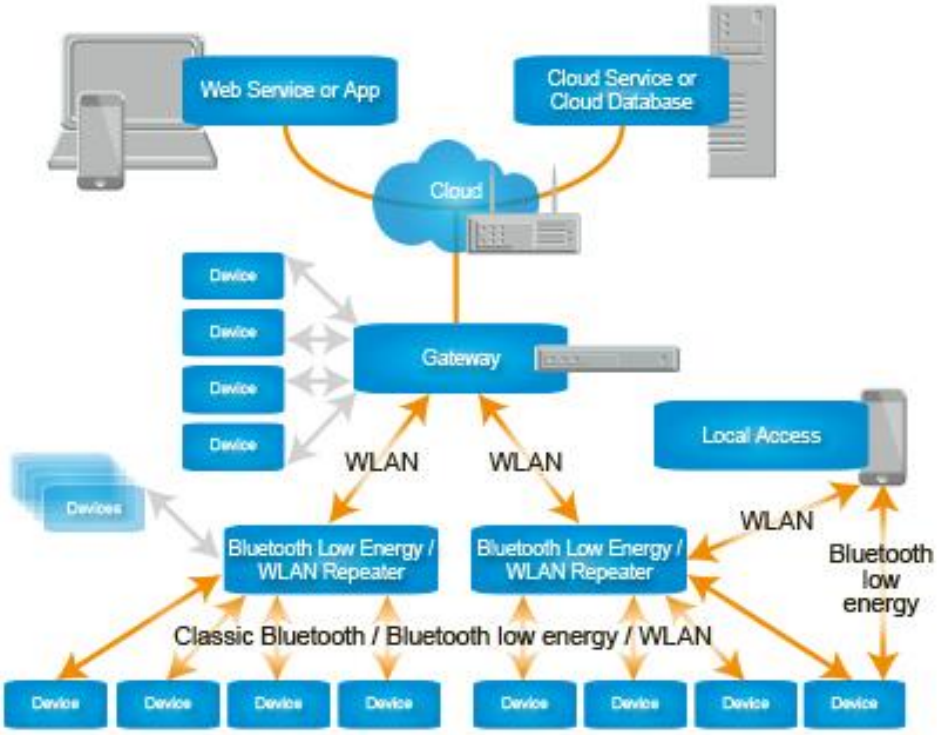
SECURITY, PRIVACY AND TRUST IN INTERNET OF THINGS: THE ROAD AHEAD

S. Sicari, A. Rizzardi, L.A. Grieco, A. Coen-Porisini

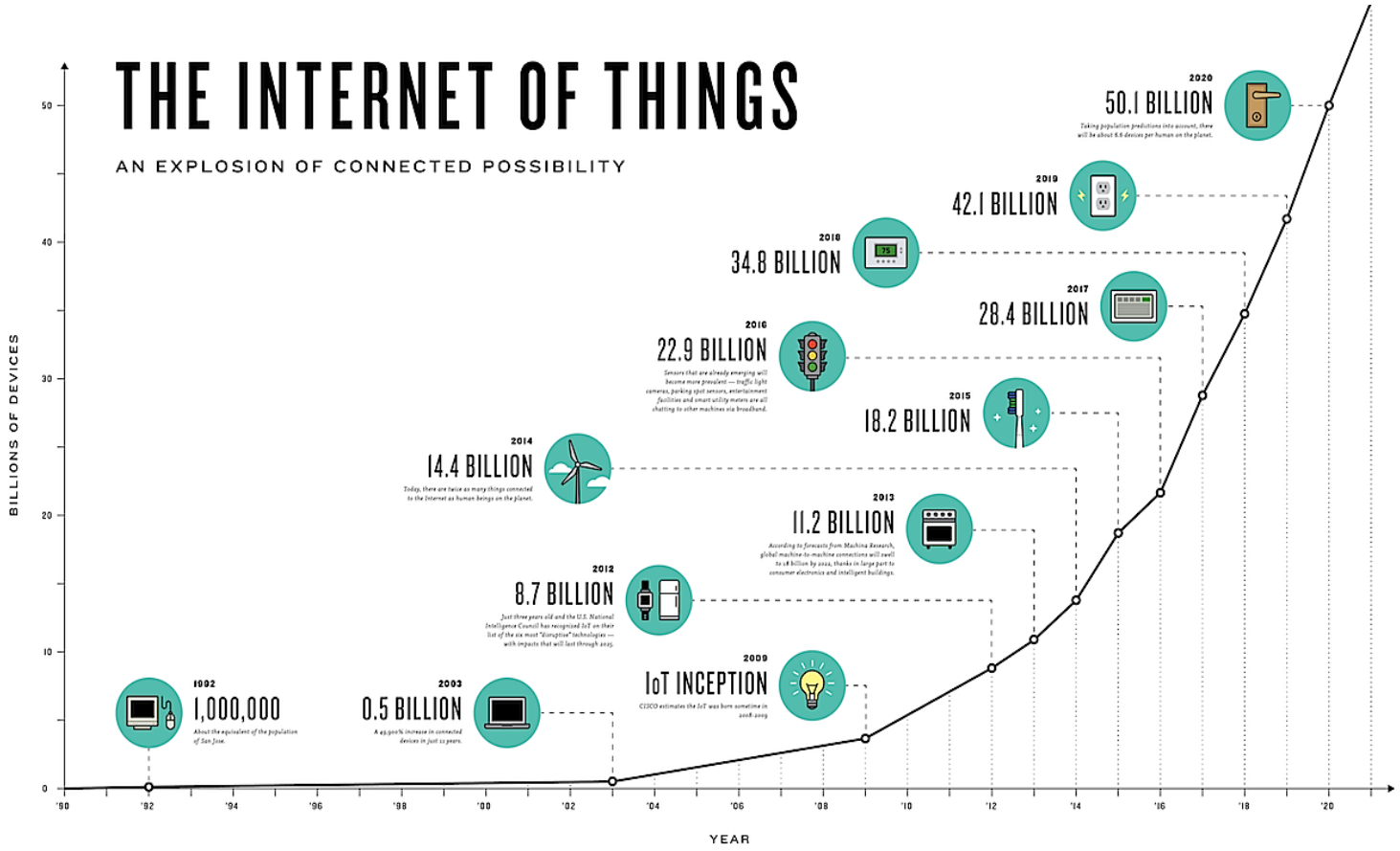
Tran Song Dat Phuc
SeoulTech 2015

Table of Contents

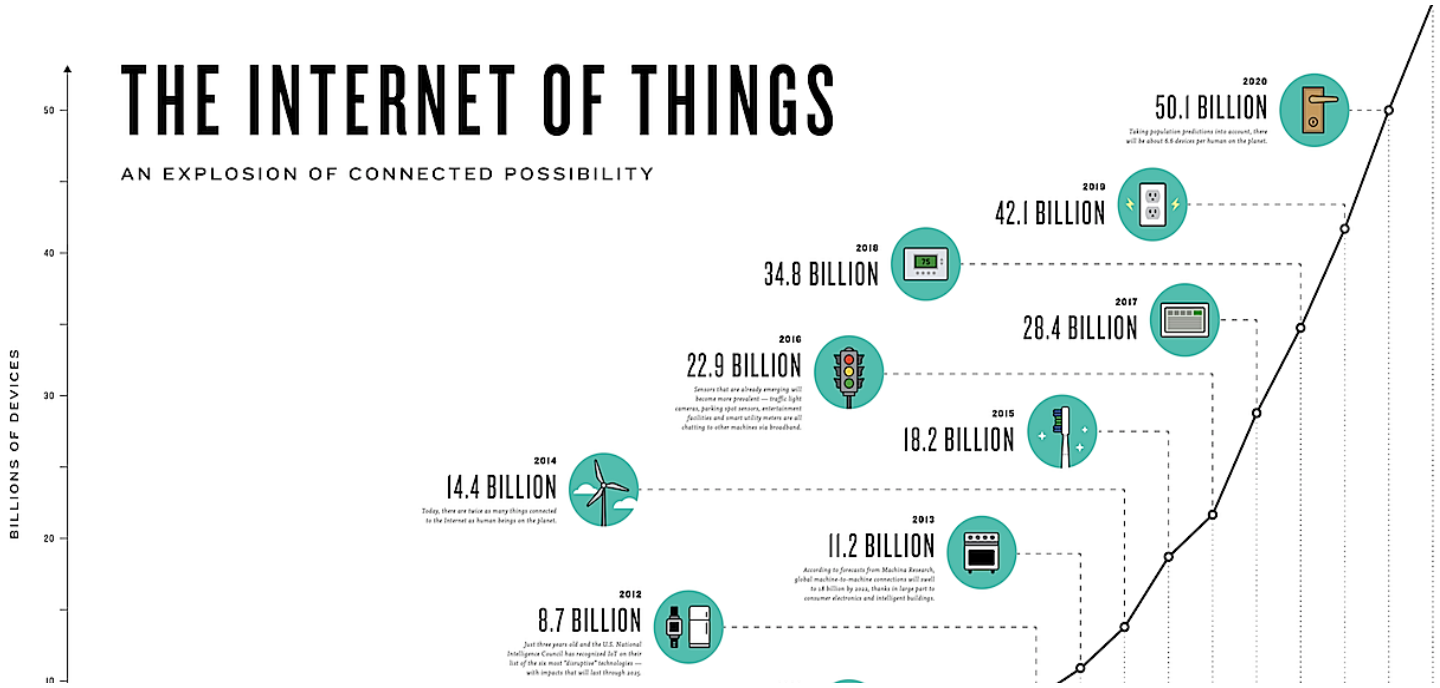
Introduction



Introduction



Introduction

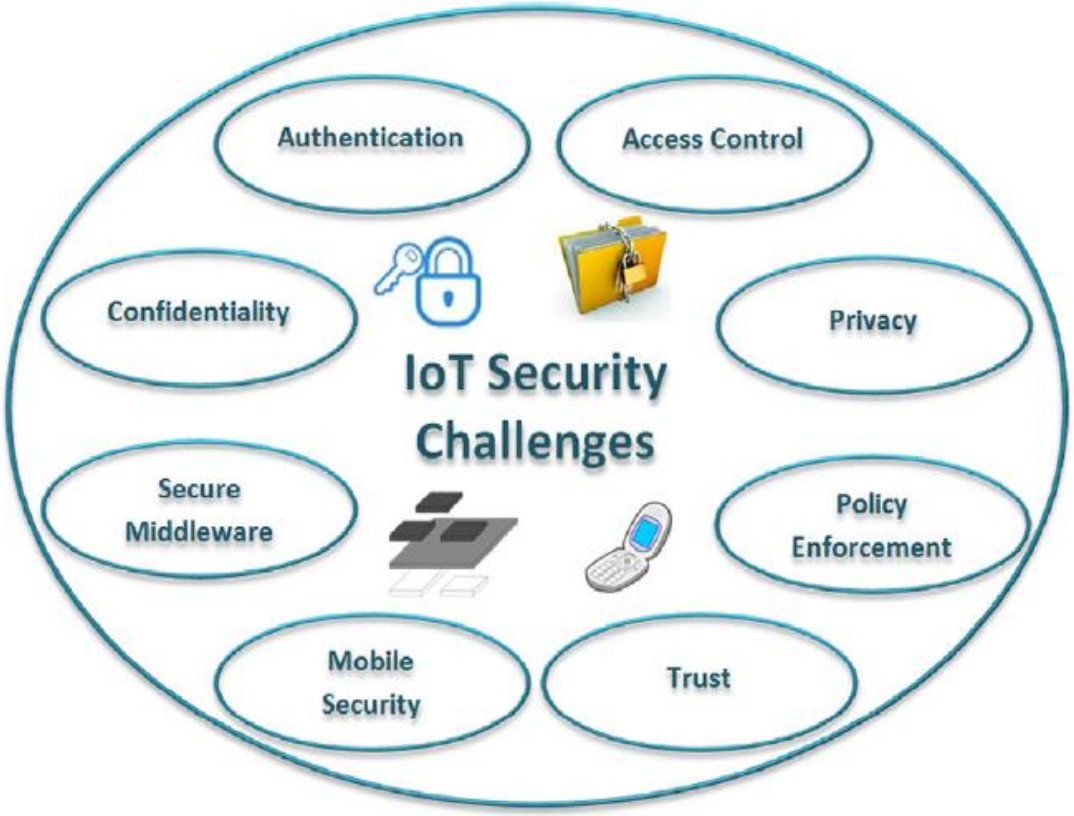


"The **Internet of Things** (**IoT**) is the network of physical objects or "things" embedded with electronics, software, sensors and connectivity to enable it to achieve greater value and service by exchanging data with the manufacturer, operator and/or other connected devices." – wikipedia.

Introduction

The high level of heterogeneity, coupled to the wide scale of IoT systems, is expected to magnify security threats of the current Internet.

The high number of inter-connected devices arises scalability issues.



Main Security Issues in IoT

Objectives

- Analyzes available solutions related to security (CIA), privacy, and trust in IoT field.

Contribution of available surveys on IoT security.

	[1]	[8]	[2]	[15]	[10]	[16]	[17]	Our work
Security	Yes	No	Yes	Yes	Yes	Yes	No	Yes
Privacy	Yes	Yes	Yes	No	Yes	Yes	No	Yes
Trust	No	Yes	Yes	No	Yes	No	Yes	Yes
Middleware	Yes	No	No	No	No	No	No	Yes
Mobile	No	No	No	No	No	No	No	Yes
Projects	No	No	Yes	No	No	No	No	Yes

IoT Security Requirements: Authentication, Confidentiality and Access Control

- IoT enables a constant transfer and sharing of data among things and users.
- In such a sharing environment, authentication, authorization, access control and non-repudiation are important to ensure secure communication.

Authentication and Confidentiality

