Internet of Things and Cloud Computing
2019; 7(3): 80-87
http://www.sciencepublishinggroup.com/j/iotcc
doi: 10.11648/j.iotcc.20190703.14
ISSN: 2376-7715 (Print); ISSN: 2376-7731 (Online)

SciencePG
Science Publishing Group

Letter

Security Review in Internet of Things

Farhan Ali[1, *], Muhammad Sulaiman Khan[2], Hassan Akhtar[3]

[1]School of Electrical Engineering and Automation, Hefei University of Technology, Hefei, P. R. China

[2]Department of Computer Science and Information Technology, Hefei University of Technology, Hefei, P. R. China

[3]Wateen Telecom, Lahore, Pakistan

Email address:
farhan.ali9566@gmail.com (F. Ali)

[*]Corresponding author

To cite this article:
Farhan Ali, Muhammad Sulaiman Khan, Hassan Akhtar. Security Review in Internet of Things. *Internet of Things and Cloud Computing*. Vol. 7, No. 3, 2019, pp. 80-87. doi: 10.11648/j.iotcc.20190703.14

Received: September 7, 2019; **Accepted**: September 26, 2019; **Published**: October 16, 2019

Abstract: In this decade, the exceedingly rising state of the art industry is internet of things where trillion devices will be connected. IoT is being appraised to transform the concept of communication. To support this paradigm shift, companies and organizations are endowing worthwhile attention with researchers and scholars. Internet of thing is lending a hand with its essential role to build a new and smart world in a smarter way where everything will be under the umbrella of it. The internet of things enables an overwhelming smartness to help the humankind with various entities and diverse applications. Although, it is greatest achievement in this decade but some prevails are being engendered calamitous situations with subject to security concerns such as threats, vulnerabilities, attacks in internet of things with its connected and inter-connected devices and objects. Some hazards are critically perilous and alarming to internet of things such as physical attacks, network attack, encryption attacks, software attacks, authorization, surveillance, identity theft, vandalism, secure communication and so on. The most salient concern and important part on internet of things is secure architecture of internet of things. In near future with the connectivity of billion or trillion devices, it would be very difficult to resolve the security issues for impending generations. In this paper, we reviewed different security architecture of IoT and highlighted the absence of security layer in all models.

Keywords: Internet of Things, Architecture, Security

1. Introduction

The internet of things emerging industry paradigm clasps the pledge to remodel the communication concept with its estimated worth of trillion dollars, with the connectivity of billion devices and objects through its substantial virtual and physical infrastructure by which IoT is proclaiming to transfigure concept of communication such as smartphones, smart grids, video connectivity, video conferencing, GPS connectivity, vehicular connectivity, health devices and so on. In broad spectrum, transmitting and receiving data is tranquil in this era. According to Ericson internet of things has the connectivity of 5.7 million devices every day. In near future connectivity of IoT will be billion devices. So, the triumph and on growing curve of IoTs with bright future lean on its security. To support this revolution or paradigm shift, a layered architecture is required like OSI model to deal with its vulnerabilities. This contribution will pave the way to acquire a better security solution. We divided our contribution in sections: in Section II we described previous work in IoT's and in section III we delineated absence and importance of security layer in internet of things architecture. In section IV we discussed; conclusion and future discussion

2. Previous Work

The state of art emerging industry in this decade with its extra-ordinary growth and the impact on the people life with regime or paradigms shift industry is considered internet of things industry. Where, it is reshaping the modus operandi of people life and paths of communication, there, it is also gaining the credibility of changing the business concept. It is extremely entrancing fact that the emerging industry in this

decade is internet of things, from its start to up to 2019 every paper and every researcher who is paying great attention to internet of things has taken into account its layered architecture. In this section we analyzed the fact which is mentioned. So, we defined absence of security layer in architecture for IoT which might be imperative for upcoming generations. If we categorize the presented architecture proposed by different scholars [1-107] they proposed three layers, four layers, five layers and even some illustrated six layers but none of them added security layer as a separate layer as it is essentially required or needed. In every communication device through its virtual of substantial infrastructure either software/hardware even if we download or upload or install applications through network or sharing are with built in bugs and even, they collect or gather personal information and have access to device data. So, with the help of these paper and literature review, we come to this point that security layer is the most important layer in the architecture of internet of things which is missing from the architecture of internet of things.

