data Sharing in Smart Cities," Computers & Security, vol. 88, pp. 101653, 2020. **Research Question 3**

## Conference Papers

- C-1. I. Makhdoom, M. Abolhasan, H. Abbas and W. Ni, "Blockchain for IoT: The Challenges and a Way Forward," in 15<sup>th</sup> International Conference on Security and Cryptography (SECRYPT), Porto, Portugal, Jul. 2018, pp. 428-439. **Research Question 2**
- C-2. I. Makhdoom, I. Zhou, M. Abolhasan, J. Lipman and W. Ni, "PrivySharing: A Blockchain-Based Framework for Privacy-Preserving and Secure Data Sharing in Smart Cities," in 16<sup>th</sup> International Conference on Security and Cryptography (SECRYPT), Prague, Czech Republic, Jul. 2019, pp. 363-371. **Research Question 3**
- C-3. I. Zhou, I. Makhdoom, M. Abolhasan, J. Lipman and S. Negin, "A Blockchain-based File-sharing System for Academic Paper Review," in 13<sup>th</sup> International Conference on Signal Processing and Communication Systems (ICSPCS), Gold Coast, Queensland, Australia, Dec. 2019, pp. 1-10.
- C-4. I. Makhdoom, F. Tofigh, I. Zhou, M. Abolhasan and J. Lipman, "PLEDGE: A Proof-of-Honesty based Consensus Protocol for Blockchain-based IoT Systems," **In press** in the IEEE International Conference on Blockchain and Cryptocurrency (ICBC), Toronto, Canada, May. 2020. **Research Question 4**

## **Patents**

- P-1. I. Makhdoom, F. Tofigh, "A Method of Electronic Device Integrity Check Based on Device Digital Genome (D2iGen)," Australia Patent 2018204784, Jun. 29, 2018.

# CONTENTS

<b>1</b>	<b>Introduction</b>	<b>1</b>
1.1	Motivation . . . . .	2
1.2	Challenges . . . . .	3
1.3	Objectives and Research Questions . . . . .	4
1.4	Deliverables . . . . .	5
1.5	Stakeholders . . . . .	5
1.6	Research Methodology . . . . .	5
1.7	Organization of the Thesis . . . . .	6
<b>2</b>	<b>Anatomy of Threats to the IoT</b>	<b>9</b>
2.1	Related Work . . . . .	9
2.2	IoT Architecture . . . . .	10
2.2.1	IoT vs Traditional Networks . . . . .	13
2.3	Generalized Threats . . . . .	14
2.3.1	Security and Privacy Issues . . . . .	15
2.3.2	Threats to eHealth IoT Devices . . . . .	15
2.3.3	Device Integrity Issues . . . . .	15
2.3.4	Software/Code Integrity Issues . . . . .	15
2.3.5	Issues Concerning Communication Protocols . . . . .	16
2.3.6	Hardware Vulnerabilities . . . . .	18
2.3.7	DoS Attacks . . . . .	18
2.3.8	DDoS Attacks . . . . .	18
2.3.9	Security Challenges Specific to WSN . . . . .	18
2.3.10	Security Issues of RFID and Bluetooth Devices . . . . .	18

2.3.11	User Unawareness	19
2.4	Threats at Different Layers of IoT Architecture	19
2.4.1	Physical/Perception Layer	21
2.4.2	MAC/Adaptation/Network Layer	25
2.4.3	Application Layer	25
2.4.4	Semantics Layer	28
2.5	Security and Privacy Challenges to the Cloud-Supported IoT	28
2.5.1	Security of Data	29
2.5.2	Handling of Heterogeneous Data	29
2.5.3	User Anonymity vis-a-vis ID Management	29
2.5.4	In-Cloud Data Sharing	29
2.5.5	Large-Scale Log Management	30
2.5.6	Vulnerability to DoS Attacks	30
2.5.7	The Threat of Malicious Things	30
2.5.8	Security and Privacy Issues in Fog Computing for IoT	31
2.6	Malware Threat	31
2.6.1	Anatomy of Malware	32
2.6.2	Attack Methodology	35
2.7	Gap Analysis and Security Framework	38
2.8	Summary	41
<b>3</b>	<b>Defense-in-Depth Approach</b>	<b>43</b>
3.1	Guidelines for IoT Security Framework	43
3.1.1	Risk Assessment and Threat Modelling	43
3.1.2	Defense-in-Depth	44
3.2	Cost-Benefit Analysis for the Selection of Suitable Security Measure	58
3.3	Conclusions, Lessons Learnt and Pitfalls	60
3.4	Open Research Challenges	64
3.4.1	Baseline Security Standards	64
3.4.2	Privacy-Preserving Data Aggregation and Processing	65
3.4.3	Software/Code Integrity	65
3.4.4	Blockchain - An Instrument to Augment IoT Security	65