- In [18], presented intelligent Service Security Application Protocol. It combines cross-platform communications with encryption, signature, and authentication, to improve IoT apps development capabilities.
- In [19], the authors introduced the first fully implemented two-way authentication security scheme for IoT, the Datagram Transport Layer Security (DTLS) protocol, based on RSA and designed for IPv6 over Low power Wireless Personal Area Networks (6LoWPANs), placed between transport and app player. It provides message integrity, confidentiality, and authenticity.
- In [20], classified the Key Management System (KMS) protocols in weaknesses of four major categories: key pool framework, mathematical framework, negotiation framework, and public key framework. The combinatorics-based KMS protocols suffer both connectivity and scalability, authentication.

Authentication and Confidentiality

- Another suitable KMS protocols for IoT scenarios are Blom [21] and the polynomial schema [22]. In such those schemes, several counter-measures are required to manage authentication and MitM attacks. And also in [23, 24], presented a framework for IoT based on Public Key Infrastructure (PKI).
- In [25], proposed a transmission model with signature-encryption schemes, which addresses the IoT security requirements (anonymity, trustworthy and attack resistance) by Object Naming Service (ONS) queries. It provides identities authentication, platform creditability, data integrity.
- In [26], defined that a unique and well solution able to guarantee the confidentiality in a IoT context is still missing, and some efforts have been conducted in the WNS field [27-32].

