Introducing Secure Provenance in IoT: Requirements and Challenges

Sabah Suhail, Choong Seon Hong
Department of Computer Science and Engineering,
Kyung Hee University,
Yongin,Korea
Email: sabah,cshong@khu.ac.kr

Zuhaib Uddin Ahmad
Department of Computer Sciences,
Bahria University,
Islamabad, Pakistan
Email: zuhaibuddin82@yahoo.com

Faheem Zafar, Abid Khan
Department of Computer Science,
COMSATS Institute of Information Technology,
Islamabad, Pakistan
Email: faheemiiui@gmail.com, abidkhan@comsats.edu.pk

***Abstract*—In current cyber-physical systems, IoT represents interconnection of highly heterogeneous networked entities, providing goods and services to a variety of domains including environment monitoring, energy management, health-care system, and industrial automation. However, in-spite of the advantages of global connectivity, the Internet of Things (IoT) encounter various security challenges and resource constraints including identity management, traceability, storing and processing of veracious sensory data. The security research in IoT so far has not focused on provenance and its usefulness in IoT. To keep data traces of IoT devices, provenance can play a vital role as it solves many issues related to data trustworthiness, decision-making, data reconciliation and data replication. In this paper, we have discussed the challenges on the technical infrastructure of IP-based, WSN-based and RFID-based IoT. We have identified the possible ways to integrate secure provenance into IoT grounded on security issues and other resource constraints in IoT.**

***Keywords*-Internet of Things; Provenance; WSN-based IoT; RFID-based IoT; IP-based IoT**

I. Introduction

Provenance is a metadata describing the complete lineage of data and processes chain. Provenance-aware system has the ability to keep track of issues including tracking ownership of data, process time-stamps, transformation applied on input data and environment settings in which data is processed or evolved at granularity level. Provenance being beneficial in auditing, debugging, performance measurement, result reproducibility, forensics investigation and quality assessment have been extensively focused in various domains including databases, scientific work-flows, distributed systems, and networks [1].

Internet of Things-a paradigm for connecting heterogeneous networked things to facilitate goods and services in various domains including global supply chain, industrial automation, building automation (heating, ventilation, air conditioning, lighting, access control, fire), smart things (connected home, grid, cars, cities), health care system, environmental monitoring, urban sensor networks, energy management, assets tracking, and refrigeration [2].

Despite the comforts provided by IoT there is a high risk of security and privacy breach of the involved stakeholders. Furthermore, the trustworthiness of data being generated is highly questionable. Therefore, provenance can be integrated with IoT to track inconsistencies in data and to guarantee the integrity and authenticity of data. In healthcare IoT, for instance, telemedicine where doctors can remotely treat their patients and may inquire about their health condition by observing their life-log provenance data. Such tracking may facilitate medical experts to devise which drug should be substituted to achieve optimum sudden recovery and thus can monitor the causes of the severity of any particular chronic disease. Currently, many fitness devices (for example, Fitbit) are being used to bring patient provided data into the cycle of care delivery also need a track of events due to security threats. Similarly in smart agriculture, to analyze the crop yielding keeping in view the fertilizer application, nutrients, soil mapping, weather data, machinery, livestock etc. The farming association can track yearly crop production and can be able to identify the factors which may enhance the quality of agriculture products based on the information obtained from data provenance. Such metadata may help in making agronomic decision.

Although, provenance has been studied in various domains such as scientific work-flows [3], [4], [5], [6], [7], [8], databases [9], [10], [11], cloud computing [12], [13], [14], [15], [16], [17], wireless sensor networks [23], [24], [34], [35], [36], [37] and other domains. However, the fusion of provenance with IoT has not been explored so far. A conceptual architectural model to identify the connecting points between IoT and provenance has been proposed in [40]. However, the underlying challenges resulting from implementation of secure data provenance in the IoT are not

978-1-5090-5091-8/16 $31.00 © 2016 IEEE
DOI 10.1109/SIoT.2016.9

discussed in detail. Similarly, the provenance management schemes have been proposed for sensor networks [34], [35], [36], [37], however, these schemes are not directly applicable to IoT scenarios due to the complex IoT architecture.

Specifically, the major contributions of the work presented in this paper are:

- Highlight security challenges on resource-constraint IoT devices addressed in existing literature.
- Provide a discussion on potential secure provenance techniques which may be incorporated in or customized for IoT (WSN-based, RFID-based and IP-based).
- Identify generic secure provenance management challenges for IoT along with future research direction.
- Formulate a threat model for WSN-based, RFID-based and IP-based IoT.