3.4.5	Challenges to Fog Computing in IoT . . . . .	66
3.5	Summary . . . . .	68
<b>4</b>	<b>Blockchain's Adoption in the IoT</b>	<b>69</b>
4.1	Introduction . . . . .	69
4.1.1	Related Work . . . . .	70
4.1.2	Contributions of this Chapter . . . . .	71
4.1.3	Organization . . . . .	72
4.2	IoT Requirements . . . . .	72
4.2.1	Security Requirements . . . . .	72
4.2.2	Performance Requirements . . . . .	73
4.3	Blockchain: An Overview . . . . .	74
4.3.1	Key Concepts . . . . .	75
4.3.2	Blockchain Consensus Protocols . . . . .	80
4.4	Progression of Blockchain Technology and its Impact on IoT . . . . .	85
4.5	Challenges to the Blockchain's Adoption in IoT . . . . .	93
4.5.1	Lack of IoT-Centric Consensus Protocol . . . . .	95
4.5.2	TX Validation Rules . . . . .	97
4.5.3	Scalability . . . . .	98
4.5.4	IoT Device Integration . . . . .	99
4.5.5	Protection of IoT Devices against Malware/Remote Code Execution Attacks	100
4.5.6	Secure and Synchronized Software Upgrade . . . . .	100
4.5.7	Additional Issues . . . . .	101
4.6	Latest Trends in Blockchain-based IoT Applications and Related Voids . . . . .	101
4.6.1	Consensus-based P2P Telemetry . . . . .	103
4.6.2	Blockchain-based Security for Smart Cities . . . . .	103
4.6.3	Secure Firmware Update . . . . .	103
4.6.4	Blockchain-based Smart Home Architecture . . . . .	104
4.6.5	Blockchain-based Self-Managed VANETS . . . . .	105
4.6.6	IoT eBusiness Model . . . . .	105
4.6.7	Transparency of Supply Chain Management (SCM) . . . . .	106

4.6.8	Blockchain-driven IoT for Food Traceability with an Integrated Consensus Mechanism . . . . .	108
4.6.9	Managing Things' Services through Smart Contracts . . . . .	108
4.6.10	Security and Privacy of Data . . . . .	109
4.7	Gap Analysis . . . . .	110
4.8	A Way Forward . . . . .	113
4.8.1	IoT-Centric Consensus Protocol and TX Validation Rules . . . . .	113
4.8.2	Managing Blockchain Size . . . . .	114
4.8.3	Improving Upon TX Confirmation Time . . . . .	115
4.8.4	Secure IoT Device Integration with the Blockchain . . . . .	117
4.8.5	Integration of IoT Communication Protocols with the Blockchain . . . . .	118
4.8.6	Resolution of Bitcoin Blockchain's Limitations . . . . .	118
4.9	Summary and Future Work . . . . .	119
<b>5</b>	<b>PrivySharing: A Framework for Privacy-Preserving and Secure Data Sharing</b>	<b>121</b>
5.1	Background . . . . .	121
5.1.1	Related Work . . . . .	123
5.1.2	Basic Terminologies . . . . .	127
5.1.3	Organization of the Chapter . . . . .	128
5.2	PrivySharing: Blockchain-based Secure Data Sharing . . . . .	128
5.2.1	Smart City Scenario . . . . .	128
5.2.2	Selection of a Suitable Blockchain Platform . . . . .	131
5.2.3	Network Architecture . . . . .	132
5.2.4	Smart City Blockchain - Plain TX Flow . . . . .	135
5.2.5	Smart City Blockchain - Private Data TX Flow . . . . .	137
5.2.6	Reward Mechanism . . . . .	138
5.3	Security Analysis . . . . .	139
5.3.1	ACL Rules . . . . .	142
5.3.2	Security of REST API and DApp . . . . .	144
5.3.3	Restricted Access to User Data Assets via Multiple Chs . . . . .	146
5.4	Experimental Results . . . . .	148
5.4.1	Validation of ACL Rules . . . . .	149