3. Absence of Security Layer

Fact can be observed that there are different types of layers in IoT architecture [1-107] such as perception, things. middle wear. 6lowpan, data-link, internet, adaptation, transport, sensing, decision, support, action, link session, transmission, router, hub, cloud messaging, objected oriented, SOA layers and so on but these models do not define the security layer as an independent layer for internet of things. In the papers from [1-107], they stated different layers architectures and they disclosed different types of threats in IoT and also described their prospective solutions in that papers. But with the passage of time, as the internet of thing industry is going to be matured, threats are rapidly increasing day by day. In next decade, every device will be connected to internet. And IoT will gain credit of modernization to remodel the concept of communication. Due to these reasons, internet of things is transforming from internet of things to internet of everything. Where, the internet of things is enabling an overwhelming smartness to help the humankind with various entities and diverse applications there, threats are increasing besides these facts. Although, it is a magnificent procurement in this decade, regardless of all accomplishments, yet, some persuade are being provoked for devastating situations and conditions with subject to security concerns such as threats, vulnerabilities, attacks in internet of things with its connected and inter-connected devices and objects. Some pitfalls are critically periling and alarming to internet of things such as physical attacks, network attack, encryption attacks, software attacks, authorization, surveillance, identity theft, vandalism, secure communication and so on. The most pivotal concern and important part of internet of things is secure architecture. There are usually two types of hacker which gain access to system or network are considered as active attackers and passive attackers. Active attacks are frequently blatant and aggressive in which victims promptly become aware because of transmutation behavior of system, when they transpire. These are immensely malicious in nature, such as destroying memory or files, locking out users, or forcefully gaining access to a targeted network or system. Usually, hackers which avail oneself of active attacks are not much concerned with their activities being detected because by the time the attack is detected the damage is already over and done or is underway. Passive attacks frequently retain non-disruptive and conventional methods so that the hacker does not draw attention to the attack. The major aim of the passive attack is to attain access to user/system or network and to gather all data without detection. Many security breaches and data hacking are usually targeted data collections including the exposure of debit card and credit card payment information as well as personal data of user identifying information and legitimate access to confidential data

The attacker/ hacker takes unauthorized access to data, purloins the system data, rejigs the system, information (See Figure 1). Because of these facts, security infrastructures are becoming arduous issues for standardization. To overcome these challenges campiness, organizations and countries are paying fruitful attention such as Hydra, Runes, IoT-A, E Japan strategy, I-Core, Sensei, IoT-6, IoTivity, AllJoyn's. Fp7, horizon2020, one M2M platform, 4ward&sail, Fire++, Find, FIA, GENI and so on. Proliferation devices connectivity increase data collection of users which is not plain sailing to handle such as smart phones, tablets, laptop which brings with personal information like credit card, debit card, bank accounts, passwords, email account, business history, office information, contacts, controlled vehicle information and various others which are vulnerable to user and easily accessible, hacked and theft by hacker

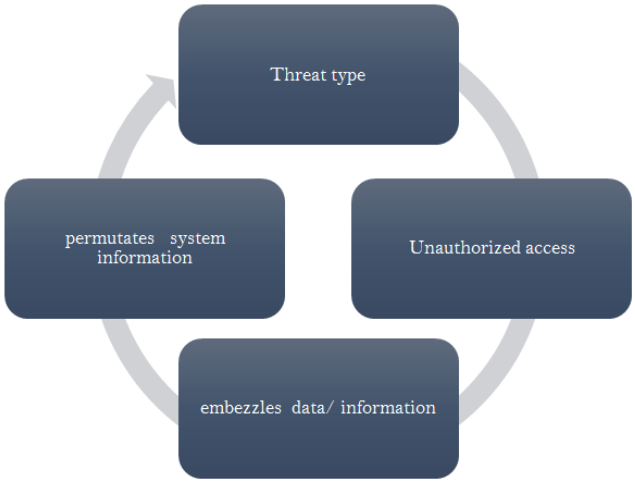


Figure 1. *Security breaches in IoTs.*

In past surveys almost more than 80 percent organizations have been affected with threats Either internal threats or external threats. Threats usually occurs due to lack of web interface, authentications, insecure networks, transport encryption, cloud interface, mobile interface, security configurations firmware security, physical security and so on. If we categorize the internal and external threats, internal

threats up to 60 percent while remaining threats are external Threats can be classified in two important branches, so it can be discussed as internal attacks and external attacks. Which are shown in Figure 2.

