International Journal of Engineering & Technology, 7 (4) (2018) 4899-4904

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET
doi: 10.14419/ijet.v7i4.23147
Research paper



Internet of things security vulnerabilities and recommended solutions

Rashidah F. Olanrewaju [1], Burhan ul Islam Khan [1] *, Farhat Anwar [1], Roohie Naaz Mir [2]

[1] Department of ECE, Kulliyyah of Engineering, IIUM Malaysia
[2]Department of CSE, National Institute of Technology, J&K, India
**Corresponding author E-mail: Burhan.iium@gmail.com*

Abstract

The applications based on IoT are ubiquitous in providing passive user involvement on the collective approach of sensor technology, embedded system, networking and communication convergence with analytical computing. The application framework of IoT comprises of devices that are highly heterogeneous and compute migrations from sensor to IoT gateways to edge/fog computing to the cloud and then back to the client along with various alarming components. As observed from the review work, providing security for such networks is in its young stage in the form of an integrated architecture offering perfect security together with network and application possibilities although the shortcomings of IEFT and IEEE contribute more towards the same. Besides, the present researchers have not yet achieved the actual threshold of real-time performance potentials with respect to lesser computational complexity, usage of smaller key size, conformable security, lesser memory overheads, smaller ciphertext size, speedy processing time of algorithms, robust to possible threats and reduced communication/network overhead for ensuring a lighter security mechanism. This paper focusses on the security issues posed by large-scale heterogeneous IoT paradigm and arriving at a secure architectural framework adoptable by a variety of applications that include smart transportation, smart cities, smart healthcare, etc. based on IoT.

Keywords: *Internet of Things (IoT); IoT Security; Authentication, Key Management; Signcryption.*

1. Introduction

The IoT describes the scenarios where the internet connectivity and computing capability are collaborated with heterogeneous objects, devices, sensors and other day-to-day items. It provides many applications to the humans by attaching devices to a human being as either in wearable or ingestible forms, to monitor and maintain human health wellness, disease management, increased fitness, etc. [1-4]. IoT provides applications in controller and security systems in the retail environments where consumers are engaged in commerce such as Stores, Banks, Restaurants (applications like self-checkout, in-store offers, inventory optimization, etc.). Apart from these, other applications include: 1) Energy management and Security in office buildings 2) Improved productivity in industrial environments 3) Public spaces and infrastructure in urban settings including adaptive traffic control, smart meters, environmental monitoring, resource management, etc. 4) Outside uses include railroad tracks, autonomous vehicles (outside urban locations), and flight navigation; real-time routing, connected navigation, shipment tracking, etc. [5-9].

All the above applications during their real-time implementations may present some of the new and unique security as well as privacy challenges [10-14]. Gaining the trust of users in the context that IoT devices and related data services are secure from vulnerabilities has turned out to be a critical task for allowing IoT to become more pervasive and integral part of our daily lives. Poorly secured IoT devices and services can serve as potential entry points for cyber-attack and expose user data to theft by leaving data streams inadequately protected [15], [16].

Auto-interconnectivity of participating devices of IoT makes it more vulnerable and affects the security and resilience of the Internet globally. Besides, the distributed computing in such networks also adds to the security loopholes [17]. This challenge becomes more complicated if there is a large-scale deployment of heterogeneous IoT devices being realized in physically unsecured environments.

It becomes a principal motivation for the researchers, developers and designers of IoT devices and systems to have a collective obligation for ensuring that they do not expose users and the IoT itself to potential harm. Accordingly, a collaborative approach to security will be needed for the development of effective and appropriate solutions to IoT security challenges that are well suited to the scale and complexity of the issues.

The rest of the paper is organized into five sections where Section 2 presents the research evolution in IoT related to security. Section 3 discusses the problem statement deduced from the literature review conducted. The recommended solutions for overcoming the issues posed by IoT have been presented in Section 4. Finally, the conclusion has been given in Section 5.