Authentication and Confidentiality

- In [33], presented an authentication protocol using lightweight encryption based on XOR manipulation for anti-counterfeiting and privacy protection, coped with constrain IoT devices.
- In [34], proposed an user authentication and key agreement scheme for WSN, by using hash and XOR computations. It ensures mutual authentication among users, sensor nodes and gateway nodes (GWN).
- In [35], presented the authentication and access control method, establishes session key on a lightweight encryption mechanism, Elliptic Curve Cryptography (ECC). This scheme defines attribute-based access control policies, managed by an attribute authority, to enhance authentication.

Access Control

- Access control refers to the permissions in the usage of resources, assigned to different actors of a wide IoT network.
- In [36], identified two subjects: data holders - feed data collectors with a specific target, and data collectors - identify and authenticate users and things from which info. are collected.
- In [37], focused on the layer responsible for data acquisition, presented a hierarchical access control scheme for this layer. It provides a single key and necessary keys by using a deterministic key derivation algorithm, for increasing the security and reducing nodes storage costs.
- In [38], presented an identity based system for personal location in emergency situations. It consists of: registration, users authentication, policy, and client subsystems.

Access Control

- In [39], developed a security architecture, aims at ensuring data integrity and confidentiality.
- In [40], a prototype query processing engine for data streams, call Nile. This mechanism is based on FT-RC4, an extension of the RC4 algorithm, represents a stream cipher encryption scheme.
- In [41, 42], addressed the authentication problem of outsourced data streams with CADS (Continuous Authentication on Data Streams). It includes the authentication info, verification info, authenticity, and completeness.
- In [43], represented streams as linear algebraic queries, provides the product authentication, by using the hash operations, modular additions/ multiplications and cryptographic security functions.

Access Control

- In [44], proposed a semi-distributed approach, a security framework and access control model called DSMSs (Data Stream Management Systems).
- In [45], proposed the Borealis data stream engine with security requirements.
- In [46], presented the OxRBAC framework, an extension of RBAC (Role-Based Access Control).
- In [47, 48], exploited metadata to guarantee the security of the tuples in the stream. Proposed a stream-centric approach, which security constraints are directly embedded into data stream, reduces overhead, and enriches data streams with metadata called streaming tags.

Access Control

- In [49], implemented and tested a framework based on CAPE engine, still exists overhead and memory issues.
- In [50], presented an enforcement to the solution provided in [51], which based on the Aurora data model [52]. This framework supports two types of privileges, named read and aggregate, and two temporal constraints, named general and window.
- In [53], defined a common query model, focuses on access control requirements for data streams. This framework is able to work among wide range of different DSMSs.
- In [54], the authors affirmed that authorization frameworks (RBAC, ABAB-Attribute Based Access Control) do not provide sufficient scalable, manageable, and effective mechanisms to support distributed systems.

Access Control

- In [55], the EU FP7 IoT Work project, developed the Capability Based Access Control (Cap-BAC), which can be used to manage the access control processes to services and info with least-privilege operations.
- In [56], addressed identity issues of specific identity management framework for IoT.
- In [57], addressed authentication and access control in the IoT framework, proposed an authorization scheme for constrained devices combines Physical Unclonable Functions (PUFs) with Embedded Subscriber Identity Module (eSIM). It provides cheap, secure, tamper-proof secret keys, authentication, scalability, interoperability, compliance with security protocols.

Access Control

- In [58], multicast communication are secured by using a common secret key, denoted as group key, reduces overhead, network traffic. Protocol can be applied in 1/ secure data aggregation in IoT and 2/ Vehicle-to-Vehicle (V2V) communications in Vehicular Ad hoc Networks (VANETs).
- In [59], defined a general UML conceptual model suitable for all IoT apps and architectures.

Privacy in IoT

Ref No.	Approach	Definition
[60]	Data tagging, techniques from the Info Flow Control	Managed privacy, allow system to reason about flows of data and preserve privacy of individuals.
[61]	User-controlled privacy-preserved access control protocol	Based on context-aware k-anonymity privacy policies, privacy protection mechanisms.
[62]	Continuously Anonymizing STreaming, data via adaptive cLustEring (CASTLE)	Cluster-based scheme, ensures anonymity, freshness, delay constraints of data streams, enhance privacy preserve techniques.
[63]	Privacy mechanism: Discretionary Access and Limited Access	Addressed the minimum privacy risks, prevents disclosure or cloning of data, avoid attacks.
[64]	Privacy protection enhanced DNS (Domain Name System)	Analyzed privacy risks. This scheme provides identity authentication, rejects illegal access.
[65]	Attribute-Based Encryption (ABE): Key Policy ABE and Cipher-text Policy ABE	Provided a public key encryption scheme, enables a fine-gained access control, scalable key management, flexible data distribution.
[66]	Attribute-based Signature (ABS) scheme, ePASS	Aims to guarantee privacy in IoT, provides attribute privacy for the signer.

Privacy in IoT

Ref No.	Approach	Definition
[67]	Key-changed mutual authentication protocol for WSN and RFID systems	Integrated a random number generator and a one-way hash function, reduces risks of replay, replication, DOS, spoofing, and tag tracking.
[68]	Privacy preserving data mining (PPDM) techniques	Addressed user privacy awareness issue, proposed a privacy management scheme, aims to develop a robust sensitive detection system.
[69]	Assessment of privacy requirements of data architecture	Defined a layered architecture for IoT, estimates both data quality and security, privacy level.

Trust in IoT

- Trust concept is used in various contexts. Trust is a complex notation about which no definitive consensus exists in scientific literature.
- The trust requirements in IoT are related to identify management and access control issues..

Summary of related works on trust assessment.

Exploited technique	Works
Social networking	[70–72,78]
Fuzzy technique	[79–82,89]
Cooperative approach	[83–85,90]
Identity-based method	[86,87]

Enforcement in IoT

Ref No.	Approach	Definition
[91]	Network security, security policies, policy enforcement, firewall policy management system	Proposed to use security services: authentication, encryption, antivirus software, firewalls, protects data confidentiality, integrity, and availability.
[92]	Policy enforcement languages	Aimed at combining policy enforcement and analysis languages, ensures correct policies.
[93]	Web Service Policy (WSP), eXtensible Access Control Markup Language (XACML)	Implemented a simulation environment: Web Ontology Language (OWL), used both policy languages and enforcement mechanisms.
[94]	Hierarchical Policy Language for Distributed System (HiPoLDS)	Presented policy enforcement in distributed reference monitors, controls the flow of info.
[95]	Enforcement of privacy issues in Ecommerce Applications	Proposed paradigms protects customer privacy: user trustworthiness and user anonymity.
[96]	Formal and modular framework	Allowed to enforce security policy on concurrent system, generates fault negative and positive.
[97]	Algebra for Communication Process (ACP), Basic Process Algebra (BPA) language	Enhanced with an enforcement operator, to monitor the requests and satisfaction of related policies.