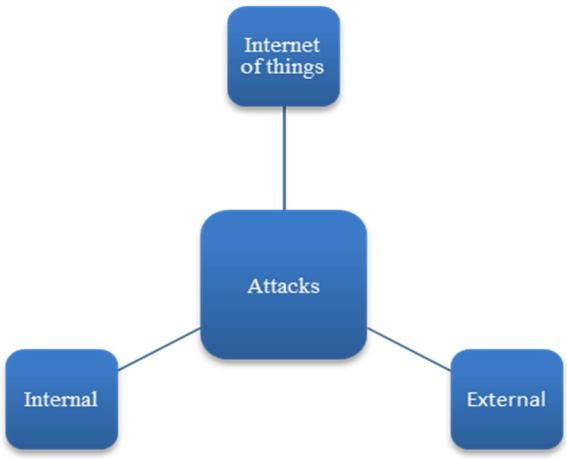
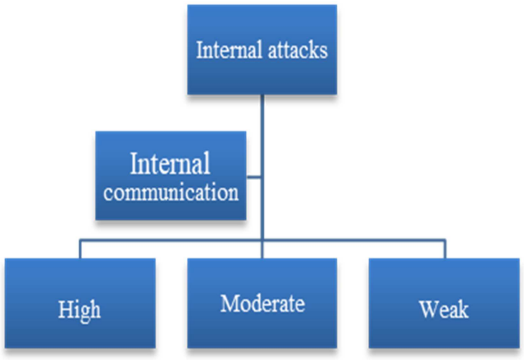
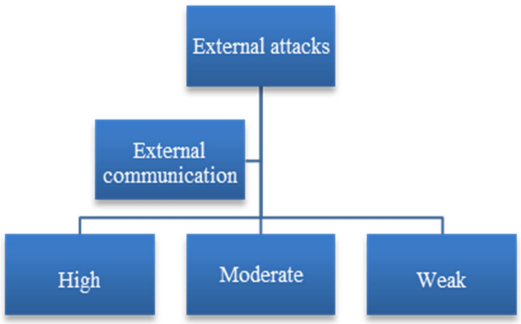


Figure 2. *Internet of things attacks classifications.*

Internal attacks explain the security of internal communications and data whereas, the external attacks define the external communication Furthermore, these attacks have further three more classifications. Weak Moderate and high which are described in Figure 3(a) and Figure 3(b). (See Figure 3 (a and b)



(a) description of internal attacks



(b) description of external attacks

Figure 3. *Description of internal attacks and external attacks.*

Weak threats usually attack to unclassified data, weak passwords, and less sensitive information with monitoring the system vulnerabilities. So, such types are happening on daily basis.

Moderate threats usually come about on classified data due to dearth of monitoring control because systems transfer considerable amount of sensitive data / information through network or over network with common user interface. These types of activities usually occur once in a weak or in or month.

High Threats commonly transpire on confidential and classified data/information with access upon private/ regulated data due to lack of security control on transmission. These types of attacks usually crop up on isolate systems once in a year or in 5 years. These types of attacks ratio are very less.

These types of attacks can be divided in to four major classes which can be described as physical, software, encryption and network. Physical attack executed nearby or short distance of device. Network attack is perpetrated on network layer to gambit on network for manipulation or damage of internet of things network and as well as hacking of passwords, data and larceny of information. Software attacks ensues when system when system contains vulnerabilities and proffers chance to hacker to enter system to harm. Encryption attacks usually transpire for breaking encryption [19]. Sensor attack happens on node/ gateways. These four attacks are major type of attacks which have their sub- classes to destroy the IoT network. Some important attacks are defined in table 1 (see Table 1) which have capability to lead the catastrophic conditions to the network (see Table 1).

Table 1. *Common Attacks in IoT [21, 29] - [32, 66-108] in internet of thing.*

Physical	Network	Software	Encryption
Sensor	Fake node	Side channel	Fragmented
Replication	Forged	Channel blocking	Impersonation
Tempering	Selfish	Wormholes	Selective forward
Timing	Node Capture	Sync	Software Bugs
Malicious	Routing	Dos	DDos
Cross heterogeneous Network	MAN, in Middle	Synbil	Sinkhole
Sleep deprivation	Spoofing	Eavesdropping	Insert
Privacy	Replay	Capture	Atmosphere
Power loss	Power disclosure	Noisy data	Node Tempering

As well as security concern is important, privacy part must also be included in that layer. There are three important privacy issues in IoTs which can be described as Trust management. Data protection and Vulnerabilities (see Figure 4) [110]. Privacy of the consumer and customers are very important because IoT is estimating with trillions of dollars industry in upcoming future with billions of the customer where more than half world will be dependent of IoTs or IoEs. In wireless communications it is absolutely provoking to list of challenges such as big data, data processing, data

management, efficient battery management system, communication infrastructure, technology infrastructure, immaturity, standards, procuring, privacy breaches and last but not least security risks. So, privacy and security challenges of internet of things are most important [111]. Some parameter must be defined such as integrity, confidentiality, authentication, data management and interoperability to attain secure and reliable communication. [73-78]

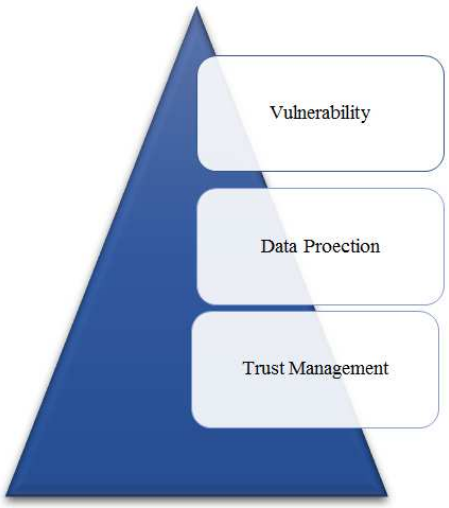


Figure 4. *Major privacy issues in IoTs.*

In Internet of things Network, Software and Encryptions attacks are most common attack are now a days. due to absence of the security layer, the attackers gain more chance to hack the data (the ratio of these have been described in Figure 5, (see Figure 5) So. with concerned of internet of things, there should be a standard model or a frame of reference model to protect the data and liabilities including with the security layer in IoTs because sooner or later it will be the part of internet of things With the maturity of internet of thing the attacks will perfoliate to the roof. So, a frame of reference model is essentially required with the addition of security layer.