5.4.2	Performance Efficiency . . . . .	151
5.4.3	Limitation and A Way Forward . . . . .	155
5.5	Summary . . . . .	157
<b>6</b>	<b>Pledge: A PoH-based Consensus Protocol</b>	<b>159</b>
6.1	Introduction . . . . .	159
6.1.1	The Motivation . . . . .	160
6.1.2	Related Work . . . . .	161
6.1.3	Organization . . . . .	163
6.2	The Pledge Protocol . . . . .	163
6.2.1	Properties of an Ideal IoT-Centric Consensus Protocol . . . . .	163
6.2.2	Pledge Methodology . . . . .	164
6.2.3	Computing $H_{MATCumScore}$ . . . . .	167
6.2.4	IoT-Oriented TX Validation . . . . .	168
6.3	Security Guarantees and Performance Analysis . . . . .	169
6.3.1	Limitations and A Way Forward . . . . .	178
6.4	Summary . . . . .	179
<b>7</b>	<b>Conclusions and Future work</b>	<b>181</b>
7.1	Summary of the Thesis . . . . .	182
7.1.1	Chapter 2 . . . . .	182
7.1.2	Chapter 3 . . . . .	182
7.1.3	Chapter 4 . . . . .	183
7.1.4	Chapter 5 . . . . .	183
7.1.5	Chapter 6 . . . . .	184
7.2	Future Research . . . . .	184
	<b>Bibliography</b>	<b>185</b>



# LIST OF FIGURES

1.1	Objectives, research questions, and deliverables . . . . .	4
1.2	Research methodology . . . . .	6
2.1	Generalized IoT architecture . . . . .	12
2.2	IoT protocol stack . . . . .	13
2.3	Classification of IoT attacks based on their impact on deployment . . . . .	19
2.4	Home automation device setup . . . . .	23
2.5	Attack sequence of compromising a smart home controller through an open interface	24
2.6	Attacking a Belkin WeMo Switch by exploiting an SQL injection vulnerability . . . . .	26
2.7	Threats to the Philips Hue connected bulb . . . . .	27
2.8	Malware attack . . . . .	33
2.9	Methodology of a malware attack targeting IoT/ICS . . . . .	36
2.10	IoT botnet . . . . .	38
2.11	DDoS attack on the IoT . . . . .	39
2.12	IoT security against DDoS attacks . . . . .	40
3.1	Guidelines for the IoT security framework . . . . .	44
3.2	Guidelines for the IoT security framework - Preventive measures . . . . .	45
3.3	NB-IoT security in the IoT threat environment . . . . .	60
3.4	Blockchain for the IoT . . . . .	66
3.5	Blockchain-based ID authentication in fog computing . . . . .	67
4.1	Security requirements for the IoT systems . . . . .	73
4.2	Performance requirements for the IoT systems . . . . .	74
4.3	Benefits of the blockchain . . . . .	86