Enforcement in IoT

Ref No.	Approach	Definition
[98]	Access control framework, Policy Machine (PM)	Integrated with secure framework, expresses and enforces policy objectives, faces Trojan attacks.
[99, 100]	Chinese Wall, MAC and DAC Models	Demonstrated PM abilities of enforcing policy objectives.
[101]	Sematic web framework, meta-control model	Orchestrated policy reasoning with identification and access of sources of information.
[102]	Application logic, embodied in system components, middleware	Supported a secure, dynamic reconfiguration, provides policy enforcement mechanism.
[103]	Enforcement solution: SecKit	Based on Model-based Security Toolkit, integrated with MQ Telemetry Transport (MQTT) protocol layer, guarantees enforcement of security and privacy policies.

Secure Middlewares in IoT

Ref No.	Approach	Definition
[104]	Smart devices support IPv6 communication	Considered different communication mediums for wide scale IoT deployments.
[105]	VIRTUS Middleware	Replied on eXtensible Messaging and Presence Protocol (XMPP), provides reliable and secure communication channel for distributed apps.
[106]	Aml Framework, Otsopack	Designed to be simple, modular and extensible, runs in different platforms (Java SE, Android).
[107]	Trivial File Transfer Protocol (TFTP)	Enhanced security, privacy, and trust in embedded system infrastructures.
[108]	Naming, Addressing and Profile Server (NAPS)	Served as a key module at the back-end data center to aid the upstream, content-based data filtering, matching and downstream from apps.
[109]	Global service layer platform for M2M communications	Supported secure and end-to-end data transmission among M2M devices and user apps.
[110]	Resource allocation middleware	Distributed the burden of app execution, distributes mechanisms and demonstrates better performance.

Secure Middlewares in IoT

Ref No.	Approach	Definition
[111]	General-purpose middleware	Generated from high level algebraic structures, adaptable to heterogeneous systems.
[112]	Security architecture for IoT transparent middleware	Based on existing security (AES, TLS and oAuth), includes privacy, authenticity, integrity and confidentiality.

Mobile Security in IoT

Ref No.	Approach	Definition
[113]	Ad hoc protocol	Provided identification, authentication and privacy protection.
[114]	Heterogeneity Inclusion and Mobility Adaptation through Locator ID Separation (HIMALIS)	Analyzed security challenges, supports scalable inter-domain authentication, solves security and privacy vulnerabilities.
[115]	Mobile RFID (Radio Frequency Identification) network	Based on EPC (Electronic Product Code), guarantees security and efficiency.
[116]	Security and privacy of mobile RFID systems	Supported tags corruption, reader corruption, multiple readers and mutual authenticated key exchange protocol.
[117]	Existing location privacy issues in mobile devices	Paid attention on Android, iPhone, and Windows Mobile platforms.
[118]	Secure handshake scheme	Established a mobile hierarchy to query a secure deployed WSN.
[119]	Secure healthcare service	Proposed a security and privacy mechanism, includes trustworthiness, authentication, cryptography credentials.

Mobile Security in IoT

Ref No.	Approach	Definition
[120]	Mobile e-health apps	Combined RFID tag identification and secure IoT solution, to enable ubiquitous and easy access, provides control and security to interactions.
[121]	Ultra-lightweight and privacy preserving authentication protocol	Provided privacy properties, and avoided numerous attacks.
[122]	Mobile Intrusion Prevention System (m-IPS)	Provided precise access control.
[123]	Mobile info collection system	Provided authentication, reduces problems of device connection, improves efficiency of info transmission.
[124]	Quantum Lifecycle Management (QLM) messaging standard	Provided generic and standardized app-level interfaces, guarantees two-way communications through any type of firewall.
[125]	Mobile Sensor Data Processing Engine (MOSDEN)	Allowed to collect and process sensor data, supports push and pull data streaming mechanisms.

Mobile Security in IoT

Ref No.	Approach	Definition
[126, 127, 128, 129, 130]	Mobility management protocol, video dissemination, mobile Bluetooth platform, Web of Things (WoT)	Proposed lightweight architecture, provides integration with other IoT technologies.

Ongoing Projects

	Butler	EBBITS	Hydra	uTRUSTit	iCore	HACMS	NSF	FIRE	EUJapan
Authentication	x			x	x	x	x	x	
Confidentiality	x	x	x		x	x	x	x	x
Access Control	x	x		x	x	x	x	x	
Privacy	x				x		x	x	x
Trust				x	x		x		
Enforcement									
Middleware		x	x		x				
Mobile	x						x		

Ongoing Projects

- Butler [131] – European Union FP7 project: enables the development of secure and smart life assistant applications (smart-cities, smart-health, smart-home/ smart office, smart-shopping, smart-mobility/ smart transport) on the security and privacy requirements; and implement a mobile framework.
- EBBITS [132] – EU FP7 project: presents Intrusion Detection System (IDS) by IPv6 over 6LoWPAN devices. Since 6LoWPAN protocol is vulnerable to wireless and Internet protocol attacks, the proposed IDS framework includes a monitoring system and a detection engine.
- Hydra [133] project: develops a middleware for Network Embedded Systems, based on a Service-Oriented Architecture (SOA). Hydra contemplates distributed security issues and social trust among the middleware component. Hydra means for Device and Service Discovery, Semantic Model Driven Architecture, P2P communication and Diagnostics.

Ongoing Projects

- uTRUSTit, Usable Trust in the IoT [134] - EU FP7 project: creates a trust feedback toolkit to enhance the user trust; enables system manufacturers and system integrators to express security concepts, allow to make valid judgments on the trustworthiness.
- iCore [135] - EU project: provides a management framework with three levels of functionality: virtual objects (VOs), composite virtual objects (CVOs), and functional blocks. The iCore solution is equipped with essential security protocols/ functionalities, related to the ownership and privacy of data and the access to objects. Includes of ambient-assisted living, smart-office, smart-transportation, and supply chain management.
- HACMS, High Assurance Cyber Military Systems [136] - U.S DARPA project: try to patch the security vulnerabilities of IoT. Includes of military vehicles, medical equipment, and drones. HACMS provides the seeds for future security protocols, achieves sufficient standardization and security.

Ongoing Projects

- NSF, National Science Foundation [137, 138, 139, 140, 141, 142] – multi-institutional project: focus on security in the cyber-physical systems. Aims at finding the efficient solutions, exploring novel network architectures and networking concepts, new communication protocols, considering the integrity and authentication, trust data, trust models, technical challenges, and the tradeoffs of between mobility and scalability, use of network resources on mobile environments.
- FIRE, Future Internet Research and Experimentation [144, 145] – EU, China, Korea project: aims at finding solutions for the deployment of IoT technologies in several application areas (public safety, social security, medical and health service, urban management, people livelihood). Attention to information security, privacy and intellectual property right.
- EUJapan ICT Cooperation [146] project: establishes the common global standards to ensure seamless communications and common ways to store and access information, the guarantee of highest security, and energy efficiency standards.