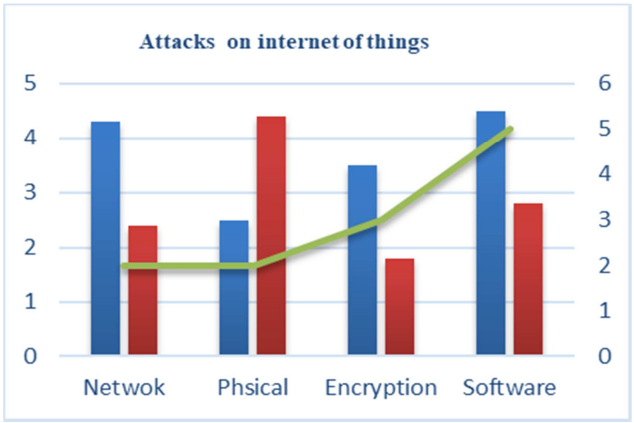


Figure 5. *Ratio of attacks in IoTs.*

It is true fact that great opportunities always come with great responsibilities such as internet of things are engendering unprecedented security problems such as Data security, network security, operating system security, server security, device/physical security, secure devices, authorization and authentication, devices updates managements, data confirmation,, communication security, data privacy, data integrity, high availability, data transmission safety, software updates, network size management, hardware security, lack of specialists, lack of a universal standard and so on.

4. Conclusion and Future Discussion

In this paper, we analyzed pervious published work by researchers, scholars and scientists where three, four, five and six layers are presented in IoT layered architecture but security layer is not included as independent layer in it. They did great work to secure IoTs but they did not add an independent security layer to make these models more and more secure. Because security layer independently can perform better and achieve great results to provide better security and secure communication Security layer must be including in this architecture as independent layer. In near future, with the maturity of IoTs, there will be massive escalation in connectivity of devices, Number of threats or attacks will be rapidly increased. So, it will be very difficult to manage security issues of IoTs. So, more work is required to make a global standard architecture model for IoTs and also need to pay vital attention to include security layer as independent layers which is the essential part of it.

References

[1] A. GhaffarianHoseini, et al., The essence of future smart houses: From embeddingict to adapting to sustainability principles, Renewable SustainableEnergy Rev. 24 (1) (2013) 593–607.

[2] S. Greengard, Smart transportation networks drive gains, Commun. ACM58 (1) (2015) 25–27.

[3] G. Pan, et al., Trace analysis and mining for smart cities: issues, methods, andapplications, IEEE Commun. Mag. 121 (6) (2015) 120–126.

[4] M. Amin, W. Bruce, Toward a smart grid: power delivery for the 21st century, IEEE Power Energ. Mag. 3 (5) (2005) 34–41.

[5] D. X. Li, W. He, S. Li, Internet of things in industries: A survey, IEEE Trans. Ind. Inf. 10 (4) (2014) 2233–2243.

[6] J. Gubbi, et al., Internet of Things (iot): A vision, architectural elements, andfuture directions, Future Gener. Comput. Syst. 29 (7) (2013) 1645–1660.

[7] Z. Liu, K-K. R. Choo, M. Zhao, Practical-oriented protocols forprivacy-preserving outsourced big data analysis: Challenges and future research directions, Comput. Secur. 69 (2017) 97–113.

[8] A. L. L. Atzori, G. Morabito, The internet of things: A survey, Comput. Netw. 54 (15) (2010) 2787–2805.

[9] Lan Li, "Study on security architecture in the Internet of Things," Proceedings of 2012 International Conference on Measurement, Information and Control, Harbin, 2012, pp. 374-377. doi: 10.1109/MIC.2012.627327.

[10] Alberto M. C. Souza, Joseé R. A. Amazonas, An Outlier Detect Algorithm using Big Data Processing and Internet of Things Architecture, Procedia Computer Science, Volume 52, 2015, Pages 1010-1015, ISSN1877-0509, https://doi.org/10.1016/j.procs.2015.05.095.

[11] S. Vashi, J. Ram, J. Modi, S. Verma and C. Prakash, "Internet of Things (IoT): A vision, architectural elements, and security issues," 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), Palladam, 2017, pp. 492-496. doi: 10.1109/I-SMAC.2017.8058399.