2. Literature review

The issue of secure communication with optimal usage of resources in a heterogeneous environment of IoT is vital because without having a guarantee of security of data, seamless communication plus the adoptability and sustainability of IoT for mission-critical applications will be a question mark. Though the individual efforts towards securing communication channel among WSN and internet/IoT besides handling the issue of authentication and key management in perspective of IoT provides certain achievement towards these goals but having a designed framework of integrated security at a different layer to be synchronized with many other

Copyright © 2018 Rashidah F. Olanrewaju et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

network parameters and resources becomes a bottleneck. Consideration of architecture for secure communication for over-all requirements of meeting an objective of a balance between security and the application goal is the requirement to study and research in huge heterogeneity. Thus, the focus should be more on an open security system; however, it is a fact that provision of security system is not merely a core technical problem, it needs the collaboration and synchronization of many policies, laws, and regulations to have a complete and faultless system for mutual collocation [18], [19].

The market time of conceptualizing the application and technological improvement gap is meager today, so many solutions or technology vendors are having their initiatives towards architecting the secure models [20], where various questions are dealt with, and it is concluded that there is no single silver bullet and locking doors but leaving a window open isn't enough. Fortunately, IoT security can be covered with four cornerstones: Protecting Communications, Protecting Devices, Managing Devices, and Understanding Your System with IoT system's unique additional security needs and challenges. The research direction towards novel security architecture has become a de facto in today's research time domain [21-23]. Table 1 highlights the significant contribution along with the limitation of many prior works access management in the field of IoT.

Table 1: Summary of the Findings

Author	Contribution	Limitations
(Zhao et al., 2011) [24]	A lightweight mutual identity authentication scheme for IoT.	• No concept of hierarchical accesses control. • Consideration of general IoT. • Heterogeneity within the network not taken into account.
(Ye et al., 2014) [25]	Efficient access control and authentication method for the perception layer of IoT.	• Consideration of general IoT. • Limited applicability • Heterogeneity among nodes at perception layer not considered. • Provides forward secrecy only. • Not tested on open architecture/ Standard architecture.
(Hu et al., 2012) [26]	Mutual identity authentication using modified elliptic mapping in authentication and key update mechanisms for multi-hop relay.	• Heterogeneity of the network not considered. • No distinctions between global and local IoT. • Absence of an authorization component.
(Patel et al., 2016) [27]	Capability Based Access Control (CBAC) and Elliptic Curve Cryptography based Mutual Authentication (EMA) model for securing authorization	• No distinctions between global and local IoT. • Heterogeneity of nodes not considered.
(Ma and Chen, 2016) [28]	Authentication protocol based on quantum key distribution using the decoy-state method for heterogeneous IoT.	• Authorization Component is missing. • Consideration of general IoT.
(Barreto et al., 2005) [29]	IBC-based signcryption scheme	• Can't be used for heterogeneous communication.
(Li et al., 2010) [30]	PKI-based signcryption scheme	• Can't be used for heterogeneous communication.
(Sun and Li, 2010) [31]	Heterogeneous signcryption scheme	• Not Secure against Insider attacks • High computational cost makes it unsuitable in WSN scenarios.
(Huang et al., 2011) [32]	Heterogeneous signcryption with provisions of Key privacy.	• High computational cost makes it unsuitable in WSN scenarios. • High offline storage requirement limits its applicability in PAN sensors.
(Li and Xiong, 2013) [33]	Heterogeneous Online / Offline based signcryption.	• Usage of point multiplication limits its applicability resource-constrained devices. • No provisions to accommodate the secure mobility of motes.
(Li et al., 2016) [34]	Heterogeneous Certificateless online/offline signcryption.	• Offline storage issue is still unsolved.

3. Problem statement

The security mechanism in traditional ad-hoc networks including wireless sensor network, mobile ad-hoc network, etc. is limited to small-scale node to node authentication and a viable key management system [30], [35]. The applications where these networking paradigms are conceptualized are usually deployed in human-inaccessible areas, where all the nodes have pre-deployment keys. The communication takes place in a reverse multicast way, where all the sensor node data or aggregated data on the cluster head node need to be delivered to a sink node which is generally kept on the nearby distance from the deployment zone. Thus, a simple node to node authentication utilizing pre-installed keys is enough in some energy efficient ways to meet the resource as well as the security optimization goal in such a pure homogeneous system. The only possible alternative to disturb the security model is to perform a node capture attack, where physically the deployed nodes are taken for understanding the pre-installed keys and its exchange mechanism. Later, the spoofed nodes are deployed into the application terrain, where the solution approach like identifying the cloned node and revocation of a compromised node through some probabilistic approaches is adopted [36].

