International Journal of Engineering, Science and Mathematics
Vol. 6 Issue 8, December 2017 (Special Issue)
ISSN: 2320-0294 Impact Factor: 6.765
Journal Homepage: http://www.ijesm.co.in, Email: ijesmj@gmail.com Double-Blind
Peer Reviewed Refereed Open Access International Journal - Included in the International Serial Directories Indexed & Listed at: Ulrich's Periodicals Directory ©, U.S.A., Open J-Gage as well as in Cabell's Directories of Publishing Opportunities, U.S.A

Security for Internet of Things: A Survey

J Maruthi Nagendra Prasad*
VamshiKrishna Mangalampalli**

Abstract

The Internet of Things is a paradigm where everyday objects can be equipped with identifying, sensing, networking and processing capabilities that will allow them to communicate with one another and with other devices and services over the internet to provide innovative services in various application domains.

In this scenario, there is a need for security and privacy which include confidentiality, authentication, authorization, access control, privacy and trust management among users and things. The document discusses challenges and the solutions in the field of IoT security.

Keywords:

Internet of Things;
Security;
Survey;
Middleware;
Communication.

Author correspondence:

J MARUTHI NAGENDRA PRASAD
Research Scholar,
Dept. of CSE, Centurion University, Paralekhemundi, Odisha

1. Introduction

Internet of Things, allows over internet direct communication to happen between machines, which made the researches to use this to bring more devices online and allow them to participate in the web.In modern wireless telecommunication this paradigm is gaining ground.In an internet-like structure objects are uniquely addressed and represented virtually through Internet of things [1]. Radio-Frequency Identification Technology (RFID) [2, 3, 4, 5] can track a large number of Uniquely Identifiable Objects with this it is considered as a key enabler of the Internet of Things. Barcodes, or 2D-codes are other kinds of ubiquitous sensor devices which can be used to enable the Internet of Things.Pervasive computing, ubiquitous computing and internet of things all are related because all these concepts are enabled by embedded sensor devices used in the large scale.Objects of everyday life can be equipped with sensors which can track some useful information about these objects this becomes the vision of the internet of things.

The main objective is to give the reader the opportunity of understanding what has been done and what still remains to be addressed.

Security Properties:

In this section,with a special focus on IoT systemsthree key security properties are analyzed in depth: authentication, confidentiality, and access control. Information transfer and information sharing among things and users happens constantly in IoT. Non-repudiation, authentication,access control and authorization are to be taken care to guarantee secure communication in such situations Existing techniques are to be tailored for this new environment.

*Research Scholar,Dept. of CSE,Centurion University,Odhisa
**HOD, Dept. of CSE, Centurion University,Odhisa

Authentication:

Two types of encapsulation techniques are presented in Ref. [6]. They are smart business security IoT application protocol and intelligent service security application protocol. Signature, encryption and authentications are combined to improve IoT application development capabilities by establishing a secure communication between different things. Two-way authentication secure scheme was introduced for IoT in Ref. [7] Using the Datagram Transport Layer Security protocol.

Confidentiality and integrity:

Ref. [8] shows the applicability of key management systems in the context of IoT. Key pool framework, negotiation framework, mathematical framework and public key framework are the four classes of Management System Protocols.

Ref. [9] proposes a more practical transmission model with signature encryption schemes which addresses IoT security requirements by means of Object Naming Service Queries.

Using lightweight encryption method, an authentication protocol for IoT was proposed in [10]. And [11] proposes an user authentication and key agreement scheme for heterogeneous wireless sensor networks, which enables a remote user to securely negotiate a session key with a sensor node, using a lean key agreement protocol.

Access control:

Ref. [12] presents another encryption mechanism which generates a session key based on Elliptic Curve Cryptography. It is responsible for enhancing mutual authentication among the users and addresses the resource constrained issue and provides access control policies. Access control refers to the permission to use the resource and Resources will be assigned to different actors in the wide IoT networks Ref. [13] identifies two actors called data holders and data collectors. Authenticaters are Data collectors who authenticate data holders as legitimate.