[12] Kanagavelu R., Aung K. M. M. (2019) A Survey on SDN BasedSecurity in Internet of Things. In: Arai K., Kapoor S., Bhatia R. (eds) Advances in Information and Communication Networks. FICC 2018. Advances in Intelligent Systems and Computing, vol 887. Springer, Cham.

[13] XML-Based Structural Representing Method for Information of Things in Internet of Things GuiPing Dai1 and Yong Wang2 DOI 10.1007/978-3-642-30126-1 Springer Heidelberg New York Dordrecht London.

[14] Shimin Yang, Xiangming Wen, Wei Zheng and Zhaoming Lu, "Convergence architecture of Internet of Things and 3GPP LTE-A network based on IMS," 2011 Global Mobile Congress, Shanghai, 2011, pp. 1-7. doi: 10.1109/GMC.\2011.6103911.

[15] Lee, S. K., Bae, M., & Kim, H. (2017). Future of IoT networks: A survey. Applied Sciences (Switzerland), 7 (10), doi.org/10.3390/app7101072.

[16] V. Tyagi and A. Kumar, "Internet of Things and social networks: A survey," *2017 International Conference on Computing, Communication and Automation (ICCCA)*, Greater Noida, 2017, pp. 1268-1270. doi: 10.1109/CCAA.2017.8230013.

[17] P. V. Paul and R. Saraswathi, "The Internet of Things — A comprehe nsive survey,"2017InternationalConference on Computation of Power, EnergyInformationandCommuincation (ICCPEIC), Melmaruvathur, 2017, pp. 421-426. doi: 10.1109/ICCPEIC.2017.8290405.

[18] Miloslays, N. & Tolstoy, A Cluster Comput (2019) 22: 103 http//doi.org/10.1007/s10586-018-2823-6.

[19] H. Derhamy, J. Eliasson, J. Delsing and P. Priller, "A survey of commercial frameworks for the Internet of Things," *2015 IEEE 20th Conference on Emerging Technologies & Factory Automation (ETFA)*, Luxembourg, 2015, pp. 1-8. doi: 10.1109/ETFA.2015.7301661.

[20] S. Kraijak and P. Tuwanut, "A survey on internet of things architecture, protocols, possible applications, security, privacy, real-world implementation and future trends," *2015 IEEE 16th International Conference on Communication Technology (ICCT)*, Hangzhou, 2015, pp. 26-31. doi: 10.1109/ICCT.2015.7399787.

[21] U. Banerjee, C. Juvekar, S. H. Fuller and A. P. Chandrakasan, "eeDTLS: Energy-Efficient Datagram Transport Layer Security for the Internet of Things," *GLOBECOM 2017 - 2017 IEEE Global Communications Conference*, Singapore, 2017, pp. 1-6. doi: 10.1109/GLOCOM.2017.8255053.

[22] Alberto M. C. Souza, Joseé R. A. Amazonas, An Outlier Detect Algorithm using Big Data Processing and Internet of Things Architecture, Procedia Computer Science, Volume 52, 2015, Pages 1010-1015, ISSN 1877 0509, doi.org/10.1016/j.procs.2015.05.095.

[23] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari and M. Ayyash, "Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications," in *IEEE Comlamunications Surveys & Tutorials*, vol. 17, no. 4, pp. 2347-2376, Fourthquarter2015. doi: 10.1109/COMST.2015.2444095.

[24] Z. Yang, Y. Yue, Y. Yang, Y. Peng, X. Wang, and W. Liu, "Study and application on the architecture and key —— technologies for IOT," in Multimedia Technology (ICMT), 2011 International Conference on, 2011, pp. 747–751.

[25] L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A survey," Comput. Networks, vol. 54, no. 15, pp. 2787–2805, 2010.

[26] R. Khan, S. U. Khan, R. Zaheer, and S. Khan, "Future internet: the internet of things architecture, possible applications and key challenges," in Frontiers of Information Technology (FIT), 2012 10th International Conference on, 2012, pp. 257–260.

[27] L. Nastase, "Security in the Internet of Things: A Survey on Application Layer Protocols," *2017 21st International Conference on Control Systems and Computer Science (CSCS)*, Bucharest, 2017, pp. 659-666. doi: 10.1109/CSCS.2017.101.

[28] S. Deshmukh and S. S. Sonavane, "Security protocols for Internet of Things: A survey," *2017 International Conference on Nextgen Electronic Technologies: Silicon to Software (ICNETS2)*, Chennai, 2017, pp. 71-74. doi: 10.1109/ICNETS2.2017.8067900.

[29] I. Andrea, C. Chrysostomou, G. Hadjichristofi, "Internet of Things: Security vulnerabilities and challenges", Proc. IEEE Symp. Comput. Commun. (ISCC), pp. 180-187, Jul. 2015.