However, these ways of detection and revocation of a node can't come handy in the context of networks of massive scales like the Internet of Things with multi-dimension heterogeneities in terms of the type of nodes, communication standards, network protocol, etc. Within the context of IoT, it is critical for the participating sensor motes to communicate securely with the Internet or other upper layers of the IoT [37], hence establishing a process of a secure channel between sensor motes and internet emerges as an essential requirement in any secure communication framework for IoT eco-system. The development of the secure data transmission channel between the motes and gateways in IoT needs to handle various challenges including how to manage the differences in communication protocol between sensors and IoT gateways as it opposes the faster transmission process among these two different subnets [38]. Further, the sensors can directly interact with the internet gateway; so, it will pose a potential threat to the gateway/TCP/IP overlay based communication in IoT. The existing internet-based security protocols are less supportable owing to limited resource availability and

restricted computational capability available in sensor motes. These conventional protocols will cause overhead and thus offer a significant trade-off between security requirement and resource utilization among sensor network and IoT [39].

The optimal process of secure communication among motes and IoT gateway only covers up one layer of the security requirements. The requirement of a secure architecture of IoT remains incomplete without the existence of a robust authentication mechanism. Authentication, or verifying the genuineness of smart devices and establishing the trust for critical infrastructure, plays a vital role in the realization of the IoT [40], [41]. Moreover, devices in the IoT are frequently (i) resource-constrained, and (ii) deployed in unmonitored, physically unsecured environments. Securing these devices requires tractable cryptographic protocols, as well as cost effective tamper resistance solutions along with handling the challenges and problems which are identified in this study as: 1) developing a scheme or modelling of authentication for global IoT (till date the authentication is primarily limited to only local IoT). 2) Existing research work towards security aspects of the system, network, and applications doesn't cover up all the security threats. 3) Existing authentication mechanism towards IoT security mainly doesn't support forward security or robust mutual authentication and access control. 4) Present cryptographic protocols used are just an enhanced version of the existing protocols, and hence they could overcome their legacy pitfalls. 5) Existing research work also emphasized incorporating a complex encryption mechanism with the usage of recursive orders [42].

In continuation, another essential requirement identified for the unified, secure framework of IoT is the optimization of key management. The various problems which are detected while the study of the related literature to this research includes that 1) Occurrences of optimization techniques towards security measures are sporadic to be found on research work in route for IoT frameworks. 2) The existing secure communication protocols don't scale to massive pool IoT devices with resource constraints. 3) Current techniques of trusted key management don't offer any form of enhanced security for exponentially increasing threats over IoT [39], [43].

4. Recommended solutions

The anticipated contribution/novelty of the proposed study are as follows:

- Framework for Secure Transmission between Sensor & IoT: A very simple framework that relates the bridge of transmission between sensor and internet host by incorporating security transmission. The framework targets to accomplish maximum security standards, e.g. non-repudiation, integrity, privacy, etc. Use of heterogeneous security protocol on transmitting and receiving node is also new to be seen in the proposed study. The study will also support encryption in case of availability as well as non-availability of active internet host thereby supporting a highly flexible encryption scheme in IoT.
- Framework for Robust Authentication in IoT: This is the first time where a research-based framework will be presented to address the problem of integrating securely local and global IoT. The authentication protocol equally supports both forward and backward secrecy as well as it maintains a robust mutual authentication mechanism among any actors involved in the process of IoT. With the usage of lightweight ciphertext-based encryption, it is expected to obtain faster response time good enough to complete authentication while resisting any forms of lethal threats.
- Optimized Framework for enhancing key management in IoT: This part of the study will present a novel optimization towards secure authentication that targets to create a secure communication pipeline among users and highly distributed cloud clusters to offer secure service delivery. The complete optimization will be carried out towards enhancing the existing key management system in IoT.