In IoT processing of streaming data also plays a vital role as in traditional database systemsthemain focus in [14] is on the layers responsible for data acquisition information collection is done by these layers.

In emergency situations, the location of the user can be made available under normal conditions users location information is confidential. Ref. [15] proposes an identity based system for emergency situations.

In [16] a security architecture is proposed which aims at providing data integrity and confidentiality for data streams and in [17] the performance of the DBMS is improved and scalability also improved.

Data streams outsourced will be facing authentication problems which are addressed in Ref. [18, 19]. Outsourcing of data is in main focus of Ref. [20]. Streaming data companies may not have the resources for deploying large amount of streaming data in a data stream management systems.

To safeguard data stream management system an access control model was proposed in [21] and to secure the data in the stream metadata was exploited in Ref [22, 23]. In [22] it's proposed a stream-centric approach, in which the security constraints are directly embedded into data streams and not stored on the data stream management system server.in [23] an extended approach is proposed, which enriches data streams with metadata called streaming tags.

Ref. [24] supports the solutions provided in [25]. Two types of privileges are supported by this framework namely read and aggregate and also two temporal constraints named general and window.

Ref. [26] extends the two previous works in order to make their solution stream engine independent. Each data stream management system adopts its own language and to solve such an issue and to allow all the interaction among different data stream management system [26] proposes a common query model and the most frequent operations are translated by the deployment module into the specific engine query language.

Identification:

With the Rise in pervasive computing and ubiquitous computing the requirement for device identification is not met adequately in IoT.

Ref. [27] addresses the authentication and reformulation of the architecture.Authentication in IoT is addressed in [28]. It combines physical unclonable function with embedded subscriber identity module to authorize constrained devices. Ref. [29] defines a conceptual model suitable for all IoT applications.

2. Privacy

IoT application for example: patient's remote monitoring, energy consumption control, traffic control, smart parking system, inventory management. In all of the above users personal information must be secured.

Ref. [30] proposes a technique called data tagging for managing privacy in IoT. In [31] based on context aware k-anonymity privacy policies access control protocol was proposed which preserves the privacy of the user.

In [32], using adaptive clustering a technique was proposed which continuously ananymizes streaming data.

In [33], the privacy mechanisms are classified into two classes: discretionary access and limited access. When a domain name which is static if assigned to IoT node there can be privacy risk which is analyzedin [34].

Ref. [35] focus on two major types of attribute based encryption: key policy attribute based encryption and cipher text policy attribute based encryption. Using attribute based signature scheme in [36] an approach was presented which ensure privacy in IoT.Here a novel attribute-based signature scheme, name ePASS, uses an attribute tree and expresses any policy consisting of AND/OR which are unforgeable for the computational Diffie-Hellman assumption.

Ref. [37] proposes an authentication protocol based on mutual key change. Data mining techniques are used to address privacy protection by minimizing the sensitive data disclosure. The assessment of privacy requirements of data was done in [39] to estimate both the data quality and the security and privacy level, it defines a layered architecture for IoT in order.

3. Trust

In [40, 41], the main focus is on trust level assessment of IoT entities. Ref. [40] proposes a trust management protocol in distributed, encounter-based and activity-based environment. Communicating nodes can rate each other and exchange trust evaluation about one another.

In [42], a trustworthiness evaluation is carried out in social internet of things. [43-47] proposes a techniques in which, on their own experience basis, nodes compute the trustworthiness of their friends.

Ref. [48] proposes a secure distributed adhoc network which is based on direct peer-to-peer interactions and community's creation.

In [49], it's proposed that for decentralized and dynamic IoT scenarios traditional access control models are not suitable. Layered trust mechanism is proposed in [50] using fuzzy set theory and formal semantic based language.

Ref. [51, 52] combines location aware and identity aware information and authentication history to propose a trust model to protect the user security.

Ref. [53] proposes a hierarchical trust model for IoT which detect malicious organization. Ref. [54] proposes a Trust management system which is able to access the trust level of a node from its past behavior in distinct cooperative services. Ref. [55] proposes a trust management model for routing in IoT.