[30] Y. Yang, L. Wu, G. Yin, L. Li and H. Zhao, "A Survey on Security and Privacy Issues in Internet-of-Things," in IEEE Internet of Things Journal, vol. 4, no. 5, pp. 1250-1258, Oct. 2017. doi: 10.1109/JIOT.2017.2694844.

[31] M. Amadeo et al., "Information-centric networking for the internet of things: challenges and opportunities," in IEEE Network, vol. 30, no. 2, pp. 92-100, March-pril2016. doi: 10.1109/MNET.2016.7437030.

[32] K. Sha, W. Wei, A. Yang, W. Shi, Security in internet of things: Opportunitiesand challenges, in: Proceedings of International Conference on Identification, Information & Knowledge in the Internet of Things (IIKI 2016), 2016.

[33] C. Lin, G. Wu, Enhancing the attacking efficiency of the node capture attackin wsn: a matrix approach, J. Supercomput. 66 (2) (2013) 989–1007.

[34] I. Rouf, et al., Neighborhood watch: security and privacy analysis of automaticmeter reading systems, in: Proceedings of the 2012 ACM Conference onComputer and Communications Security, 2012.

[35] X. Pan, Z. Ling, A. Pingley, W. Yu, K. Ren, N. Zhang, X. Fu, How privacy leaksfrom bluetooth mouse? IEEE Trans. Dependable Secure Comput. (TDSC) 13 (4) (2016) 461–473.

[36] A. Molina-Markham, et al., Private memoirs of a smart meter, in: Proceedingsof the Second ACM Workshop on Embedded Sensing Systems for Energy-Efficiency in Buildings, 2010.

[37] J. Lin, W. Yu, X. Yang, On false data injection attack against multistep electricityprice in electricity market in smart grid, IEEE Trans. Parallel Distrib. Syst. (TPDS) 27 (1) (2016) 286–302.

[38] Q. Yang, J. Yang, W. Yu, D. An, N. Zhang, W. Zhao, On false data-injectionattacks against power system state estimation: Modeling and countermeasures, IEEE Trans. Parallel Distrib. Syst. (TPDS) 25 (3) (2014) 717–729.

[39] X. Yang, J. Lin, W. Yu, P. Moulema, X. Fu, W. Zhao, A novel en-route filteringscheme against false data injection attacks in cyber-physical networkedsystems, IEEE Trans. Comput. (TC) 64 (1) (2015) 4–18.

[40] Q. Yang, D. An, R. Min, W. Yu, X. Yang, W. Zhao, On optimal pmu placementbaseddefense against data integrity attacks in smart grid, IEEE Trans. Inf. Forensics Secur. 12 (7) (2017) 1735–1750.

[41] X. Zhang, X. Yang, J. Lin, G. Xu, W. Yu, On data integrity attacks against realtime pricing in energy-based cyber-physical systems, IEEE Trans. Parallel Distrib. Syst. (TPDS) 28 (1) (2017) 170–187.

[42] Y. Chahid, M. Benabdellah and A. Azizi, "Internet of things security," 2017 International Conference on Wireless Technologies, Embedded and Intelligent Systems (WITS), Fez, 2017, pp. 1-6. doi: 10.1109/WITS.2017.7934655.

[43] Z. Ling, J. Luo, Y. Xu, C. Gao, K. Wu, X. Fu, Security vulnerabilities of internetof things: A case study of the smart plug system, IIEEE Int.-of-Things (IoT) J. pp (99) (2017) 1–1.

[44] C. D'Orazio, K.-K. R. Choo, L. T. Yang, Data exfiltration from internet of thingsdevices: ios devices as case studies, IEEE Internet Things J. 4 (1) (2017) 524–535.

[45] C. D'Orazio, K.-K. R. Choo, A technique to circumvent ssl/tls validations on iosdevices, Future Gener. Comput. Syst. 74 (2017) 366–374.

[46] C. J. D'Orazio, R. Lu, K.-K. R. Choo, A. V. Vasilakos, A Markov adversary modelto detect vulnerable ios devices and vulnerabilities in ios apps, Appl. Math. Comput. 293 (2017) 523–544.

[47] C. D'Orazio, K.-K. R. Choo, Circumventing ios security mechanisms for aptforensic investigations: A security taxonomy for cloud apps, Future Gener. Comput. Syst. 79 (2018) 247–261.

[48] Q. Do, B. Martini, K.-K. R. Choo, Is the data on your wearable device secure?An Android Wear smartwatch case study, Softw. Pract. Exper. 47 (3) (2017) 391–403.

[49] Q. Do, B. Martini, K.-K. R. Choo, A data exfiltration and remote exploitationattack on consumer 3d printers, IEEE Trans. Inf. Forensics Secur. 11 (10) (2016) 2174–2186.

[50] Q. Do, B. Martini, K.-K. R. Choo, Exfiltrating data from android devices, Comput. Secur. 48 (2015) 74–91.