The application framework of IoT comprises of devices that are highly heterogeneous and compute migrations from sensor to IoT gateways to edge/fog computing to the cloud and then back to the client along with various alarming components. As observed from the review work, providing security for such networks is in its young stage in the form of an integrated architecture offering perfect security together with network and application possibilities although the shortcomings of IEFT and IEEE contribute more towards the same. Besides, the present researchers have not yet achieved the actual threshold of real-time performance potentials with respect to lesser computational complexity (less time and space complexity), usage of smaller key size, conformable security, lesser memory overheads, smaller ciphertext size, speedy processing time of algorithms (quicker response time), robust to possible threats and reduced communication/network overhead for ensuring a lighter security mechanism. Thus, the essential security challenges in IoT can be tackled with some of the recommended solutions given in this paper that are presented below:

4.1. Secure transmission between sensor & IoT

The basic principle behind this framework design is grounded on the effective supportability offered by public key cryptography to sensor nodes [44]. This section of the study takes into consideration that internet gateway (IoT) comprises of the receiver and sensor motes comprise of transmitters. Both of these have computational as well as architectural differences; therefore, two separate security protocols shall be devised, one primarily for the sensor nodes in WSN and another for internet gateway. The targeted data shall be captured by the transmitter (i.e. sensor node) and subjected to the process of ciphering using digital signature and encryption. This encrypted data shall then be sent to the internet host. Fig. 1 given below shows the schematic representation of this design.

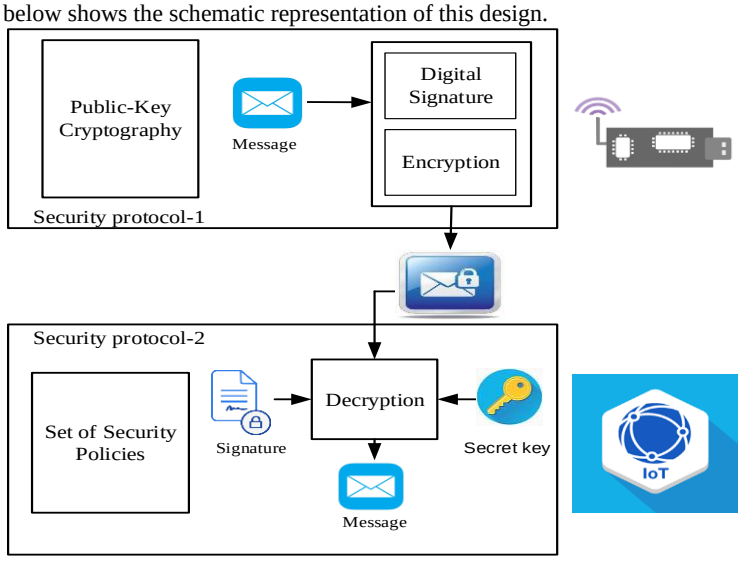


Fig. 1: A Tentative Schema for Secure Transmission between Sensor and IoT.

Two algorithms shall support the proposed framework; the first one shall involve the preliminary security parameter set employing unique public key cryptography. It formulates master key as well for computing the public key (master). After that, a process of key generation is performed for each security protocol. The first protocol shall select a particular attribute (to be scrutinized) for public key encryption which also computes the secret key whereas the second protocol shall comprise a collection of security policies and roles. Further, the secret key shall be computed in this protocol by random number selection performed by receiver nodes, i.e., sensor motes in IoT. To enhance the cryptosystem efficiency, this study shall implement encryption as well as a digital signature in one step

only, referred to as signcryption. For strengthening the protocol further, secure communication prospects need to be explored between various sensor nodes linked to IoT gateways directly or indirectly, i.e., whether or not the IoT gateway is the subsequent immediate host for some specific sensor mote. Lastly, decryption shall be performed taking into consideration the signature as well as a secret key.
The application of the recommended solution shall result in the following desired outcome:

- Lesser computational cost (low time and space complexity).
- Optimal key size.
- Higher security.
- Optimal ciphertext size.