The rest of the paper is organized as follows. Section 2 presents the threat model. Section 3 discusses the resource constraints and security challenges for various IoT technical infrastructure including WSN-based IoT, RFID-based IoT, and IP-based IoT. An overview of generic requirements for a provenance-aware IoT model is provided in Section 4. Finally, we conclude the paper with a discussion of future work.

II. Threat Model

Consider a hypothetical scenario: A sensor node n_s (source node) has to transmit d (data) to another sensor node n_d (destination node). An adversary m (Mallory) may collude to execute any form of attack including extracting, altering or forging P_{data} provenance data as follows:

1) Eavesdrop or perform traffic analysis on data path d_p between n_s and n_j in the hope to gain information about participating entities, data or metadata. The communication channel is subject to various others attacks including packet dropping, injecting packets or overwriting d or P_{data} or carrying out conflict collusion (tags or readers).
2) Compromise any n_i (legitimate node) to extract K (keying material) or to gain access to confidential information including d and P_{data}.
3) Deploy any arbitrary n_m (intruder node) to tunnel traffic to another network i.e. performing wormhole/sinkhole attack. For instance, during bootstrapping and operational phase n_m might be installed which ultimately results in the loss of P_{data}.
4) Breach personal or data privacy by accessing RFID tags even after decommissioning of IoT devices. The individuals carrying tags can be followed based on their traces in cyberspace without even being aware of it.
5) Execute provenance forgery by using fake key pairs to make provenance records unverifiable.
6) Selectively removing a certain part of the preceding P_{chain} (provenance chain) without being tamper-evident may have deleterious affect on reconstruction of events, data reconciliation or inferring data quality.
7) Impersonating border routers or synchronizing nodes.
8) Oblivious to the legitimate nodes, replaying old data to end-users.

III. Binding IoT and Provenance: Challenges and Constraints

Secure IoT infrastructure leads to reliable data and ultimately trustworthy provenance. Without considering secure environment for IoT devices, it may be impractical to think of secure data and associated metadata against each device in IoT. Therefore, leveraging the security solutions for IoT, the associated provenance data can enforce the authenticity of data required in various applications including supply chain, e-health, agriculture domain etc. In this section we will discuss the security challenges related with resource constraints in terms of IoT technical infrastructure including RFID-based IoT, WSN-based IoT, IP-based IoT. We have further evaluated each of the infrastructure based on security and resource constraints.

A. RFID-based IoT

RFID (Radio-Frequency Identification) technology can automatically identify tag signal to obtain relevant data from objects. There are many security challenges associated with resource constraints in RFID-tagged items ranging from uniform coding to conflict collision, privacy protection to trust management and traceability issues of node failures. We focus on these requirements with reference to provenance collection. For instance, to enforce data privacy many physical-based and password-based schemes have been proposed [70], [69], [67], [68]. Depending on application and vendor, RFID tag can only store basic information. Due to this limitation, along with other important information, provenance data can also be maintained at upper level services. Provenance data can enable the information provider to trace data and client privacy thereby thwarting inference attack. Similarly, to provide resilience to attacks and to establish trust among RFID tag, reader and base station (BS), considering digital signatures and cryptographic algorithms, the tag storage and computing power is part of ongoing research [30].

IoT comprise of network of interconnected devices which may complicate traceability, for example, tracking and monitoring of food logistics [18], [19], pharmaceutical supply chain [20], [21], agriculture product [22], item-level supply chain [25], dairy farming system [26]. Thus another perspective of provenance in IoT devices is to resolve traceability issues in IoT by associating metadata tag with each individual part of composite object. For example, tracking such metadata is more beneficial when RFID tags are combined with senors helping store agents in supply chains to track the status (quantity and quality) of goods [31].

In addition to security concerns, the resource-related constraints are particularly important to consider for provenance collection. For instance, data processing awareness along with data volume and deep heterogeneity [30]. Such constraints tend to effect the collection of provenance i.e. it raises the question of how to gather provenance in case of network congestion, massive heterogeneous raw data formats, complexity of tag (active and passive, rewritable) [27] and other processing constraints.

B. IP-based IoT

The introduction of IPv6 and web services facilitate homogeneous protocol ecosystem allowing simple integration with Internet hosts and development of different appliances for IoT applications [29]. Coupling resource-constrained networks and powerful Internet results in diverse security requirements ranging from end-to-end security (node security, application security) to communication channel security (bootstrapping security, network security) [29].