Ref. [56] proposes a trust management for IoT, based on identity-based key agreement. To identify network nodes which moves themselves from a host-to-host during the handover process an identity-based network protocol was presented in [57].

In [58], a mechanism for heterogeneous environments was designed with which we can select the most suitable trust and reputation model. Ref. [59] proposes a trust management mechanism for layered IoT architecture.

4. Securing MiddleWare

A few sorts of middleware layers are utilized to enforce the integration and the security of devices and data within the IoT.

Ref. [60] focuses on networking and security issues and proposed a VIRTUS middleware which relys on the open extensible messaging and presence protocol to provide secure event driven communications within an IoT scenario.

Ref. [61] proposes a framework called Otsopack, which provides two core functionalities: it's designed to be simple and it runs in different computational platform.

To enhance security, privacy and trust in embedded system, a framework is proposed in [62]. Light weight symmetric encryption is used for data and for trivial file transfer protocol symmetric encryption - protocols are used. To bridge different platforms in IoT environments a Naming, Addressing and profile server is used as a middleware in [63]

A global service layer platform for M2M communication is proposed in [64] OneM2M.it enables the interoperability of different M2M systems across multiple networks and topologies on top of IP to unify the global M2M community. Secure end-to-end data transmission among the communicating parties is supported by middleware.

Ref [65] addresses allocation of tasks in IoT. To perform a given task the nodes have to cooperate and also consider the available resources.

A method was defined to systematically construct a general purpose middleware for IoT in [66] The middleware is adaptable to heterogeneous systems which is generated starting from high level algebraic structures then they are mapped into building components depending on the underlying computing infrastructure.

Ref. [67] proposes a secure and transparent architecture for IoT middleware it uses existing technologies for security. To provide security for smart objects, services and users privacy, authenticity, integrity and confidentiality of exchanged data are integrated.

5. Secure Communication Protocols

IoT Security Solutions are classified into two main categories based on:

- Asymmetric key schemes
- Pre-distribute symmetric keys

Asymmetric Key Schemes:

Public key cryptography is based on Asymmetric key scheme which is considered as a very common approach to establish a secure communication between two or more parties.

Asymmetric algorithms are widely deployed in conventional internet. There is one major inconvenience when Asymmetric Key Schemes are used in IoT, Which is the computation cost and energy consumption. And the approaches are classified into two categories: key transport based on public key encryption and key agreement based on asymmetric techniques.

Symmetric Key Pre-distribution schemes:

To bootstrap secure communication in the IoT researcher's proposed multiple techniques using symmetric key establishment. Nodes involved in the symmetric key establishment share common credentials.

Symmetric key or some random bytes are the pre-shared credentials, flashed into the sensor before its deployment. Symmetric Key Pre-distribution schemes are classified into 2 sub categories they are probabilistic key distribution and deterministic key distribution.

Asymmetric key schemes:

<u>Key transport based on public key encryption</u>

- Raw Public Key Encryption:
  Ref. [77] or Ref. [81] have been recommended for WSNs, proposal in Ref. [77] is very similar to the RSA algorithm and is also based upon the hardness of the factorization problem. A lattice-based alternative to RSA and ECC primitives is proposed in Ref. [81](NtruEncrypt). This mechanism is best suited for the devices with constrained resources. In [81], a comparison of the three PKC mechanisms proposed for constrained devices was presented.
- Certificate-based encryption:
  TLS [74] has been recommended by many standards specified by IETF for security service. Ref. [68] Implement DTLS using hardware assistance on sensor nodes. A modification of DTLS was presented by Ref. [69] using the 6LoWPAN compression mechanism. An idea to effectively reduce the overhead of the DTLS handshake was proposed by Ref. [83]. A similar modifications to DTLS was presented by Ref. [82] but the DTLS handshake is mediated by the 6LoWPAN border router.
  Ref. [96] proposes a protocol which works jointly with IPsec to provide security between two entities.
- Identity-based schemes:
  Identity based cryptography was first implemented in Ref. [70]. IBE paradigm is implemented using the ECC primitive in a constrained environment. TinyIBE a very simple authenticated key distribution based on IBE was proposed in Ref. [89, 82, 71] for heterogeneous sensor networks. Ref. [73] proposes Diffie-Hellman protocol and its varients are classical examples for symmetric key agreement. A combination of ECDH and IBE for sensor networks was proposed in [90]. This scheme depends on the ECDH protocol and provides the privacy of message exchanges using identity based scheme [89]. Ref. [95] tailor HIP-DEX to the IoT by adapting the session resumption mechanism.