4.4	Impediments of permissioned blockchains . . . . .	91
4.5	Benefits of permissioned blockchains . . . . .	94
4.6	Challenges for a blockchain-based IoT system . . . . .	95
4.7	Comparison of consensus protocols . . . . .	96
4.8	Bitcoin TX validation rules . . . . .	97
4.9	Ethereum TX validation rules . . . . .	98
4.10	Disadvantages of bigger blocks . . . . .	99
4.11	Managing the IoT device services using smart contracts . . . . .	109
4.12	Considerations for the IoT-centric consensus protocol . . . . .	113
4.13	Sharding . . . . .	116
4.14	IOTA vs. Blockchain . . . . .	117
4.15	Blockchain and the IoT integration using fog nodes . . . . .	118
5.1	Issues in the smart city environment . . . . .	122
5.2	Network participants . . . . .	131
5.3	Smart city blockchain-network architecture . . . . .	132
5.4	Smart Contract TXs . . . . .	134
5.5	a) Plain TX flow, and b) Private data TX flow . . . . .	136
5.6	Reward mechanism based on PrivyCoins . . . . .	138
5.7	Error for not having enough coins . . . . .	139
5.8	Elements of PrivySharing network security . . . . .	141
5.9	ACL rules . . . . .	143
5.10	PrivySharing REST server OAuth protocol . . . . .	144
5.11	PrivySharing REST server OAuth flowchart . . . . .	145
5.12	Access denied for out-of-Ch data query . . . . .	146
5.13	Experimental settings phase-1 . . . . .	149
5.14	Validation of assets access control . . . . .	149
5.15	Validation of TX initiation rights . . . . .	150
5.16	Historical record of purged data asset and visibility of TX history . . . . .	150
5.17	Avg TX commit time . . . . .	151
5.18	Comparison of state validation, block commit, and state commit avg time . . . . .	152
5.19	Comparison of avg latency and avg throughput in one-Ch and three-Ch scenario . . . . .	153

5.20	a) Correlation between TX send rate and latency. b) Relation between TX send rate and network throughput . . . . .	155
5.21	Correlation between the number of peers and network throughput at the send rate of (a) 5 TPS, (b) 10 TPS, and (c) 20 TPS . . . . .	155
5.22	Integration of blockchain with MEC . . . . .	156
6.1	Pledge methodology . . . . .	165
6.2	Probability of being malicious . . . . .	167
6.3	IoT TX validation rules . . . . .	169
6.4	Transaction cost vs. Number of nodes . . . . .	171
6.5	Probability of a node being malicious . . . . .	171
6.6	Consensus termination and block agreement, a) Normal scenario. b) Split network	173
6.7	Avg CPU time to execute Pledge protocol vs Number of nodes . . . . .	175
6.8	Ten iterations of CPU usage measurement vs Number of nodes . . . . .	176



# LIST OF TABLES

2.1	Comparison of existing surveys . . . . .	11
2.2	Threats to the IoT . . . . .	20
2.3	Trending in cyber/malware attacks . . . . .	32
2.4	Security provided by the IoT communication protocols . . . . .	40
3.1	Security measures and their impact . . . . .	54
3.2	Comparison of LPWA technologies . . . . .	61
4.1	Benefits of Bitcoin Blockchain . . . . .	75
4.2	Public vs. Private blockchains . . . . .	78
4.3	Cloud vs. Blockchain . . . . .	87
4.4	Comparison of blockchain platforms . . . . .	89
4.5	IoT requirements vs. Progression in blockchain technologies . . . . .	92
4.6	Blockchain applications . . . . .	102
4.7	Main characteristics of blockchain-based IoT applications . . . . .	107
4.8	Gap analysis . . . . .	111
4.9	Resolution of Bitcoin Blockchain limitations . . . . .	119
5.1	List of assets . . . . .	128
5.2	Assets, stakeholders, and access rights . . . . .	129
5.3	Methodology to achieve PrivySharing objectives . . . . .	146
5.4	Experimental settings phase-2 . . . . .	152
5.5	Experimental settings phase-3 . . . . .	154
6.1	Attributes' scoring criteria . . . . .	166

6.2	Storage requirements for the attributes . . . . .	170
6.3	Avg difference in avg CPU usage . . . . .	175
6.4	Security and performance comparison of consensus protocols . . . . .	177