In IP-based IoT, gathering provenance is another important issue which raises the question, "Provided the constraints, provenance should be gathered at which level to attain optimal information about participating sensor nodes". In this regard, provenance collection can be classified as Level-based (node level, network level, or application level) and Phase-based(bootstrapping phase and operational phase) provenance collection. Since each of the level is mapped to a phase thereby provenance data may duplicate itself which may facilitate confidence of correctness in sensors provenance metadata. Furthermore, collection of provenance at any level or phase also affects the level of accuracy of provenance data. For instance, provenance collected at node level can depict more specialized details as compared to the data that may arrived at application with the high probability of suffering from tampering.

Level-based provenance collection:

The resource-constrained things/nodes in IoT vary in terms of energy supply, for example, battery-oriented and battery-less nodes focusing on low energy consumption or lowest power mode/sleep mode. Under such circumstances, provenance collection may suffer because of the unavailability of dormant mode of sensor at a particular instant or due to energy supply constraints. In IP-based IoT [29], provenance collection at network level may lead to other issues including integration of provenance capture mechanism at either network layer or data link layer. Provenance can be collected at application level but it may not be trustworthy as attacker may already have forged the sensor data while in transit.

Phase-based provenance collection:

The collection of provenance can be carried out at bootstrapping phase- which denotes joining thing in the IoT at a particular time and location. The trust bootstrapping between the nodes of different vendors [29] is of significant importance, because device identity and security parameters are provided to the device during this phase. Therefore, collected provenance data can provide information about device identification and security parameters of participating entities. Similarly, the collection of provenance at operational phase may consist of information including decommissioning, re-ownership of devices and maintenance needs to be gathered during operational phase.

C. WSN-based IoT

If we want to completely integrate WSN into the Internet, we should know what kind of integration approaches can be used to connect both infrastructures. According to Grangal et al. [32] WSN to Internet based integration can be classified as:

1) Cloud-based integration approaches: One integration approach for WSN to Internet is via cloud web services. In this approach, the sensing data retrieved from WSN sensing devices is transmitted to cloud servers via a gateway, which may also support operations such as data aggregation, protocol translation etc. The interconnection of different WSN applications using cloud-based services may be difficult and may require tailor made applications, rather than being enabled by standard Internet communication mechanisms as in other approaches. Nevertheless, this integration approach does provide a simple solution to the problem of accessing distributed sensing data in the context of Internet applications. Some of the approaches which are following cloud based integration approach include LogMeIn [43], SensorCloud [44], SensaTrack [45], NimBits [46] and ThingSpeak [47].

2) Front-end proxy integration approaches: In this approach a gateway exists to isolate WSN communications from the Internet and acts as a front-end proxy. The proxy may obtain the data from sensing devices following two main strategies. One approach consists of data being collected from a sensing device as soon as a request arrives from an Internet client. The other approach employs a push protocol where sensing devices update data on the proxy only when a change occurs, and in this case the proxy maintains a local cache for all the relevant sensed data.

3) Architecture frameworks: Various research projects [48], [49], [50], [51] want to target the design of architecture frameworks that support different strategies to enable communications between various WSN domains over the Internet. Most of these proposals tend to propose a middleware to abstract operations on sensing devices from the particularities of WSN communications. As a result, these proposals provide complex applications over distributed WSN islands instead of focusing on design of Internet communication mechanisms for WSN environments.

4) Integration via standard Internet communication protocols: Using this approach, mechanisms and techniques may be designed to adapt Internet communications and security technologies to WSN environments. A group of protocols based on 6LoWPAN is currently being designed at various working groups of the IETF (Internet Engineering Task Force), which will enable Internet communications on low-power WSN environments [32]. These protocols would provide the basis for extending existing Internet communication architectures to encompass WSN applications. This approach enables WSNs to be fully integrated with the Internet. While this approach can certainly be more complex with respect to security and can open up sensing devices to a large number of threats and attacks.

WSNs can be connected to Internet using three main approaches as mentioned by [33], differing from the WSN integration degree into the Internet structure. The first proposed approach consists of connecting both independent WSN and the Internet through a single gateway. In the second approach dual sensor nodes can access the Internet via multiple gateways. In the third approach multiple sensor networks can join the Internet in one hop through gateways.

IV. Challenges for Provenance-Aware IoT

In this section, challenges for a provenance-aware IoT system are identified. The requirements for secure provenance can be categorized into generic provenance management challenges and provenance security challenges.

A. Provenance Management Challenges

1) Data Storage and Processing: -Scalability: Demands efficiently managing the increase in granularity level of information captured by provenance with the increase in sensor nodes in a network. In IoT, the provenance tends to grow very fast due to increasing number of participating nodes. Thus the transmission of a large amount of provenance information along with data from each sensory node will obviously incur significant bandwidth overhead, resulting in scalability issues. Achieving scalability needs analysis of space complexity and energy computation overhead thereby using any lightweight secure provenance framework, for example, SPROV [41].