References

- [1] L. Atzori, A. Iera, G. Morabito, The internet of things: a survey, Comput. Netw. 54 (15) (2010) 2787–2805.
- [2] D. Miorandi, S. Sicari, F. De Pellegrini, I. Chlamtac, Survey internet of things: vision, applications and research challenges, Ad Hoc Netw. 10 (7) (2012) 1497–1516.
- [3] M. Palattella, N. Accettura, X. Vilajosana, T. Watteyne, L. Grieco, G. Boggia, M. Dohler, Standardized protocol stack for the internet of (important) things, IEEE Commun. Surv. Tutorials 15 (3) (2013) 1389–1406.
- [4] B. Emmerson, M2M: the internet of 50 billion devices, Huawei Win–Win Mag. J. (4) (2010) 19–22.
- [5] D. Boswarthick, O. Elloumi, O. Hersent, M2M Communications: A Systems Approach, first ed., Wiley Publishing, 2012.
- [6] O. Hersent, D. Boswarthick, O. Elloumi, The Internet of Things: Key Applications and Protocols, second ed., Wiley Publishing, 2012.
- [7] L.A. Grieco, M.B. Alaya, T. Monteil, K.K. Drira, Architecting information centric ETSI-M2M systems, in: IEEE PerCom, 2014.
- [8] R.H. Weber, Internet of things - new security and privacy challenges, Comput. Law Secur. Rev. 26 (1) (2010) 23–30.
- [9] H. Feng, W. Fu, Study of recent development about privacy and security of the internet of things, in: 2010 International Conference on Web Information Systems and Mining (WISM), Sanya, 2010, pp. 91–95.
- [10] R. Roman, J. Zhou, J. Lopez, On the features and challenges of security and privacy in distributed internet of things, Comput. Networks 57 (10) (2013) 2266–2279.
- [11] J. Anderson, L. Rainie, The Internet of Things will Thrive by 2025, PewResearch Internet Project, May 2014. <http://www.pewinternet.org/2014/05/14/internet-of-things/>.
- [12] S. Bandyopadhyay, M. Sengupta, S. Maiti, S. Dutta, A survey of middleware for internet of things, in: Third International Conferences, WiMo 2011 and CoNeCo 2011, Ankara, Turkey, 2011, pp. 288–296.

- [13] M.A. Chaqfeh, N. Mohamed, Challenges in middleware solutions for the internet of things, in: 2012 International Conference on Collaboration Technologies and Systems (CTS), Denver, CO, 2012, pp. 21–26.
- [14] S. Babar, A. Stango, N. Prasad, J. Sen, R. Prasad, Proposed embedded security framework for internet of things (iot), in: 2011 2nd International Conference on Wireless Communication, Vehicular Technology, Information Theory and Aerospace and Electronic Systems Technology, Wireless VITAE 2011, Chennai, India, 2011, pp. 1 – 5.
- [15] M.C. Domingo, An overview of the internet of underwater things, J. Network Comput. Appl. 35 (6) (2012) 1879–1890.
- [16] J. Gubbi, R. Buyya, S. Marusic, M. Palaniswami, Internet of Things (IoT): a vision, architectural elements, and future directions, Future Gener. Comput. Syst. 29 (7) (2013) 1645–1660.
- [17] Z. Yan, P. Zhang, A.V. Vasilakos, A survey on trust management for internet of things, J. Network Comput. Appl. 42 (0) (2014) 120–134.
- [18] Y. Zhao, Research on data security technology in internet of things, in: 2013 2nd International Conference on Mechatronics and Control Engineering, ICMCE 2013, Dalian, China, 2013, pp. 1752–1755.
- [19] T. Kothmayr, C. Schmitt, W. Hu, M. Brunig, G. Carle, Dtls based security and two-way authentication for the internet of things, Ad Hoc Netw. 11 (8) (2013) 2710–2723.
- [20] R. Roman, C. Alcaraz, J. Lopez, N. Sklavos, Key management systems for sensor networks in the context of the internet of things, Comput. Electrical Eng. 37 (2) (2011) 147–159.
- [21] W. Du, J. Deng, Y. Han, P. Varshney, J. Katz, A. Khalili, A pairwise key predistribution scheme for wireless sensor networks, ACM Trans. Inf. Syst. Secur. (TISSEC) 8 (2) (2005) 228–258.
- [22] D. Liu, P. Ning, Establishing pairwise keys in distributed sensor networks, in: CCS ’03 Proceedings of the 10th ACM Conference on Computer and Communications Security, Washington, DC, USA, 2003, pp. 52–61.
- [23] H. Pranata, R. Athauda, G. Skinner, Securing and governing access in ad-hoc networks of internet of things, in: Proceedings of the IASTED International Conference on Engineering and Applied Science, EAS 2012, Colombo, Sri Lanka, 2012, pp. 84–90.

- [24] H. Ning, A security framework for the internet of things based on public key infrastructure, Adv. Mater. Res. 671–674 (2013) 3223–3226.
- [25] Z.-Q. Wu, Y.-W. Zhou, J.-F. Ma, A security transmission model for internet of things, Jisuanji Xuebao/Chin. J. Comput. 34 (8) (2011) 1351–1364.
- [26] G. Piro, G. Boggia, L.A. Grieco, A standard compliant security framework for ieee 802.15.4 networks, in: Proc. of IEEE World Forum on Internet of Things (WF-IoT), Seoul, South Korea, 2014, pp. 27–30.
- [27] I. Akyildiz, W. Su, Y. Sankarasubramaniam, E. Cayirci, A survey on sensor networks, IEEE Commun. Mag. 40 (8) (2002) 102–114.
- [28] H. Chan, A. Perrig, Security and privacy in sensor networks, IEEE Commun. Mag. 36 (10) (2003) 103–105.
- [29] J. Yick, B. Mukherjee, D. Ghosal, Wireless sensor network survey, Comput. Netw. 52 (12) (2008) 2292–2330.
- [30] N. Li, N. Zhang, S.K. Das, B. Thuraisingham, Privacy preservation in wireless sensor networks: a state-of-the-art survey, Ad Hoc Netw. 7 (8) (2009) 1501–1514.
- [31] J. Zhang, V. Varadharajan, Security and privacy in sensor networks, J. Network Comput. Appl. 33 (2) (2010) 63–75.
- [32] G.Sharmam, S. Bala, A.K. Verma, Security frameworks for wireless sensor networks-review, in: 2nd International Conference on Communication, Computing & Security, ICCCS-2012, 2012, pp. 978–987.
- [33] J.-Y. Lee, W.-C. Lin, Y.-H.Huang, A lightweight authentication protocol for internet of things, in: 2014 International Symposium on Next- Generation Electronics, ISNE 2014, Kwei-Shan, 2014, pp. 1–2.
- [34] M. Turkanovi, B. Brumen, M. Hlbl, A novel user authentication and key agreement scheme for heterogeneous ad hoc wireless sensor networks, based on the internet of things notion, Ad Hoc Netw. 20 (2014) 96–112.
- [35] N. Ye, Y. Zhu, R.-C. b. Wang, R. Malekian, Q.-M. Lin, An efficient authentication and access control scheme for perception layer of internet of things, Appl. Math. Inf. Sci. 8 (4) (2014) 1617–1624.
- [36] A. Alcaide, E. Palomar, J. Montero-Castillo, A. Ribagorda, Anonymous authentication for privacy-preserving iot targetdriven applications, Comput. Secur. 37 (2013) 111–123.