Symmetric key Pre-distribution schemes:

- Probabilistic key distribution
  Random key pre-distribution was proposed in [91]. Ref. [84,92-94] pre-distribution phase is improved to enhance the key connectivity between nodes and reduce the memory space needed for key storage. In [84] key pre-distribution scheme was proposed that depends on the deployment knowledge and avoids unnecessary key assignments. Ref. [93] develops a scheme based on Ref. [84] works, but the keys are mapped on two-dimensional positions. Ref [92] develops a mechanism to reinforce the path-key establishment phase.
- Deterministic key distribution
  Ref [72,80] focuses on the schemes based on bivariate polynomials. In these schemes there is an exchange of bivariate n-degree polynomial f(x,y) is happening between two communicating nodes. One node can obtain the pairwise key with another node by calculating the value of $f(Id_A,Id_B)$. Ref. [85] proposed a scheme where a secret symmetric matrix D is generated from the shared secret key between the two communicating nodes. Ref. [88, 86, 87] proposes key establishment schemes where the session key is generated without the need for a key server to perform key management. Ref. [79] implements the standard internet security protocol IPsec in an IP based WSN. Ref. [68] is inspired by the TLS pre-shared key cipher suite. MIKEY-Ticket [75] is an additional mode to the basic MIKEY [78] protocol, in which a KDC is involved in the process of establishing a security association between the two parties. MIKEY-Ticket originated from the ticket concept of Kerberos [76].

  Ref [112] SAKE was proposed which is a new key establishment based on the MIKEY-Ticket mode and removes the threat of DoS attacks.
  In [113] PANA protocol was proposed which is a solution for key distribution based on an external server. Ref. [114] an advancement of PANA was proposed which can adapt to the resource constraints. Considerable modifications consists of reducing the number of message exchanges and minimizing the collection of cryptographic primitives at the resource constrained device.
  In [115] a secure authentication and key establishment between sensor node and an external internet host called SAKES is proposed. Ref. [116] Distributed HIP exchange protocol was presented.

6. Mobile Security in IoT

In IoT, there is a need for privacy and authentication because mobile nodes transient from one location to another. Ref. [97] proposed a protocol which is used to authenticate and protect privacy of a mobile node when a mobile node joins a new cluster.

In [98] author proposes analysis the security challenges for the Heterogeneity Inclusion and Mobility Adaptation through Locator ID separation architecture regarding features from IoT and the ID/locator management messages vulnerable to attacks.

In IoT technologies using RF signals without direct contact we can automatically identify tagged objects using RFID systems based on Electronic Product Code Network Environment. Possible Threats in mobile RFID networks are analyzed in [99].

Ref. [100] proposes a model in which privacy of tags and readers are addressed and corruption of tags and readers are supported.

IoT framework with the advent of pervasive computing have the ability to enable mass surveillance and to violate the location privacy of the user. Existing location privacy issues are addressed in [101].

In an intelligent transportation system a secure handshake scheme among mobile nodes is proposed in [102] .Ref. [103] point's outs that new demand for mobile solutions is secure healthcare service. Which is responsible to protect the privacy and security of patients in a healthcare context using an IoT infrastructure, a security and privacy mechanism is proposed.

Ref. [104] proposes a secure architecture which can be deployed on mobile platforms for mobile e-health applications. Also in [105] addresses solvution for the security and privacy issues.

In [106] author proposes an efficient and secure intrusion prevention system for business activities using mobile devices for human centric computing. Ref. [107] designs an access gateway for smart mobile devices which is responsible for mobile information collection system based on IoT.