-Data-Provenance Binding: A coupling between data and provenance is required to avoid inconsistencies issues (during backup, restoration and copying of data) and to thwart the attacker from altering data or swapping provenance. A solution to this problem has been suggested in [34] where the data provenance coupling is ensured at each node in routing path rather than at BS.

-Interoperability of heterogeneous data: Data from diverse sensor devices may create problems related to interoperability of data, for instance, aggregation of data in various formats including (navigational sensors, motion sensors, temperature sensors, environmental sensors) and their associated provenance. Therefore, it is necessary to achieve service and semantic interoperability, amongst other things. RSN (RFID sensor network) technology can be used to solve heterogeneity problem [30].

2) Fault Tolerance: There are certain situations when sensor devices stop sending data or start sending problematic data. Such scenario can be easily handled in centralized IoT architecture as the central entity have access to all data flows. However in distributed IoT architecture, to assure survivability of the network it is necessary to develop a discovery mechanism for identification of data flow, data providers, service providers and data processing entities [28]. Under such circumstances, ensuring trustworthiness of provenance data is a challenging task. A WSN-based scheme [34] for data-provenance binding resolve this issue by performing data aggregation verification at BS and data-provenance coupling verification at node level. In case of RFID tags faulty read will result in processing of faulty data, causing undesirable results, such as inaccurate inventories are yet to be resolved.

B. Provenance Security Challenges

1) Integrity and Confidentiality: Confidentiality is an important requirement for provenance-aware IoT model. Confidentiality must ensure that an adversary should not be able to gain any knowledge (for instance, data or keying material) of provenance by analyzing data. In the context of IoT, confidentiality implies that just by analyzing the packet data and metadata an adversary cannot infer information about the provenance attached to the data. Bloom Filter scheme [34] has satisfied the confidentiality requirement by encoding provenance information in bloom filters using one way hash functions. The inter-packet delay scheme [36] achieves confidentiality by hiding provenance in inter-packet delays. The arithmetic coding scheme [37] achieves confidentiality by encoding provenance in intervals defined by two real numbers. The PKLC scheme [39] tends to achieve confidentiality by encrypting sensitive fields using single session key and then encrypt each copy of the session key with public key of trusted auditor. The mutual agreement scheme [42] achieves confidentiality using the same broadcast encryption [66] as used by PKLC scheme. The integrity of provenance is of three types:

Data Integrity: Data Integrity ensures that provenance information must be tamper-evident. The PKLC [39] scheme ensures data integrity by hashing provenance information field and signing it by corresponding node. The mutual agreement scheme [42] achieves data integrity by using current signature, which protects the field of the same record.

Origin Integrity: Origin Integrity ensures that any node making changes to provenance chain cannot deny its ownership to a provenance record. To resolve false provenance, PKLC [39] scheme uses digital signatures for origin integrity. The mutual agreement signature scheme [42] uses chained signatures to assure origin integrity by including records containing signature of every subsequent user in chain.

Chain Integrity: Chain integrity ensures that an adversary acting alone or colluding cannot modify the order of provenance records. Bloom Filter based scheme of Sultana et el. [34] ensures chain integrity by sharing secret keys with all nodes that attackers must know to reconstruct provenance for adding or removing nodes in the provenance chain. Dictionary scheme [35] uses AM-FM sketch, which is a node level digital signature scheme, to achieve chain integrity. The AM-FM sketch uses a one way hash function that makes it hard for an adversary to obtain provenance from digest and any removal of nodes from provenance will be detected by AM-FM verification at the BS. This makes it difficult to modify the order of records since modifying the order consist of steps of adding and deleting records. The inter-packet delay scheme (IPDs) [36] uses delays in order to achieve chain integrity as an attacker will have to adjust IPDs of non-colluding packets, thereby adding too much delay to packets and hence getting detected at the BS. The Arithmetic coding scheme [37] achieves chain integrity by using association probabilities and cumulative association probabilities which the BS shares secretly with each node. The PKLC [39] ensures chain integrity using a chain of linked public keys and any removal or addition to provenance can be detected by checking whether the chain of linked public keys is broken or not. The mutual agreement scheme [42] provides chain integrity by providing previous and next signature fields that form the mutual agreement between users that links the provenance records of the chain.