4.2. Robust authentication in IoT

In this part of the study, secure modelling of global and local IoT is the prime concern. Global IoT signifies formation of a centralized network involving several diverse applications while local IoT signifies a network comprising only one application. Primarily, simple modelling is being performed for defining actors involved in global IoT (network associated with data centres) as well as in local IoT (target IoT, data centres, sensors). The research methodology tentatively being followed is displayed in Fig. 2.

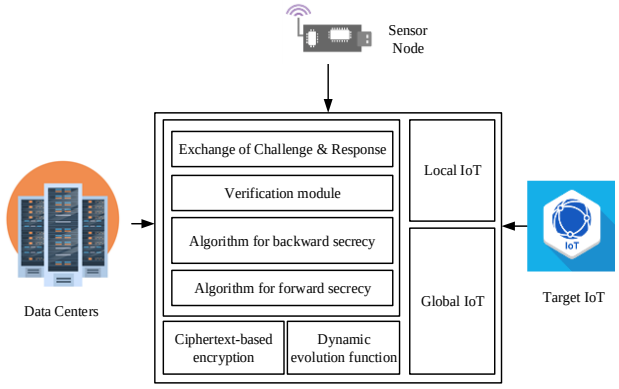


Fig. 2: Tentative Outline for Robust Authentication in IoT.

A challenge-response based strategy is being incorporated for designing a novel authentication scheme among actors residing inside global and local IoT domains. A highly sophisticated verification unit responsible for validating the requestor node's legitimacy will be developed. To maintain backward as well as forward secrecy in the presented authentication framework, two separate algorithms will be designed to offer protection against numerous probable threats. A unique dynamic evolution function and Ciphertext based encryption will be employed to improve the strength of the authentication technique further.
The solution will offer the following desired outcomes:

- Fast response time or fast algorithm processing time.
- Reduced communication operating costs.
- Access control through hierarchical means.

4.3. Enhancing key management in IoT

An extra actor in the form of an auxiliary node will be considered among users and cloud clusters in the proposed framework.
With the help of auxiliary authenticator node, the cloud cluster which is widely distributed and geographically spread offers the requested resources to the clients. The widely distributed cloud clusters and the multiple authenticators share a distinct secret key. The client will be expected to claim the secret key from the auxiliary node, which ultimately will offer the concerned client with a secret key along with a shared key identity. The information received by the client regarding the keys will be employed for the establishment of protected communication between user and cloud clusters. Tentative schematic illustration of the presented technique is shown in Fig. 3.

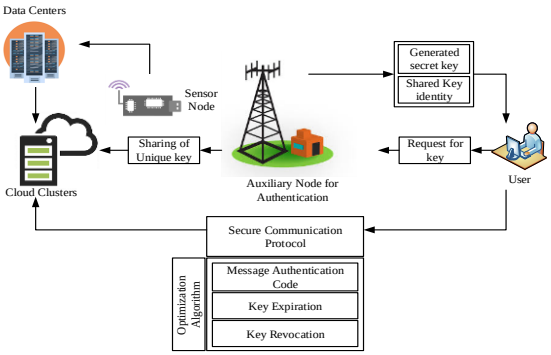


Fig. 3: Tentative Outline for Key Management Enhancement in IoT.

The design of the optimization algorithm will be based on the revocation information as well as on the key expiry specifications plus on the Message Authentication Code (MAC). The robust implementation of the proposed authentication amongst the diverse actors in the IoT based network will be achieved by utilizing the framework of previous phases.
Utilization of the said solution will offer the following desired outcome:

- Immune to numerous substantial attacks such as DOS, replay attacks, etc.
- Ability to scale well.
- Conforming with space and time complexities as well as able to bridge the computation and communication trade-off.