Security and mobility in IoT is specially treated in [108]. Firewalls are used by the people and companies to secure their data which leads to a challenging conflict between data security and usability.

Ref. [109] presents a mobile sensor data processing engine which is plug-in-based IoT middleware for mobile devices having constrained resources which enables collection and processing of sensor data without programming efforts.

Ref. [110] proposes an efficient video dissemination mechanism in mobile multimedia IoT applications, while [111] points out the interaction happening between smart things with the mobile Bluetooth platform.

7. Conclusion

The real dissemination of IoT services requires customized security and concealment levels to be guaranteed. A bound together vision with respect to the insurance of security and protection essential in such a heterogeneous circumstance, including diverse advances and correspondence measure is as yet absent.Reasonable arrangements should be designed and deployed which are independent from the exploited platform and able to ensure: confidentiality, access control and privacy for users and things, trustworthiness among devices and users, compliance with defined security and privacy policies.

8. References

[1] K. Ashton. That 'Internet of Things' Thing. In: RFID Journal,22 July, 2009.
[2] C. Bornhovd, T. Lin, S. Haller, J. Schaper. Integrating Automatic Data Acquisition with Business Processes Experiences with SAP's Auto-Id Infrastructure, VLDB Conference, 2004.
[3] A. Gupta, M. Srivasatava. Developing auto-id solutions using sun java system rfid software, October 2004. http://java.sun.com/developer/technicalArticles/ Ecommerce/rfid/sjsrfid/RFID.html
[4] S. E. Sarma, S. A. Weis, D.W. Engels. Radio-frequency identifica- tion systems. CHES, pp. 454–469, 2002.
[5] S. E. Sarma, S. A. Weis, D.W. Engels. RFID systems, security and privacy implications. Technical Report MIT–AUTOID–WH–014, AutoID Center, MIT, 2002.
[6] 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
[7] T. Kothmayr, C. Schmitt, W. Hu, M. Brunig, G. Carle, Dtls based security and two-way authentication for the internet of things, AdHoc Netw. 11 (8) (2013) 2710–2723
[8] 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.
[9] 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.
[10] 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.
[11] 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.
[12] 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.
[13] A. Alcaide, E. Palomar, J. Montero-Castillo, A. Ribagorda, Anonymous authentication for privacy-preserving iot target-driven applications, Comput. Secur. 37 (2013) 111–123.
[14]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.
[15]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.
[16]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).
[17]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
[18]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.
[19]S. Papadopoulos, Y. Yang, D. Papadias, Continuous authentication on relational data streams, VLDB J. 19 (1) (2010) 161–180.

[20]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.
[21]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.
[22] 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.
[23] R. Nehme, E. Rundesteiner, E. Bertino, Tagging stream data for rich real-time services, Proc. VLDB Endowment 2 (1) (2009) 73–84.
[24] 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.
[25] 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
[26] 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
[27] 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.
[28] 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
[29] 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.
[30] 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
[31] 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.
[32] J. Cao, B. Carminati, E. Ferrari, K.L. Tan, CASTLE: continuously anonymizing data streams, IEEE Trans. Dependable Secure Comput. 8 (3) (2011) 337–352.
[33] J. Yang, B. Fang, Security model and key technologies for the internet of things, J. China Universities Posts Telecommun. 8 (2) (2011) 109–112.
[34] Y.Wang, Q.Wen, A privacy enhanced dnsscheme for the internet of things, in: IET International Conference on Communication Technology and Application, ICCTA 2011, Beijing, China, 2011, pp. 699–702.
[35] 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.
[36] 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.
[37] 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.
[38] 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.
[39] 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.
[40] 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.
[41] 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.