2) Privacy: In IoT, privacy is one of the primitive considerations for the protection of information of individuals from exposure in the IoT environment, in which almost any physical or logical entity has been assigned a unique identifier and the ability to communicate autonomously over the Internet or similar network. The provenance generated as result of data deluge by smart objects can be alarming to the privacy. For any privacy-aware provenance system, privacy needs to be ensured at data/module level and structural level. The privacy assurances tends to be more challenging under interoperability of things when data along with metadata from multiple endpoints is gathered, collated and analyzed.

3) Access Control: To establish trust management for data provenance, the differentiated access control policies can be employed. For example, a trusted central entity containing access control policies can regulate access to provenance data by defining user's privileges through access control lists (ACLs) or role-based access control (RBAC) mechanisms. Thus it may avoid adversaries from masking illicit actions (for instance, modifying provenance data or forging provenance chain), certain designated auditors exist that can read any provenance chain.

4) Freshness: The freshness requirement requires that an adversary cannot replay captured data and provenance without being detected. It means that even if an adversary captures part of data and provenance information they cannot replay it to authorized nodes without being detected by auditors. Bloom filter based scheme [34] achieves freshness using the variation in bloom filter hash. The bloom filter value varies from packet to packet making it difficult to associate any previous bloom filter with more recent data. Dictionary scheme [35] achieves freshness by associating a packet with a sequence number that is incremented in subsequent rounds. The inter-packet delay scheme [36] achieves freshness by making provenance bit for any IPD to depend upon the timestamp of next packet and making it change with varying timestamps. The arithmetic coding scheme [37] satisfies freshness property by giving each packet a sequence number and ensuring that the packet arrives within a preset tolerance interval.

5) Availability: The availability requirement requires that no nodes in the provenance chain can selectively drop nodes from the provenance chain without being detected. This means that any two nodes colluding or not cannot remove records in a valid provenance chain between them. Bloom Filter based scheme of Sultana et al. [34] ensures availability by providing secret keys for all nodes that must be known to the attackers to reconstruct provenance in order to remove nodes to the provenance chain. Dictionary scheme [35] uses AM-FM sketch to provide availability. The inter-packet delay scheme [36]uses delays for achieving availability as an attacker will have to adjust IPDs of non-colluding packets, which would add too much delay to packets. This increased delay would be detected at the BS. The Arithmetic coding scheme [37] achieves availability by using association probabilities and cumulative association probabilities which the BS shares secretly with each node. The PKLC [39] ensures availability by using a chain of linked public keys. Any removal or addition to provenance can be detected by detecting whether the chain of linked public keys is broken or not. The mutual agreement scheme [42] provides availability by providing previous and next signature fields that form the mutual agreement between users that links the provenance records of the chain.

6) Key Distribution and Establishment: The key distribution and establishment is an important requirement for provenance in IoT. In sensor networks, base stations are responsible for sharing keys among sensor nodes. These shared keys are then used to encrypt provenance information. However, this is not applicable for IoT scenarios where keys have to be established between clients and servers both located on different networks. Hence, key distribution and establishment mechanisms need to be addressed. Various key management and distribution schemes have been proposed for WSNs [53], [65]. However, these schemes are not directly implementable in IoT due to constraints such as not being able to agree on keys present among base stations located in different IoT networks, not being able to determine the correct size of the pool of keys for the different IoT networks from where keys for sensor nodes have to be chosen and not being able to synchronize the pool of keys among various IoT networks.

V. Conclusion

In this paper, we addressed the need for integration of secure provenance in IoT. Considering the security concerns in IoT, we have primarily focused on the provenance management issues in IoT. A threat model has been presented that illustrate the potential threats to provenance data in IoT scenario. We have discussed the possible solutions for incorporating provenance in IoT. Furthermore, we have highlighted the available schemes in literature for the secure provenance data to ensure the trustworthiness of data being generated by sensor devices. A logical extension of this research is to make provenance-aware IoT model scale to RFID-based IoT, WSN-based IoT and IP-based IoT. We are also looking to find more efficient ways to solve the trustworthy provenance data. Our solutions to such challenging problems will be the subject of the forthcoming research.

VI. Acknowledgement

This work was supported by the Industrial Core Technology Development Program(10049079 , Development of Mining core technology exploiting personal big data) funded by the Ministry of Trade, Industry and Energy (MOTIE, Korea). Dr. CS Hong is the corresponding author.

References

[1] Hasan, Ragib, Radu Sion, and Marianne Winslett. *Introducing secure provenance: problems and challenges*, Proceedings of the 2007 ACM workshop on Storage security and survivability. ACM, 2007.