- [37] J. Ma, Y. Guo, J. Ma, J. Xiong, T. Zhang, A hierarchical access control scheme for perceptual layer of iot, Jisuanji Yanjiu yu Fazhan/ Comput. Res. Dev. 50 (6) (2013) 1267–1275.
- [38] C. Hu, J. Zhang, Q. Wen, An identity-based personal location system with protected privacy in IoT, in: Proceedings - 2011 4th IEEE International Conference on Broadband Network and Multimedia Technology, IC-BNMT 2011, Shenzhen, China, 2011, pp. 192–195.
- [39] M. Ali, M. ElTabakh, C. Nita-Rotaru, FT-RC4: A Robust Security Mechanism for Data Stream Systems, Tech. Rep. TR-05-024, Purdue
- University (November 2005).
- [40] M.A. Hammad, M.J. Franklin, W. Aref, A.K. Elmagarmid, Scheduling for shared window joins over data streams, in: Proceedings of the 29th International Conference on Very Large Data Bases, VLDB ’03, Berlin, Germany, 2003, pp. 297–308.
- [41] S. Papadopoulos, Y. Yang, D. Papadias, Cads: continuous authentication on data streams, in: Proceedings of the 33rd International Conference on Very Large Data Bases, VLDB ’07, Vienna, Austria, 2007, pp. 135–146.
- [42] S. Papadopoulos, Y. Yang, D. Papadias, Continuous authentication on relational data streams, VLDB J. 19 (1) (2010) 161–180.
- [43] S. Papadopoulos, G. Cormode, A. Deligiannakis, M. Garofalakis, Lightweight authentication of linear algebraic queries on data streams, in: Proceedings of the 2013 ACM SIGMOD International Conference on Management of Data, SIGMOD’13, New York, USA, 2013, pp. 881–892.
- [44] W. Lindner, J. Meier, User interactive internet of things privacy preserved access control, in: 10th International Database Engineering and Applications Symposium, 2006, IDEAS’06, Delhi, 2006, pp. 137–147.
- [45] D.J. Abadi, Y. Ahmad, M. Balazinska, M. Cherniack, J. Hwang, W. Lindner, A.S. Maskey, E. Rasin, E. Ryvkina, N. Tatbul, Y. Xing, S. Zdonik, The design of the borealis stream processing engine, in: CIDR, 2005, pp. 277–289.
- [46] R.S. Sandhu, E.J. Coyne, H.L. Feinstein, C.E. Youman, Role-based access control models, Computer 29 (2) (1996) 38–47.

- [47] R. Nehme, E. Rundesteiner, E. Bertino, A security punctuation framework for enforcing access control on streaming data, in: Proceedings of the 24th International Conference on Data Engineering, ICDE ’08, Cancun, Mexico, 2008, pp. 406–415.
- [48] R. Nehme, E. Rundesteiner, E. Bertino, Tagging stream data for rich real-time services, Proc. VLDB Endowment 2 (1) (2009) 73–84.
- [49] Y. Zhu, E.A. Rundensteiner, G.T. Heineman, Dynamic plan migration for continuous queries over data streams, in: Proceedings of the ACM SIGMOD International Conference on Management of Data,
- SIGMOD ’04, Paris, France, 2004, pp. 431–442.
- [50] B. Carminati, E. Ferrari, K.L. Tan, Enforcing access control over data streams, in: Proceedings of the 12th ACM symposium on Access control models and technologies, SACMAT ’07, Sophia Antipolis, France, 2007, pp. 21–30.
- [51] B. Carminati, E. Ferrari, K.L. Tan, Specifying access control policies on data streams, in: Proceedings of the Database System for Advanced Applications Conference, DASFAA 2007, Bangkok, Thailand, 2007, pp. 410–421.
- [52] D.J. Abadi, D. Carney, U. Cetintemel, M. Cherniack, C. Convey, S. Lee, M. Stonebraker, N. Tatbul, S. Zdonik, Aurora: a new model and architecture for data stream management, VLDB J. 12 (2) (2003) 120–139.
- [53] B. Carminati, E. Ferrari, K.L. Tan, A framework to enforce access control over data streams, ACM Trans. Inform. Syst. Sec. TISSEC 13 (3) (2010) 1–31.
- [54] S. Gusmeroli, S. Piccionea, D. Rotondi, A capability-based security approach to manage access control in the internet of things, Math. Comput. Model. 58 (5-6) (2013) 1189–1205.
- [55] European FP7 IoT@Work project. <http://iot-at-work.eu>.
- [56] P. Mahalle, S. Babar, N. Prasad, R. Prasad, Identity management framework towards internet of things (IoT): Roadmap and key challenges, Commun. Comput. Inf. Sci. 89 (2010) 430–439.
- [57] A. Cherkaoui, L. Bossuet, L. Seitz, G. Selander, R. Borgaonkar, New paradigms for access control in constrained environments, in: 2014 9th International Symposium on Reconfigurable and Communication-Centric Systems-on-Chip (ReCoSoC), Montpellier, 2014, pp. 1–4.
- [58] L. Veltri, S. Cirani, S. Busanelli, G. Ferrari, A novel batch-based group key management protocol applied to the internet of things, Ad Hoc Netw. 11 (8) (2013) 2724–2737.
- [59] S. Sicari, A. Rizzardi, C. Cappiello, A. Coen-Porisini, A NFP model for internet of things applications, in: Proc. of IEEE WiMob, Larnaca, Cyprus, 2014, pp. 164–171.

- [60] D. Evans, D. Eyers, Efficient data tagging for managing privacy in the internet of things, in: Proceedings – 2012 IEEE Int. Conf. on Green Computing and Communications, GreenCom 2012, Conf. on Internet of Things, iThings 2012 and Conf. on Cyber, Physical and Social Computing, CPSCom 2012, Besancon, France, 2012, pp. 244–248.
- [61] X. Huang, R. Fu, B. Chen, T. Zhang, A. Roscoe, User interactive internet of things privacy preserved access control, in: 7th International Conference for Internet Technology and Secured Transactions, ICITST 2012, London, United Kingdom, 2012, pp. 597–602.
- [62] J. Cao, B. Carminati, E. Ferrari, K.L. Tan, CASTLE: continuously anonymizing data streams, IEEE Trans. Dependable Secure Comput. 8 (3) (2011) 337–352.
- [63] J. Yang, B. Fang, Security model and key technologies for the internet of things, J. China Universities Posts Telecommun. 8 (2) (2011) 109–112.
- [64] Y. Wang, Q. Wen, A privacy enhanced dns scheme for the internet of things, in: IET International Conference on Communication Technology and Application, ICCTA 2011, Beijing, China, 2011, pp. 699–702.
- [65] X. Wang, J. Zhang, E. Schooler, M. Ion, Performance evaluation of attribute-based encryption: Toward data privacy in the IoT, in: 2014 IEEE International Conference on Communications, ICC 2014, Sydney, NSW, 2014, pp. 725–730.
- [66] J. Su, D. Cao, B. Zhao, X. Wang, I. You, ePASS: An expressive attribute-based signature scheme with privacy and an unforgeability guarantee for the internet of things, Future Gener. Comput. Syst. 33 (0) (2014) 11–18.
- [67] L.b. Peng, W.b. Ru-chuan, S. Xiao-yu, C. Long, Privacy protection based on key-changed mutual authentication protocol in internet of things, Commun. Comput. Inf. Sci. 418 CCIS (2014) 345–355.
- [68] A. Ukil, S. Bandyopadhyay, A. Pal, Iot-privacy: To be private or not to be private, in: Proceedings – IEEE INFOCOM, Toronto, ON, 2014, pp. 123–124.
- [69] S. Sicari, C. Cappiello, F.D. Pellegrini, D. Miorandi, A. Coen-Porisini, A security-and quality-aware system architecture for internet of things, Inf. Syst. Frontiers (2014) 1–13.
- [70] F. Bao, I. Chen, Dynamic trust management for internet of things applications, in: Proceedings of the 2012 International Workshop on Self-Aware Internet of Things, Self-IoT ’12, USA, San Jose, 2012, pp. 1–6.
- [71] F. Bao, I. Chen, Trust management for the internet of things and its application to service composition, in: 13th IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks, WoWMoM 2012, San Francisco, CA, United States, 2012, pp. 1–6.