5. Conclusion

The research presented in this paper construed that the Internet of Things poses daunting challenges. Thus, compulsorily implementable security features should be incorporated in the primary IoT protocols, although those features expand the device potential. Moreover, key management automation is in itself a challenge, but it is more crucial for IoT protocols to avoid the dependence on pre-shared keys. The credentialing or registration of devices constitutes another major problem, and a well-understood pairing of protocols can be a prospective solution set to the same. Besides these issues, privacy may encourage the embracing of novel technologies which aim to prevent leakage of information in military/intelligence environments. To solve the problems found in IoT, three schematic frameworks have been suggested in this study.

Acknowledgement

This work was partially supported by the Ministry of Higher Education Malaysia (Kementerian Pendidikan Tinggi) under Research Initiative Grant Scheme (RIGS) number P-RIGS19-020-0020.

References

[1] Mukherjee S & Biswas GP (2018), Networking for IoT and applications using existing communication technology. Egyptian Informatics Journal 19(2), 107-127. https://doi.org/10.1016/j.eij.2017.11.002.
[2] Dorsemaine B, Gaulier JP, Wary JP, Kheir N & Urien P (2015), Internet of things: a definition & taxonomy. In Next Generation Mobile Applications, Services and Technologies, 2015 9th International Conference on, 72-77, IEEE. https://doi.org/10.1109/NGMAST.2015.71.
[3] Liu X & Baiocchi O (2016), A comparison of the definitions for smart sensors, smart objects and Things in IoT. In Information Technology, Electronics and Mobile Communication Conference (IEMCON), 2016 IEEE 7th Annual, 1-4, IEEE. https://doi.org/10.1109/IEMCON.2016.7746311.

[4] Voas J, Agresti B & Laplante P (2018), A closer look at IoT 's things. IT Professional 20(3), 11-14. https://doi.org/10.1109/MITP.2018.032501741

[5] Al Rabaiei KA & Harous S (2016), Internet of things: Applications and challenges. In Innovations in Information Technology (IIT), 2016 12th International Conference on, 1-6, IEEE. https://doi.org/10.1109/INNOVATIONS.2016.7880054.

[6] Miorandi D, Sicari S, De Pellegrini F & Chlamtac I (2012), Internet of things: Vision, applications and research challenges. Ad hoc networks 10(7), 1497-1516. https://doi.org/10.1016/j.adhoc.2012.02.016.

[7] Bandyopadhyay D & Sen J (2011), Internet of things: Applications and challenges in technology and standardization. *Wireless Personal Communications* 58(1), 49-69. https://doi.org/10.1007/s11277-011-0288-5.

[8] Al-Fuqaha A, Guizani M, Mohammadi M, Aledhari M & Ayyash M (2015), Internet of things: A survey on enabling technologies, protocols, and applications. IEEE Communications Surveys & Tutorials. 17(4), 2347-2376. https://doi.org/10.1109/COMST.2015.2444095.

[9] Talavera JM, Tobón LE, Gómez JA, Culman MA, Aranda JM, Parra DT, Quiroz LA, Hoyos A & Garreta LE (2017), Review of IoT applications in agro-industrial and environmental fields. Computers and Electronics in Agriculture 142, 283-297. https://doi.org/10.1016/j.compag.2017.09.015.

[10] Weber RH (2010), Internet of Things–New security and privacy challenges. Computer law & security review 26(1), 23-30. https://doi.org/10.1016/j.clsr.2009.11.008.

[11] Roman R, Zhou J & Lopez J (2013), On the features and challenges of security and privacy in distributed internet of things. Computer Networks 57(10), 2266-2279. https://doi.org/10.1016/j.comnet.2012.12.018.

[12] Jing Q, Vasilakos AV, Wan J, Lu J & Qiu D (2014), Security of the Internet of Things: perspectives and challenges. Wireless Networks 20(8), 2481-2501. https://doi.org/10.1007/s11276-014-0761-7.

[13] Khan BUI, Baba AM, Olanrewaju RF, Lone SA & Zulkurnain NF (2015), SSM: Secure-Split-Merge data distribution in cloud infrastructure. In Open Systems (ICOS), 2015 IEEE Conference on, 40-45, IEEE. https://doi.org/10.1109/ICOS.2015.7377275.