[2] Vasseur, J. P. *Terms Used in Routing for Low-Power and Lossy Networks*. RFC 7102, January, 2014.

[3] Chebotko, Artem, et al. *RDFProv: A relational RDF store for querying and managing scientific workflow provenance*, Data & Knowledge Engineering69.8 (2010): 836-865.

[4] Freire, Juliana, et al. *Provenance for computational tasks: A survey*, Computing in Science & Engineering10.3 (2008): 11-21.

[5] Wolstencroft, Katherine, et al. *The Taverna workflow suite: designing and executing workflows of Web Services on the desktop, web or in the cloud*,Nucleic acids research (2013): gkt328.

[6] B. Ludscher, I. Altintas, C. Berkley, D. Higgins, E. Jaeger, and et al. Scientific Workflow Management and the Kepler System. Concurrency and Computation: Practice and Experience, 18(10):10391065, 2006.

[7] Simmhan, Yogesh L., Beth Plale, and Dennis Gannon. *Karma2: Provenance management for data-driven workflows*,Web Services Research for Emerging Applications: Discoveries and Trends: Discoveries and Trends(2010): 317.

[8] Bowers, Shawn, Timothy M. McPhillips, and Bertram Ludscher. *Provenance in collectionoriented scientific workflows*, Concurrency and Computation: Practice and Experience 20.5 (2008): 519-529.

[9] Davidson, Susan B., et al. *On provenance and privacy*, Proceedings of the 14th International Conference on Database Theory. ACM, 2011.

[10] Vicknair, Chad, et al. *A comparison of a graph database and a relational database: a data provenance perspective*, Proceedings of the 48th annual Southeast regional conference. ACM, 2010.

[11] Zhang, Jing, Adriane Chapman, and Kristen Lefevre. *Do you know where your datas been?Tamper-evident database provenance*, Secure Data Management. Springer Berlin Heidelberg, 2009. 17-32.

[12] Asghar, Muhammad Rizwan, et al. *Securing data provenance in the cloud*,Open Problems in Network Security. Springer Berlin Heidelberg, 2012. 145-160.

[13] Muniswamy-Reddy, Kiran-Kumar, Peter Macko, and Margo I. Seltzer. *Provenance for the Cloud*, FAST. Vol. 10. 2010.

[14] Ko, Ryan KL, and Mark Will. *Progger: An Efficient, Tamper-Evident Kernel-Space Logger for Cloud Data Provenance Tracking*, Cloud Computing (CLOUD), 2014 IEEE 7th International Conference on. IEEE, 2014.

[15] Abbadi, Imad M. *A framework for establishing trust in Cloud provenance*, International journal of information security12.2 (2013): 111-128.

[16] Muniswamy-Reddy, Kiran-Kumar, and Margo Seltzer. *Provenance as first class cloud data*, ACM SIGOPS Operating Systems Review43.4 (2010): 11-16.

[17] Lu, Rongxing, et al. *Secure provenance: the essential of bread and butter of data forensics in cloud computing*, Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security. ACM, 2010.

[18] Zhao, Xiaorong and Fan, Honghui and Zhu, Hongjin and Fu, Zhongjun and Fu, Hanyu, *The Design of the Internet of Things Solution for Food Supply Chain*, 2015 International Conference on Education, Management, Information and Medicine, 2015,Atlantis Press.

[19] Zhang, Weimei, *Study about IOT's application in" Digital Agriculture" construction*, Electrical and Control Engineering (ICECE), 2011 International Conference on, 2578–2581,2011, IEEE.

[20] Barchetti, Ugo and Bucciero, Alberto and De Blasi, Mario and Mainetti, Luca and Patrono, Luigi, *RFID, EPC and B2B convergence towards an item-level traceability in the pharmaceutical supply chain*, RFID-Technology and Applications (RFID-TA), 2010 IEEE International Conference on, pages 194–199, 2010,IEEE.

[21] Barchetti, Ugo and Bucciero, Alberto and De Blasi, Mario and Mainetti, Luca and Patrono, Luigi, *Implementation and testing of an EPCglobal-aware discovery service for item-level traceability*, 2009 International Conference on Ultra Modern Telecommunications & Workshops, pages 1–8,2009,IEEE.

[22] BAI, Hong-wu and SUN, Ai-dong and CHEN, Jun and SUN, Li-rong and LU, Hai-yan and LIANG, Ying and LIU, Xian-jin, *Agricultural products traceability system for quality and safety based on internet of things*, Jiangsu Journal of Agricultural Sciences,volume 2, pages 034, 2013.