[51] H. J, G. W. B, C. K.-K. R, Medical device vulnerability mitigation effort gapanalysis taxonomy, Smart Health (2018). http://dx.doi.org/10.1016/j.smhl.2017.12.001.

[52] A. Anjum, et al., An efficient privacy mechanism for electronic healthrecords, Comput. Secur. 72 (2018) 196–211.

[53] V. Casola, A. Castiglione, K.-K. R. Choo, C. Esposito, Healthcare-related data inthe cloud: challenges and opportunities, IEEE Cloud Comput. 3 (6) (2016) 10–14.

[54] Z. K. Zhang, M. C. Y. Cho, C. W. Wang, C. W. Hsu, C. K. Chen, S. Shieh, "Iot security: Ongoing challenges and research opportunities", 2014 IEEE 7th International Conference on Service-Oriented Computing and Applications, pp. 230-234, Nov 2014.

[55] R. Putthacharoen and P. Bunyatnoparat, "Protecting cookies from Cross Site Script attacks using Dynamic Cookies Rewriting technique," 13th International Conference on Advanced Communication Technology (ICACT2011), Seoul, 2011, pp. 1090-1094.

[56] H. Takahashi, K. Yasunaga, M. Mambo, K. Kim and H. Y. Youm, "Preventing Abuse of Cookies Stolen by XSS," 2013 Eighth Asia Joint Conference on Information Security, Seoul, 2013, pp. 85-89. doi: 10.1109/ASIAJCIS.2013.20.

[57] A. Aladeokin, P. Zavarsky and N. Memon, "Analysis and compliance evaluation of cookies-setting websites with privacy protection laws," 2017 Twelfth International Conference on Digital Information Management (ICDIM), Fukuoka, 2017, pp. 121-126. doi: 10.1109/ICDIM.2017.8244646.

[58] A. Juels, M. Jakobsson and T. N. Jagatic, "Cache cookies for browser authentication," 2006 IEEE Symposium on Security and Privacy (S&P'06), Berkeley/Oakland, CA, 2006, pp. 5 pp.-305. doi: 10.1109/SP.2006.8.

[59] M. Casado, P. Cao, A. Akella and N. Provos, "Flow-Cookies: Using Bandwidth Amplification to Defend Against DDoS Flooding Attacks," 200614th IEEE International Workshop on Quality of Service, New Haven, CT, 2006, pp. 286-287. doi: 10.1109/IWQOS.2006.250484.

[60] C. Smith and A. Matrawy, "Comparison of operating system implementations of SYN flood defenses (Cookies)," 2008 24th Biennial Symposium on Communications, Kingston, ON, 2008, pp. 243-246. doi: 10.1109/BSC.2008.4563248.

[61] P. Paul et al., "Using Browser Cookies for Event Monitoring and User Verification of an Account," 2018 IEEE 9th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON), Vancouver, BC, 2018, pp. 455-460. doi: 10.1109/IEMCON.2018.8615105.

[62] K. Nirmal, B. Janet and R. Kumar, "It's More Than Stealing Cookies-Exploitability of XSS," 2018 Second International Conference on Intelligent Computing and Control Systems (ICICCS), Madurai, India, 2018, pp. 490-493. doi: 10.1109/ICCONS.2018.8663230.

[63] M. Conti, A. Gangwal, S. P. Gochhayat and G. Tolomei, "Spot the Difference: Your Bucket is Leaking: A Novel Methodology to Expose A/B Testing Effortlessly," 2018 IEEE Conference on Communications and Network Security (CNS), Beijing, 2018, pp. 1-7. doi: 10.1109/CNS.2018.8433122.

[64] YU Ping. Privacy Security in Mobile RFID Networks. Journal of Chong qing College of Electronic Engineering. 2010 (19) 91-92.

[65] X. Xingmei, Z. Jing and W. He, "Research on the basic characteristics, the key technologies, the network architecture and security problems of the Internet of things," Proceedings of 2013 3rd International Conference on Computer Science and Network Technology, Dalian, 2013, pp. 825-828. doi: 10.1109/ICCSNT.2013.6967233.

[66] S. A. Hinai and A. V. Singh, "Internet of things: Architecture, security challenges and solutions," 2017 International Conference on Infocom Technologies and Unmanned Systems (Trends and Future Directions) (ICTUS), Dubai, 2017, pp. 1-4. doi: 10.1109/ICTUS.2017.8286004.

[67] T. Kothmayr, C. Schmitt, W. Hu, M. Brünig and G. Carle, "A DTLS based end-to-end security architecture for the Internet of Things with two-way authentication," 37th Annual IEEE Conference on Local Computer Networks - Workshops, Clearwater, FL, 2012, pp. 956-963. doi: 10.1109/LCNW.2012.642408.

[68] N. W. Bergmann and P. J. Robinson, "Server-based Internet of Things Architecture," 2012 IEEE Consumer Communications and Networking Conference (CCNC), Las Vegas, NV, 2012, pp. 360-361. doi: 10.1109/CCNC.2012.6181122.