[14] Khan BUI, Olanrewaju RF, Anwar F, Mir RN & Najeeb AR, A critical insight into the effectiveness of research methods evolved to secure IoT ecosystem. International Journal of Information and Computer Security, in press.

[15] Khan BUI, Olanrewaju RF & Habaebi MH (2013), Malicious behaviour of node and its significant security techniques in MANET-A review. Australian Journal of Basic and Applied Sciences 7(12), 286-293.

[16] Olanrewaju RF, Khan BUI, Mir RN & Shah A (2015), Behaviour visualization for malicious-attacker node collusion in MANET based on probabilistic approach. American Journal of Computer Science and Engineering 2(3), 10-19.

[17] Mir MS, Suhaimi B, Adam M, Khan BUI, Mattoo MMUI & Olanrewaju RF (2017), Critical security challenges in cloud computing environment: an appraisal. Journal of Theoretical & Applied Information Technology 95(10), 2234-2248.

[18] Flauzac O, Gonzalez C & Nolot F (2015), Original secure architecture for IoT based on SDN. In Protocol Engineering (ICPE) and International Conference on New Technologies of Distributed Systems (NTDS), 2015 International Conference on, 1-6, IEEE. https://doi.org/10.1109/NOTERE.2015.7293481.

[19] Li L (2012), Study on security architecture in the Internet of Things. In Measurement, Information and Control (MIC), 2012 International Conference on, vol. 1, 374-377, IEEE. https://doi.org/10.1109/MIC.2012.6273274.

[20] An Internet of Things Reference Architecture. Symantec. https://www.symantec.com/content/dam/symantec/docs/white-papers/iot-security-reference-architecture-en.pdf. 2016. Accessed October 8, 2018.

[21] Olanrewaju RF, Khan BUI, Baba A, Mir RN & Lone SA (2016), RFDA: Reliable framework for data administration based on split-merge policy. In SAI Computing Conference (SAI), 545-552, IEEE. https://doi.org/10.1109/SAI.2016.7556033.

[22] Olivier F, Carlos G & Florent N (2015), New security architecture for IoT network. Procedia Computer Science 52, 1028-1033. https://doi.org/10.1016/j.procs.2015.05.099.

[23] Qian J, Xu H & Li P (2016), A novel secure architecture for the Internet of Things. In Intelligent Networking and Collaborative Systems (INCoS), 2016 International Conference on, 398-401, IEEE. https://doi.org/10.1109/INCoS.2016.36.

[24] Zhao G, Si X, Wang J, Long X & Hu T (2011), A novel mutual authentication scheme for Internet of Things. In Modelling, Identification and Control (ICMIC), Proceedings of 2011 International Conference on, 563-566, IEEE. https://doi.org/10.1109/ICMIC.2011.5973767.

[25] Ye N, Zhu Y, Wang RC, Malekian R & Qiao-min L (2014), An efficient authentication and access control scheme for perception layer of internet of things. Applied Mathematics & Information Sciences 8(4), 1617-1624. https://doi.org/10.12785/amis/080416.

[26] Hu T, Wang J, Zhao G & Long X (2012), An improved mutual authentication and key update scheme for multi-hop relay in Internet of Things. In Industrial Electronics and Applications (ICIEA), 2012 7th IEEE Conference on, 1024-1029, IEEE. https://doi.org/10.1109/ICIEA.2012.6360873.

[27] Patel S, Patel DR & Navik AP (2016), Energy efficient integrated authentication and access control mechanisms for Internet of Things. In Internet of Things and Applications (IOTA), International Conference on, 304-309, IEEE. https://doi.org/10.1109/IOTA.2016.7562742.

[28] Ma H & Chen B (2016), An authentication protocol based on quantum key distribution using decoy-state method for heterogeneous IoT. Wireless Personal Communications 91(3), 1335-1344. https://doi.org/10.1007/s11277-016-3531-2.