[23] Alam, SM Iftekharul, and Sonia Fahmy. *A practical approach for provenance transmission in wireless sensor networks* Ad Hoc Networks16 (2014): 28-45.

[24] Alam, SM Iftekharul, and Sonia Fahmy. *An energy-efficient approach for provenance transmission in wireless sensor networks*Sensor, Mesh and Ad Hoc Communications and Networks (SECON), 2012 9th Annual IEEE Communications Society Conference on. IEEE, 2012.

[25] Zhou, Wei, and Selwyn Piramuthu. *IoT and Supply Chain Traceability*, Future Network Systems and Security, Springer International Publishing, 2015. 156-165.

[26] SU, Zhongbin, and Yuanyuan GUO.*Application of coding based on IOT for dairy traceability system*, Journal of Northeast Agricultural University 8 (2014) 017.

[27] Weber, Rolf H. *Internet of ThingsNew security and privacy challenges*,Computer Law & Security Review 26.1 (2010): 23-30.

[28] Roman, Rodrigo, Jianying Zhou, and Javier Lopez. *On the features and challenges of security and privacy in distributed internet of things*, Computer Networks 57.10 (2013): 2266-2279.

[29] Heer, Tobias, et al. *Security Challenges in the IP-based Internet of Things*, Wireless Personal Communications 61.3 (2011): 527-542.

[30] Jing, Qi, et al. *Security of the internet of things: Perspectives and challenges*, Wireless Networks 20.8 (2014): 2481-2501.

[31] http://www.rfidjournal.com/

[32] Granjal, J., Monteiro, E., & Silva, J. S.(2015) Security in the integration of low-power wireless sensor networks with the Internet: A survey. Ad Hoc Networks, 24, 264-287.

[33] R. Roman and J. Lopez, *Integrating Wireless Sensor Networks and the Internet: a Security Analysis*, Internet Research: Electronic Networking Applications and Policy, vol. 19, no. 2, 2009.

[34] Sultana, S., Ghinita, G., Bertino, E., & Shehab, M.*A lightweight secure scheme for detecting provenance forgery and packet drop attacks in wireless sensor networks*, Dependable and Secure Computing, IEEE Transactions on, 12(3), 256-269.

[35] Wang, C., Hussain, S., & Bertino, E. (2014). *Dictionary based secure provenance compression for wireless sensor networks*.

[36] Sultana, S., Shehab, M., & Bertino, E. (2013). *Secure provenance transmission for streaming data*, Knowledge and Data Engineering, IEEE Transactions on, 25(8), 1890-1903.

[37] Hussain, S. R., Wang, C., Sultana, S., & Bertino, E. (2014, December).*Secure data provenance compression using arithmetic coding in wireless sensor networks*, In Performance Computing and Communications Conference (IPCCC), 2014 IEEE International (pp. 1-10). IEEE.

[38] Hasan, R., Sion, R., & Winslett, M. (2009, February). *The Case of the Fake Picasso: Preventing History Forgery with Secure Provenance*, In FAST (Vol. 9, pp. 1-14).

[39] Wang, X., Zeng, K., Govindan, K., & Mohapatra, P. (2012, October). Chaining for securing data provenance in distributed information networks. InMILITARY COMMUNICATIONS CONFERENCE, 2012-MILCOM 2012 (pp. 1-6). IEEE.

[40] Bauer, Sabine, and Daniel Schreckling. *"Data Provenance in the Internet of Things*,EU Project COMPOSE, Conference Seminar. 2013.

[41] R. Hasan, R.Sion, & M.Winslett, (2009). *Preventing history forgery with secure provenance*,ACM Transactions on Storage (TOS),5(4), 12.

[42] Rangwala, M., Liang, Z., Peng, W., Zou, X., & Li, F. A Mutual Agreement Signature Scheme for Secure Data Provenance.environments,13, 14.

[43] Xively by LogMeIn. <https://xively.com/>

[44] SensorCloud powered by LORD MicroStrain. <http://2234 www.sensorcloud.com/>

[45] SensaTrack. <http://www.sensatrack.com/>

[46] NimBits The Open Source Internet of Things on a Distributed Cloud. <http://www.nimbits.com/>

[47] ThingSpeak. <https://www.thingspeak.com/>

[48] SENSEI (Integrating the Physical with the Digital World of the Network of the Future) <http://www.sensei-project.eu/>.

[49] Emiliano De Cristofaro, Jens-Matthias Bohli, Dirk Westhoff, FAIR: fuzzy-based aggregation providing in-network resilience for realtime wireless sensor networks, in: Proceedings of the second ACM Conference on Wireless Network Security, ACM, 2009.