[42] 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.
[43] 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.
[44] L. Xiong, L. Liu, Peertrust: supporting reputation-based trust for peer-to-peer electronic communities, IEEE Trans. Knowl. Data Eng 16 (2004) 843–857.
[45] 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.
[46] B. Yu, M.P. Singh, K. Sycara, Developing trust in large-scale peer-to-peer systems, in: Proc. of First IEEE Symposium on Multi-Agent Security and Survivability, 2004, pp. 1–10.
[47] Z. Liang,W. Shi, Enforcing cooperative resource sharing in untrusted p2p computing environments, Mob. Netw. Appl. 10 (2005) 251–258
[48] 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.
[49] 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.
[50] 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.
[51] 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.
[52] 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.
[53] 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.
[54] 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.
[55] 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.
[56] 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
[57] P. Martinez-Julia, A.F. Skarmeta, Beyond the separation of identifier and locator: building an identity-based overlaynetwork architecture for the future internet, Comput. Netw. 57 (10) (2013) 2280–2300.
[58] 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).
[59] L. Gu, J. Wang, B.b. Sun, Trust management mechanism for internet of things, China Commun. 11 (2) (2014) 148–156
[60] 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
[61] 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.
[62] M. Isa,N.Mohamed,H.H.S.Adnan, J.Manan,R.Mahmod,A lightweight 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
[63] 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.
[64] oneM2M. <http://www.onem2m.org/>.
[65] 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.
[66] Y.Wang,M. Qiao, H. Tang, H. Pei,Middlewaredevelopment 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

[67] 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
[68] T. Kothmayr, C. Schimit, et al., A DTLS based end-to-end security architecture for the Internet of thing with two-way authentication, in: 7th IEEE International Workshop on Practical Issues in Building Sensor Network Applications, 2012
[69] S. Raza, H. Shafagh, et al., Lithe: lightweight secure CoAPs for the Internet of things, IEEE Sens. J. 13 (10) (2013).
[70] A. Shamir, Identity-based cryptosystems and signature schemes, in: Proc. Crypto'84, Santa Barbara, California, USA, 1984, pp. 47–54.
[71] P. Szczechowiak, M. Collier, TinyIBE: identity-based encryption for heterogeneous sensor networks, in: 5th International Conference on Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP), 2009.
[72] A. Fanian, M. Berenjkoub, H. Saidi, A scalable and efficient key establishment protocol for wireless sensor networks, in: IEEE Globecom Workshop on Web and Pervasive Security, 2010.
[73] E. Rescorla, Diffie–Hellman Key Agreement Method, IETF, RFC 2631, 1999
[74] S. Turner, T. Polk, Transport Layer Security, IETF, RFC 6176, 2011.
[75] J. Mattsson, T. Tian, MIKEY-TICKET: Ticket-Based Modes of Key Distribution in Multimedia Internet KEYing (MIKEY), IETF, RFC 6043, March 2011
[76] J. Kohl, C. Neuman, The Kerberos Network Authentication Service (V5), IETF, RFC 4120, 6649, July 2005.
[77] M.O. Rabin, Digitalized Signature and Public Key Functions as Intractable as Factorization, MIT/LCS/TR-212, Massachusetts Institute of Technology, 1979
[78] J. Arkko, E. Carrara, F. Lindholm, et al., MIKEY: Multimedia Internet KEYing, RFC 3830, August 2004.
[79] S. Raza, S. Duquennoy, T. Chung, et al., Securing communication in 6LoWPAN with compressed IPsec, in: International Conference on Distributed Computing in Sensor Systems and Workshop, 2011
[80] D. Liu, P. Ning, R. Li, Establishing pairwise keys in distributed sensor networks, J. ACM Trans. Inform. Syst. Secur. 8 (1) (2005)41-77
[81] G. Gaubatz, J.-P. Kaps, B. Sunar, State of the art in ultra-low power public key cryptography for wireless sensor networks in: 3rd IEEE International Conference on Pervasive Computing and Communications Workshop (PERCOMW), 2005
[82] J. Granjal, E. Monteiro, J. Silva, End-to-end transport layer security for Internet-integrated sensing applications with ECC public-key authentication, in: IFIP Networking Conference, 2013.
[83] R. Hummen, Jan H. Ziegeldorf, et al., Towards viable certificate-based authentication for the Internet of things, in: Proceedings of the 2nd ACM Workshop on Hot Topics on Wireless Network Security and Privacy (HotWiSec'13), 2013.
[84] W. Du, J. Deng, et al., A key predistribution scheme for sensor networks using deployment knowledge, IEEE Trans. Dependable Secure Comput. 3 (1) (2006) 41–77.
[85] R. Blom, An optimal class of symmetric key generation systems, in: Advances in Cryptology: Proc. EUROCRYPT '84, 1985, pp. 335–338.
[86] A. Perrig, R. Szewczyk, J.D Tygar, et al., SPINS: security protocols for sensor networks, in: ACM International Conference on Mobile Computing and Networking (MobiCom), 2001.
[87] B. Lai, S. Kim and I. Verbauwhede, Scalable session key construction protocol for wireless sensor networks, in: IEEE Workshop on Large Scale RealTime and Embedded Systems (LARTES), 2002.
[88] S. Seys, Key Establishment and Authentication Suite to Counter DoS Attacks in Distributed Sensor Networks, COSIC, 2012.
[89] D. Boneh, M. Franklin, Identity-based encryption from the Weil paring, SIAM J. Comput. 32 (2003) 586–615.
[90] L. Yang, C. Ding, M. Wu, Establishing Authenticated Pairwise Key using Pairing-based Cryptography for Sensor Network, 8th Chinacom, 2013.
[91] L. Eschenauer, V.D. Gligor, A Key-Management Scheme for Distributed Sensor Networks, 2002
[92] H. Chan, A. Perrig, D. Song, Random key predistribution schemes for sensor networks, in: Proc. IEEE Symp. Security and Privacy, May 2003
[93] T. Ito, H. Ohta, et al., A key pre-distribution scheme for secure sensor networks using probability density function of node deployment, in: Proc. 3rd ACM Workshop on Security and Ad Hoc Sensor Networks, 2005, pp. 69–75.
[94] D.D. Hwang, B. Lai, I. Verbauwhede, Energy-memory-security tradeoff distributed sensor networks, in: Proc. 3rd Conference on Ad-Hoc Networks and Wireless, 2004, pp. 70–81