# LIST OF ACRONYMS

<b>ADEPT</b>	Autonomous Decentralized Peer-to-Peer Telemetry
<b>ADS</b>	Alternate Data Streams
<b>AI</b>	Artificial Intelligence
<b>AP</b>	Attribute Provider
<b>API</b>	Application Program Interface
<b>App</b>	Application
<b>Approx</b>	Approximately
<b>ARP</b>	Address Resolution Protocol
<b>ASIC</b>	Application Specific Integrated Circuit
<b>AT&amp;T</b>	American Telephone & Telegraph
<b>Avg</b>	Average
<b>BFT</b>	Byzantine Fault Tolerance
<b>BLE</b>	Bluetooth Low Energy
<b>BNC</b>	Business Network Card
<b>BPDIMS</b>	Blockchain-based Personal Data and Identity Management System
<b>BSN</b>	Biomedical Sensor Network
<b>BSoD</b>	Blue Screen of Death
<b>CA</b>	Certificate Authority
<b>CAPTCHA</b>	Completely Automated Public Turing test to tell Computers and Humans Apart
<b>CASB</b>	Cloud Access Security Broker
<b>CC</b>	Channel Configuration
<b>CCS</b>	Command and Control Server
<b>CERT</b>	Computer Emergency Response Team
<b>CH</b>	Cluster Head
<b>Ch</b>	Channel
<b>CIoT</b>	Cognitive IoT
<b>CMSP</b>	Channel Membership Service Provider
<b>CN</b>	Core Network
<b>CoAP</b>	Constrained Application Protocol
<b>CPS</b>	Cyber Physical System

<b>CSMA</b>	Carrier Sense Multiple Access
<b>CTO</b>	Chief Technology Officer
<b>DApps</b>	Decentralized Applications
<b>DAC</b>	Decentralized Autonomous Corporation
<b>DAG</b>	Directed Acyclic Graph
<b>DAO</b>	Decentralized Autonomous Organization
<b>DARPA</b>	Defense Advanced Research Projects Agency
<b>DBFT</b>	Delegated Byzantine Fault Tolerance
<b>DDoS</b>	Distributed Denial of Service
<b>DKOM</b>	Direct Kernel Object Manipulation
<b>DH</b>	Diffie Hellman
<b>DHT</b>	Distributed Hash Table
<b>DLT</b>	Distributed Ledger Technology
<b>DNS</b>	Domain Name System
<b>DoS</b>	Denial of Service
<b>DPoS</b>	Delegated Proof of Stake
<b>DSS</b>	Digital Signature Standard
<b>DTLS</b>	Datagram Transport Layer Security
<b>DVR</b>	Digital Video Recorder
<b>ECDSA</b>	Elliptic Curve Digital Signature Algorithm
<b>EEPROM</b>	Electrically Erasable Programmable Read-only Memory
<b>eNB</b>	evolve NodeB
<b>EU</b>	European Union
<b>EU GDPR</b>	European Union General Data Protection Regulation
<b>EVM</b>	Extended Verification Module
<b>FCM</b>	Fuzzy Cognitive Maps
<b>Fintech</b>	Financial Technology
<b>FMC</b>	Follow Me Cloud
<b>FTP</b>	File Transfer Protocol
<b>FTTH</b>	Fiber-To-The-Home
<b>GDPR</b>	General Data Protection Regulation
<b>GSM</b>	Global System for Mobile Communications
<b>HDFS</b>	Hadoop Distributed File System
<b>HIPPA</b>	Health Insurance Portability Accountability Act
<b>IAT</b>	Import Address Table
<b>ICS</b>	Industrial Control System
<b>ID</b>	Identity
<b>IDM</b>	Identity Management
<b>IDP</b>	Identity Provider
<b>IDS</b>	Intrusion Detection System
<b>IMA</b>	Integrity Measurement Architecture

<b>IoT</b>	Internet of Things
<b>IoV</b>	Internet of Vehicles
<b>IPFS</b>	Interplanetary File System
<b>IPS</b>	Intrusion Protection System
<b>ISMS</b>	Information Security Management System
<b>ITS</b>	Intelligent Transportation System
<b>JTAG</b>	Joint Test Action Group
<b>KSI</b>	Keyless Signature Infrastructure
<b>LDAP</b>	Lightweight Directory Access Protocol
<b>LMSP</b>	Local Membership Service Provider
<b>LTE</b>	Long Term Evolution
<b>MAC</b>	Medium Access Control
<b>MB</b>	Megabytes
<b>MBR</b>	Master Boot Record
<b>MCMC</b>	Markov Chain Monte Carlo
<b>MEC</b>	Mobile Edge Computing
<b>MITM</b>	Man-In-The-Middle Attack
<b>MMC</b>	Mobile Micro Cloud
<b>ML</b>	Machine Learning
<b>MSISDN</b>	Mobile Station International Subscriber Directory Number
<b>MSP</b>	Membership Service Provider
<b>M2M</b>	Machine-to-Machine
<b>ms</b>	Milliseconds
<b>NC</b>	Network Configuration
<b>NMS</b>	Network Management System
<b>NMSP</b>	Network Membership Service Provider
<b>NIST</b>	National Institute of Standards and Technology
<b>O</b>	Organization
<b>OAuth</b>	Open Authorization
<b>ODS</b>	Ordering Service
<b>OFC</b>	Optical Fiber Cable
<b>OOK</b>	On-Off-Keying
<b>OPC</b>	Open Platform Communications
<b>OS</b>	Operating System
<b>OSI</b>	Open Systems Interconnection
<b>OSN</b>	Online Social Networks
<b>OTA</b>	Over-The-Air
<b>OTAA</b>	Over-The-Air Activation
<b>OWAC</b>	One Way Accountable Channel
<b>OWASP</b>	Open Web Application Security Project
<b>P2P</b>	Peer-to-Peer