[50] Santander on FIRE Future Internet Research and Experimentation <http://www.smartsantander.eu/>

[51] WISEBED. <http://wisebed.eu/site/>

[52] Zhu S, Xu S, Setia S, Jajodia S,(2003), *Establishing pair-wise key for secure communication in ad hoc networks A probabilistic approach*, In Proceedings of the 11th IEEE International Conference on Network Protocols (ICNP03), Atlanta, Georgia, November 47.

[53] Kui Ren, Kai Zeng and Wenjing Lou,(2006), *A new approach for random key pre-distribution in large-scale wireless sensor networks*, wireless communications and mobile computing, Vol 6,No 3 ,pp307-318.

[54] S.Sibi, A. R Thamizarasi,(2013), *Key Pre-Distribution Methods of Wireless Sensor Networks*, International journal of Scientific & Engineering Research, Vol 4.

[55] Shruthi. P, M. B. Nirmala & A. S Manjunath,(2013) *Secured Modified Bloom's based Q-composite Key Distribution for Wireless Sensor Networks*, International Journal on Advanced Computer Theory and Engineering (IJACTE), Vol.2, No.5, pp2319 2526.

[56] J.Deng ,Y.S.Han ,(2008) *Multipath Key Establishment for Wireless Sensor Networks Using Just Enough Redundancy Transmission*, IEEE Transactions on Dependable and Secure Computing, Volume 5, No 3, pp 177-190.

[57] Chi-Yuan chen, Han-Chen chao,(2011),*a survey of key distribution in wireless sensor networks*, published online in wiley online library.

[58] S.B.Wicker and M. J. Bartz,(1994), *Type-II hybrid-ARQ protocols using punctured MDS codes*, IEEE Trans. on Communications, vol. 42, no. 2/3/4, pp 14311440.

[59] C. Blundo, A. D. Santis, A. Herzberg, S. Kutten, U. Vaccaro, and M. Yung,(1992) Perfectly-secure key Distribution For dynamic conferences, inProc. CRYPTO 92: 12th Annual International Cryptology Conference on Advances in Cryptology. London:Springer-Verlag,pp 471486.

[60] W.Du, J.Deng, Y.S. Han and P.K.Varshney,(2003), *A pairwise key predistribution scheme for wireless sensor networks*, in Proc.10th ACM Conference on Computer and Communications Security.

[61] D.Liu, P.Ning, W.Du,(2008) *Group-Based Key Predistribution for Wireless Sensor Networks*, ACM Transactions on Sensor Networks, Vol. 4, No. 2.

[62] F.Anjum,*Location dependent key management using random key-predistribution in sensor networks*, Proceedings of the 5th ACM workshop on Wireless security.

[63] J.Wang, L.Xia, J.Jing, *Analysis for Location-Based Key Predistribution in wireless Sensor Networks*, proceedings of the 2009 Second International Conference on Information and Computing Science ,Vol. 02 ,pp 297-300.

[64] Delgosha, F., & Fekri, F. (2005, September). *Key predistribution in wireless sensor networks using multivariate polynomials*. In Sensor and Ad Hoc Communications and Networks, 2005. IEEE SECON 2005. 2005 Second Annual IEEE Communications Society Conference on (pp. 118-129). IEEE.

[65] M. Javanbakht, H.Erfani, H.H. S.Javadi and P.Daneshjoo,(2014) *Key Predistribution Scheme for Clustered Hierarchical Wireless Sensor Networks based on Combinatorial Design*, Published online in Wiley Online Library, Vol. 7, No 11, pp 20032014.

[66] D. Halevy and A. Shamir. *The LSD broadcast encryption scheme*,In Proc. of the 22nd Annual International Cryptology Conference on Advances in Cryptology (CRYPTO), pages 4760, London, UK, 2002. Springer-Verlag

[67] Juels, A., Rivest, R. L., & Szydlo, M. (2003). *The blocker tag:Selective blocking of RFID tags for consumer privacy*, In Proceedings of the 10th ACM conference on computer and communications security (CCS 2003), (pp. 103111).

[68] T2TIT Research Group. (2006). The T2TITThing to thing in the internet of things-project. ANR.

[69] Weis, S. A., Sarma, S. E., Rivest, R. L., & Engels, D. W. (2004).*Security and privacy aspects of low-cost radio frequency identification systems. Security in Pervasive Computing*, 2802, 201212.

[70] Spiekermann, S., & Berthold, O. (2005). *Maintaining privacy in RFID enabled environments.Privacy, security and trust within the context of pervasive computing* (pp. 137146). Berlin:Springer.