[29] Barreto PS, Libert B, McCullagh N & Quisquater JJ (2005), Efficient and provably-secure identity-based signatures and signcryption from bilinear maps. In International Conference on the Theory and Application of Cryptology and Information Security, 515-532, Springer, Berlin, Heidelberg. https://doi.org/10.1007/11593447_28.

[30] Li CK, Yang G, Wong DS, Deng X & Chow SS (2010), An efficient signcryption scheme with key privacy and its extension to ring signcryption. Journal of Computer Security 18(3), 451-473. https://doi.org/10.3233/JCS-2009-0374.

[31] Sun Y & Li H (2010), Efficient signcryption between TPKC and IDPKC and its multi-receiver construction. Science China Information Sciences 53(3), 557-566. https://doi.org/10.1007/s11432-010-0061-5.

[32] Huang Q, Wong DS & Yang G (2011), Heterogeneous signcryption with key privacy. The Computer Journal 54(4), 525-536. https://doi.org/10.1093/comjnl/bxq095.

[33] Li F & Xiong P (2013), Practical secure communication for integrating wireless sensor networks into the internet of things. IEEE Sensors Journal 13(10), 3677-3684. https://doi.org/10.1109/JSEN.2013.2262271.

[34] Li F, Han Y & Jin C (2016), Practical signcryption for secure communication of wireless sensor networks. Wireless Personal Communications 89(4), 1391-1412. https://doi.org/10.1007/s11277-016-3327-4.

[35] Rahayu TM, Lee SG & Lee HJ (2014), Security analysis of secure data aggregation protocols in wireless sensor networks. In Advanced Communication Technology (ICACT), 2014 16th International Conference on, 471-474, IEEE. https://doi.org/10.1109/ICACT.2014.6779005.

[36] George N & Parani TK (2014), Detection of node clones in wireless sensor network using detection protocols. International Journal of Engineering Trends and Technology 8(6), 286-291. https://doi.org/10.14445/22315381/IJETT-V8P253.

[37] Sundaram BV, Ramnath M, Prasanth M & Sundaram V (2015), Encryption and hash based security in internet of things. In Signal Processing, Communication and Networking (ICSCN), 2015 3rd International Conference on, 1-6, IEEE. https://doi.org/10.1109/ICSCN.2015.7219926.

[38] Bellavista P, Cardone G, Corradi A & Foschini L (2013), Convergence of MANET and WSN in IoT urban scenarios. IEEE Sensors Journal 13(10), 3558-3567. https://doi.org/10.1109/JSEN.2013.2272099.

[39] Granjal J, Monteiro E & Silva JS (2015), Security for the internet of things: a survey of existing protocols and open research issues. IEEE Communications Surveys & Tutorials 17(3), 1294-1312. https://doi.org/10.1109/COMST.2015.2388550.

[40] Crossman MA & Liu H (2015), Study of authentication with IoT testbed. In Technologies for Homeland Security (HST), 2015 IEEE International Symposium on, 1-7, IEEE. https://doi.org/10.1109/THS.2015.7225303.

[41] Sharaf-Dabbagh Y & Saad W (2016), On the authentication of devices in the Internet of Things. In 2016 IEEE 17th International Symposium on, 1-3, IEEE. https://doi.org/10.1109/WoWMoM.2016.7523532.

[42] Ravindranath M. Why the Internet of Things Needs Different Encryption. Nextgov.com. https://www.nextgov.com/cybersecurity/2016/08/internet-things-needs-newer-lighter-cryptography/130946/. 2016. Accessed October 8, 2018.
[43] Raza S, Seitz L, Sitenkov D & Selander G (2016), S3K: scalable security with symmetric keys—DTLS key establishment for the Internet of things. IEEE Transactions on Automation Science and Engineering 13(3), 1270-1280. http://dx.doi.org/10.1109/TASE.2015.2511301.
[44] Nadir I, Zegeye WK, Moazzami F & Astatke Y (2016), Establishing symmetric pairwise-keys using public-key cryptography in Wireless Sensor Networks (WSN). In Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON), IEEE Annual, 1-6, IEEE. https://doi.org/10.1109/UEMCON.2016.7777838.