- [72] M. Nitti, R. Girau, L. Atzori, A. Iera, G.Morabito, A subjectivemodel for trustworthiness evaluation in the social internet of things, in: 2012 IEEE 23rd International Symposium on Personal Indoor and Mobile Radio Communications, PIMRC, Australia, Sydney, 2012, pp. 18–23.
- [73] S.D. Kamvar, M.T. Schlosser, H. Garcia-Molina, The eigen-trust algorithm for reputation management in p2p networks, in: Proc. WWW'03, New York, USA, 2003, pp. 640–651.
- [74] L. Xiong, L. Liu, Peertrust: supporting reputation-based trust for peer-to-peer electronic communities, IEEE Trans. Knowl. Data Eng. 16 (2004) 843–857.
- [75] A.A. Selcuk, E. Uzun, M.R. Pariente, A reputation-based trust management system for p2p networks, in: Proc. of CCGRID 2004, Washington, DC, USA, 2004, pp. 251–258.
- [76] B. Yu, M.P. Singh, K. Sycara, Developing trust in large-scale peer-topeer systems, in: Proc. of First IEEE Symposium on Multi-Agent Security and Survivability, 2004, pp. 1–10.
- [77] Z. Liang, W. Shi, Enforcing cooperative resource sharing in untrusted p2p computing environments, Mob. Netw. Appl. 10 (2005) 251–258.
- [78] R. Lacuesta, G. Palacios-Navarro, C. Cetina, L. Penalver, J. Lloret, Internet of things: where to be is to trust, EURASIP J. Wireless Commun. Networking 2012 (1) (2012) 1–16.
- [79] P.N. Mahalle, P.A. Thakre, N.R. Prasad, R. Prasad, A fuzzy approach to trust based access control in internet of things, in: 2013 3rd International Conference on Wireless Communications, Vehicular Technology, Information Theory and Aerospace & Electronic Systems, VITAE, NJ, Atlantic City, 2013, pp. 1–5.
- [80] J. Wang, S. Bin, Y. Yu, X. Niu, Distributed trust management mechanism for the internet of things, Appl. Mech. Mater. 347-350 (4) (2013) 2463–2467.
- [81] Y. Liu, Z. Chen, F. Xia, X. Lv, F. Bu, An integrated scheme based on service classification in pervasive mobile services, Int. J. Commun. Syst. 25 (9) (2012) 1178–1188.
- [82] Y. Liu, Z. Chen, F. Xia, X. Lv, F. Bu, A trust model based on service classification in mobile services, in: Proceedings – 2010 IEEE/ACM International Conference on Green Computing and Communications, GreenCom 2010, 2010 IEEE/ACM International Conference on Cyber, Physical and Social Computing, CPSCom 2010, Hangzhou, China, 2010, pp. 572–576.

- [83] L. Wen-Mao, Y. Li-Hua, F. Bin-Xing, Z. Hong-Li, A hierarchical trust model for the internet of things, Chin. J. Comput. 5 (2012) 846–855.
- [84] Y. Saied, A. Olivereau, D. Zeghlache, M. Laurent, Trust management system design for the internet of things: a context-aware and multi-service approach, Comput. Secur. 39 (2013) 351–365.
- [85] P. Dong, J. Guan, X. Xue, H. Wang, Attack-resistant trust management model based on beta function for distributed
- routing in internet of things, China Commun. 9 (4) (2012) 89–98.
- [86] T. Liu, Y. Guan, Y. Yan, L. Liu, Q. Deng, A wsn-oriented key agreement protocol in internet of things, in: 3rd International Conference on Frontiers of Manufacturing Science and Measuring Technology, ICFMM 2013, LiJiang, China, 2012, pp. 1792–1795.
- [87] P. Martinez-Julia, A.F. Skarmeta, Beyond the separation of identifier and locator: building an identity-based overlay network architecture for the future internet, Comput. Netw. 57 (10) (2013) 2280–2300.
- [88] G.D. Tormo, F.G. Marmol, G.M. Perez, Dynamic and flexible selection of a reputation mechanism for heterogeneous environments, Future Gener. Comput. Syst. (2014).
- [89] L. Gu, J. Wang, B.b. Sun, Trust management mechanism for internet of things, China Commun. 11 (2) (2014) 148–156.
- [90] Y.-B. Liu, X.-H. Gong, Y.-F. Feng, Trust system based on node behavior detection in internet of things, Tongxin Xuebao/J. Commun. 35 (5) (2014) 8–15.
- [91] R. Macfarlane, W. Buchanan, E. Ekonomou, O. Uthmani, L. Fan, O. Lo, Formal security policy implementations in network firewalls, Comput. Secur. 31 (2) (2012) 253–270.
- [92] Y. Elrakaiby, F. Cuppens, N. Cuppens-Boulahia, Formal enforcement and management of obligation policies, Data Knowl. Eng. 71 (1) (2012) 127–147.
- [93] Z. Wu, L. Wang, An innovative simulation environment for crossdomain policy enforcement, Simul. Model. Pract. Theory 19 (7) (2011) 1558–1583.
- [94] M. Dell'Amico, M.S.I.G. Serme, A.S. de Oliveira, Y. Roudier, Hipolds: a hierarchical security policy language for distributed systems, Inf. Secur. Technical Rep. 17 (3) (2013) 81–92.

- [95] G. Bella, R. Giustolisi, S. Riccobene, Enforcing privacy in ecommerce by balancing anonymity and trust, Comput. Secur. 30
- (8) (2011) 705–718.
- [96] M. Langar, M. Mejri, K. Adi, Formal enforcement of security policies on concurrent systems, J. Symbol. Comput. 46 (9) (2011) 997–1016.
- [97] J. Baeten, A brief history of process algebra, Theoret. Comput. Sci. 335 (2-3) (2005) 131–146.
- [98] D. Ferraiolo, V. Atluri, S. Gavrila, The policy machine: a novel architecture and framework for access control policy specification and enforcement, J. Syst. Architec. 57 (4) (2011) 412–424.
- [99] D. Brewer, M. Nash, The chinese wall security policy, in: Proceedings. 1989 IEEE Symposium on Security and Privacy, Oakland, CA, 1989, pp. 206–214.
- [100] M. Bishop, Computer Security: Artand Science,AddisonWesley,2003.
- [101] J. Rao, A. Sardinha, N. Sadeh, A meta-control architecture for orchestrating policy enforcement across heterogeneous
- information sources, Web Semantics: Sci. Serv. Agents World Wide Web 7 (1) (2009) 40–56.
- [102] J. Singh, J. Bacon, D. Eyers, Policy enforcement within emerging distributed, event-based systems, in: DEBS 2014 – Proceedings of the 8th ACM International Conference on Distributed Event-Based Systems, 2014, pp. 246–255.
- [103] R. Neisse, G. Steri, G. Baldini, Enforcement of security policy rules for the internet of things, in: Proc. of IEEE WiMob, Larnaca, Cyprus, 2014, pp. 120–127.
- [104] I. Bagci, S. Raza, T. Chung, U. Roedig, T. Voigt, Combined secure storage and communication for the internet of things, in: 2013 IEEE International Conference on Sensing, Communications and Networking, SECON 2013, New Orleans, LA, United States, 2013, pp. 523–631.
- [105] D. Conzon, T. Bolognesi, P. Brizzi, A. Lotito, R. Tomasi, M. Spirito, The virtus middleware: an xmpp based architecture for secure IoT communications, in: 2012 21st International Conference on Computer Communications and Networks, ICCCN 2012, Munich, Germany, 2012, pp. 1–6.
- [106] A. Gòmez-Goiri, P. Orduna, J. Diego, D.L. de Ipina, Otsopack: lightweight semantic framework for interoperable ambient intelligence applications, Comput. Hum. Behav. 30 (2014) 460–467.