<b>P2PKH</b>	Pay to Public Key Hash
<b>PBFT</b>	Practical Byzantine Fault Tolerance
<b>PII</b>	Personally Identifiable Information
<b>PIPEDA</b>	Personal Information Protection and Electronic Documents Act
<b>PKG</b>	Public Key Generator
<b>PKI</b>	Public Key Infrastructure
<b>PLC</b>	Programmable Logic Controller
<b>PoA</b>	Proof-of-Activity
<b>PoC</b>	Proof-of-Concept
<b>PoET</b>	Proof-of-Elapsed-Time
<b>PoS</b>	Proof-of-Stake
<b>PoT</b>	Proof-of-Trust
<b>PoW</b>	Proof-of-Work
<b>PoH</b>	Proof-of-Honesty
<b>PubKeyHash</b>	Public Key Hash
<b>PubKeyScript</b>	Public Key Script
<b>QoS</b>	Quality of Service
<b>RAT</b>	Remote Access Trojan
<b>RCA</b>	Root Certificate Authority
<b>RFID</b>	Radio Frequency Identification
<b>RPL</b>	Routing Protocol for Lossy Networks
<b>RT-IoT</b>	Real-Time Internet of Things
<b>SCADA</b>	Supervisory Control and Data Acquisition
<b>SCC</b>	Small Cell Cloud
<b>SCeNB</b>	Small Cell evolve NodeB
<b>SCM</b>	Supply Chain Management
<b>SDN</b>	Software Defined Network
<b>SED</b>	Self Encrypting Drives
<b>SFTP</b>	Secure File Transfer Protocol
<b>SIEM</b>	Security Information and Event Management
<b>SigScript</b>	Signature Script
<b>SMB</b>	Server Message Block
<b>SMP</b>	Security Management Provider
<b>SoC</b>	System on Chip
<b>SSH</b>	Secure Shell
<b>TCG</b>	Trusted Computing Group
<b>TCS</b>	Trusted Candidate Set
<b>TEE</b>	Trusted Execution Environment
<b>TLS</b>	Transport Layer Security
<b>TOR</b>	The Onion Router
<b>TPM</b>	Trusted Platform Module

<b>TPS</b>	Transactions Per Second
<b>TX</b>	Transaction
<b>UART</b>	Universal Asynchronous Receiver Transmitter
<b>UDP</b>	User Datagram Protocol
<b>UE</b>	User Equipment
<b>UI</b>	User Interface
<b>UMTS</b>	Universal Mobile Telecommunications Service
<b>USD</b>	United States Dollar
<b>VANET</b>	Vehicular Ad-Hoc Networks
<b>Ver</b>	Version
<b>VPN</b>	Virtual Private Network
<b>V2V</b>	Vehicle-to-Vehicle
<b>VRF</b>	Verifiable Random Function
<b>WAP</b>	Wireless Application Protocol
<b>WebRTC</b>	Web Real-Time Communications
<b>WSN</b>	Wireless Sensor Network
<b>WWW</b>	World Wide Web
<b>XPolM</b>	Cross-Polarization Modulation
<b>XSS</b>	Cross-Site Scripting
<b>6LoWPAN</b>	IPv6 over Low-Power Wireless Personal Area Networks