[95] R. Moskowitz, P. Jokela, et al., Host Identity Protocol version 2 (HIPv2), Draft-Internet, 2013
[96] S. Ray, G.P. Biswas, Establishment of ECC-based initial secrecy usable for IKE implementation, in: Proc. of World Congress on Expert Systems (WCE), 2012.
[97] 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.
[98] 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.
[99] 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
[100] 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.
[101] 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.
[102] 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 in: International Conference on Ubiquitous and Future Networks ICUFN, Da Nang, 2013, pp. 190–191.
[103] 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.
[104] 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
[105] B. Niu, X. Zhu, H. Chi, H. Li, Privacy and authentication protocol for mobile rfid systems, Wireless Pers. Commun. 77 (3) (2014) 1713–1731.
[106] 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
[107] J. Geng, X. Xiong, Research on mobile information access based on internet of things, Appl. Mech. Mater. 539 (2014) 460–463
[108] S. Kubler, K. Frmling, A. Buda, A standardized approach to deal with firewall and mobility policies in the iot, PervasiveMobileComput. (2014)
[109] 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
[110] 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
[111] 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
[112] A. Boudguiga, A. Olivereau, N. Oualha, Server assisted key establishment protocol for WSN: a MIKEY-ticket approach, in: 12th IEEE Trustcom, 2013.
[113] D. Forsberg, Y. Ohba, et al. (Eds.), Protocol for Carrying Authentication for Network Access (PANA), RFC 5191, 2008.
[114] M. Kanda, Y. Ohba, S. Das, et al., PANA Applicability in Constrained Environments, Sources. <http://www.lix.polytechnique.fr/> (accessed February 2012).
[115] H.R. Hussen, G.A. Tizazu, et al., SAKES: secure authentication and key establishment scheme for M2M communication in the IP-based wireless sensor network (6LoWPAN), in: 5th International Conference on Ubiquitous and Future Networks (ICUFN), 2013.
[116] Y.B. Saied, A. Olivereau, D-HIP: a distributed key exchange scheme for HIP-based Internet of things, in: First IEEE WoWMoM Workshop on the Internet of Things: Smart Objects and Services (IoT-SoS), 2012.