- [107] M.Isa, N.Mohamed, H.H.S.Adnan, J.Manan,R.Mahmod,Alightweight and secure TFTP protocol for smart environment, in: ISCAIE 2012 – 2012 IEEE Symposium on Computer Applications and Industrial Electronics 2012, Kota Kinabalu, Malaysia, 2012, pp. 302–306.
- [108] C.H. Liu, B. Yang, T. Liu, Efficient naming, addressing and profile services in internet-of-things sensory environments, Ad Hoc Netw. 18 (0) (2013) 85–101.
- [109] oneM2M. <http://www.onem2m.org/>.
- [110] G. Colistra, V. Pilloni, L. Atzori, The problem of task allocation in the internet of things and the consensus-based approach, Comput. Netw. 73 (0) (2014) 98–111.
- [111] Y. Wang, M. Qiao, H. Tang, H. Pei, Middleware development method for internet of things, Liaoning Gongcheng Jishu Daxue Xuebao (Ziran Kexue Ban)/J. Liaoning Tech. Univ. (Nat. Sci. Ed.) 33 (5) (2014) 675–678.
- [112] H. Ferreira, R. De Sousa Jr., F. De Deus, E. Canedo, Proposal of a secure, deployable and transparent middleware for internet of things, in: Iberian Conference on Information Systems and Technologies, CISTI, Barcelona, 2014, pp. 1–4.
- [113] J. Mao, L. Wang, Rapid identification authentication protocol for mobile nodes in internet of things with privacy protection, J. Networks 7 (7) (2012) 1099–1105.
- [114] A. Jara, V. Kafle, A. Skarmeta, Secure and scalable mobility management scheme for the internet of things integration in the future internet architecture, Int. J. Ad Hoc Ubiquitous Comput. 13 (3-4) (2013) 228–242.
- [115] T. Yan, Q. Wen, A secure mobile rfid architecture for the internet of things, in: Proceedings 2010 IEEE International Conference on Information Theory and Information Security, ICITIS 2010, Beijing, China, 2010, pp. 616–619.
- [116] W. Zhu, J. Yu, T. Wang, A security and privacy model for mobile rfid systems in the internet of things, in: International Conference on Communication Technology Proceedings, ICCT, 2012, pp. 726–732.
- [117] M. Elkhodr, S. Shanhrestani, H. Cheung, A review of mobile location privacy in the internet of things, in: International Conference on ICT and Knowledge Engineering, Bangkok, Thailand, 2012, pp. 266–272.
- [118] S. Li, P. Gong, Q. Yang, M. Li, J. Kong, P. Li, A secure handshake scheme for mobile-hierarchy city intelligent transportation system, in: International Conference on Ubiquitous and Future Networks, ICUFN, Da Nang, 2013, pp. 190–191.
- [119] K.c. Kang, Z.-B. Pang, C.c. Wang, Security and privacy mechanism for health internet of things, J. China Universities Posts Telecommun. 20 (SUPPL-2) (2013) 64–68.

- [120] F. Goncalves, J. Macedo, M. Nicolau, A. Santos, Security architecture for mobile e-health applications in medication control, in: 2013 21st International Conference on Software, Telecommunications and Computer Networks, SoftCOM 2013, Primosten, 2013, pp. 1–8.
- [121] B. Niu, X. Zhu, H. Chi, H. Li, Privacy and authentication protocol for mobile rfid systems,Wireless Pers. Commun. 77 (3) (2014) 1713–1731.
- [122] Y.-S. Jeong, J. Lee, J.-B. Lee, J.-J. Jung, J. Park, An efficient and secure m-ips scheme of mobile devices for human-centric computing, J. Appl. Math. Special Issue 2014 (2014) 1–8.
- [123] J. Geng, X. Xiong, Research on mobile information access based on internet of things, Appl. Mech. Mater. 539 (2014) 460–463.
- [124] S. Kubler, K. Frmling, A. Buda, A standardized approach to deal with firewall and mobility policies in the iot, Pervasive MobileComput. (2014).
- [125] C. Perera, P. Jayaraman, A. Zaslavsky, D. Georgakopoulos, P. Christen, Mosden: An internet of things middleware for resource constrained mobile devices, in: Proceedings of the Annual Hawaii International Conference on System Sciences, Washington, DC, USA, 2014, pp. 1053–1062.
- [126] J. Montavont, D. Roth, T. Nol, Mobile {IPv6} in internet of things: analysis, experimentations and optimizations, Ad Hoc Netw. 14 (0) (2014) 15–25.
- [127] D. Rosario, Z. Zhao, A. Santos, T. Braun, E. Cerqueira, A beaconless opportunistic routing based on a cross-layer approach for efficient video dissemination in mobile multimedia IoT applications, Comput. Commun. 45 (0) (2014) 21–31.
- [128] J.P. Espada, V.G. Daz, R.G. Crespo, O.S. Martnez, B.P. G-Bustelo, J.M.C. Lovelle, Using extended web technologies to develop bluetooth multi-platform mobile applications for interact with smart things, Inf. Fusion 21 (0) (2014) 30–41.
- [129] J. An, X. Gui, W. Zhang, J. Jiang, J. Yang, Research on social relations cognitive model of mobile nodes in internet of things, J. Network Comput. Appl. 36 (2) (2013) 799–810.
- [130] T.-M. Gronli, P. Pourghomi, G. Ghinea, Towards NFC payments using a lightweight architecture for the web of things, Computing (2014).
- [131] BUTLER Project. <http://www.iot-butler.eu>.

- [132] P. Kasinathan, G. Costamagna, H. Khaleel, C. Pastrone, M. Spirito, Demo: An ids Framework for Internet of Things Empowered by 6lowpan, Berlin, Germany, 2013, pp. 1337–1339.
- [133] HYDRA Project. <http://www.hydramiddleware.eu/>.
- [134] Usable Trust in the Internet of Things. <http://www.utrustit.eu/>.
- [135] iCORE Project. <http://www.iot-icore.eu>.
- [136] HACMS Project. <http://www.defenseone.com/technology>.
- [137] National Science Foundation Project. <http://www.nsf.gov>.
- [138] Roseline Project. <https://sites.google.com/site/roselineproject/>.
- [139] XIA-NP Project. <http://www.cs.cmu.edu/xia/>.
- [140] NDN-NP Project. <http://named-data.net/>.
- [141] NEBULA Project. <http://nebula-fia.org/>.
- [142] MobilityFirst-NP Project. <http://mobilityfirst.winlab.rutgers.edu/>.
- [143] H.-D. Ma, Internet of things: objectives and scientific challenges, J. Comput. Sci. Technol. 26 (6) (2011) 919–924.
- [144] FIRE EU-China Project. <http://www.euchina-fire.eu/>.
- [145] FIRE EU-Korea Project. <http://eukorea-fire.eu/>.
- [146] EU-Japan Project. <http://www.eurojapan-ict.org/>.

Conclusions

- The real spreading of IoT services requires customized security and privacy levels to be guaranteed.
- This survey provided broad overview of many open issues, and some light on research directions in the IoT security field.
- It covers from the security and privacy requirements, different technologies and communication standards, suitable solutions, to security and privacy policies in the middleware environment, mobile devices.
- The secured IoT requirements: confidentiality, access control, privacy for users and things, trustworthiness among devices and users, compliance with defined security and privacy policies.
- This survey is helpful in suggesting the research road ahead, allow a massive deployment of IoT systems in real world.