[69] H. F. Sun et al., "A Security Scheme Research of the Internet of Things Based on the SA/NIA Architecture", Advanced Materials Research, Vol. 320, pp. 291-296, 2011.

[70] Isha, Luhach A. K., Kumar S. (2016) Layer Based Security in Internet of Things: Current Mechanisms, Prospective Attacks, and Future Orientation. In: Unal A., Nayak M., Mishra D., Singh D., Joshi A. (eds) Smart Trends in Information Technology and Computer Communications. SmartCom 2016. Communications in Computer and Information Science, vol 628. Springer, Singapore.

[71] Farooq, M. U., Waseem, M.: A critical analysis on the security concerns of internet of things (IoT). Int. J. Comput. Appl. III (7), 1-6 (2015).

[72] R. Roman, P. Najera and J., Lopez, "Securing the internet of things" IEEE Computer, vol 44, pp. 51-58, 2011. http://doi.org/10.1109/MC.2011.291.

[73] Roman, R, Zhou, J., Lopez, J.: on the features and challenges of security and privacy in distributed Internet of Things, comput Netw, 57 (10), 2266-2279 (2013).

[74] Rodrigo Roman, Jianying Zhou, Javier Lopez, on the features and challenges of security and privacy in distributed internet of things, Computer Ntworks, Volume 57 issue 10, 2013 Pages 2266-2279, ISSN 1389-1286.

[75] K. Singh and D. D. Singh Tomar, "Architecture, Enabling Technologies, Security and Privacy, and Applications of Internet of Things: A Survey," 2018 2nd International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC) I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), 2018 2nd International Conference on, Palladam, India, 2018, pp. 642-646. doi: 10.1109/I-SMAC.2018.8653708.

[76] Zhang Qi, P. SilpaChaitanya, T. Sudhir, "Spoofing Attack Detection Wireless Networks using Advanced KNN", International Journal of Smart Device and Appliance, vol. 4, no. 1, pp. 1-8, 2016.

[77] Li H., Zhou X. (2011) Study on Security Architecture for Internet of Things. In: Zeng D. (eds) Applied Informatics and Communication. ICAIC 2011. Communications in Computer and Information Science, vol 224. Springer, Berlin, Heidelberg.

[78] P. Rughoobur and L. Nagowah, "A lightweight replay attack detection framework for battery depended IoT devices designed for healthcare," 2017 International Conference on Infocom Technologies and Unmanned Systems (Trends and Future Directions) (ICTUS), Dubai, 2017, pp. 811-817. doi: 10.1109/ICTUS.2017.8286118.

[79] M. Smache, N. E. Mrabet, J. Gilquijano, A. Tria, E. Riou and C. Gregory, "Modeling a node capture attack in a secure wireless sensor networks," 2016 IEEE 3rd World Forum on Internet of Things (WF-IoT), Reston, VA, 2016, pp. 188-193. doi: 10.1109/WF-IoT.2016.7845447.

[80] K. Zhao and L. Ge, "A Survey on the Internet of Things Security," 2013 Ninth International Conference on Computational Intelligence and Security, Leshan, 2013, pp. 663-667. doi: 10.1109/CIS.2013.145.

[81] Y. Zhang, W. Zou, X. Chen, C. Yang and J. Cao, "The Security for Power Internet of Things: Framework, Policies, and Countermeasures," 2014 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery, Shanghai, 2014, pp.139-142. doi: 10.1109/CyberC.2014.32.

[82] A. Perrig, J. Stankovic, D. Wagner, "Security in wireless sensor networks", Communications of the ACM, vol. 47, no. 6, pp. 53-57, 2004.

[83] I. Andrea, C. Chrysostomou and G. Hadjichristofi, "Internet of Things: Security vulnerabilities and challenges," 2015 IEEE Symposium on Computers and Communication (ISCC), Larnaca, 2015, pp. 180-187. doi: 10.1109/ISCC.2015.7405513.

[84] Bostami B., Ahmed M., Choudhury S. (2019) False Data Injection Attacks in Internet of Things. In: Al-Turjman F. (eds) Performability in Internet of Things. EAI/Springer Innovations in Communication and Computing. Springer, Cham.

[85] Xu H., Sgandurra D., Mayes K., Li P., Wang R. (2017) Analysing the Resilience of the Internet of Things Against Physical and Proximity Attacks. In: Wang G., Atiquzzaman M., Yan Z., Choo KK. (eds) Security, Privacy, and Anonymity in Computation, Communication, and Storage. SpaCCS 2017. Lecture Notes in Computer Science, vol 10658. Springer, Cham.

[86] Yaseen, Q., Aldwairi, M., Jararweh, Y. et al. Multimed Tools Appl (2018) 77: 18249. https://doi.org/10.1007/s11042-017-5288-3.

[87] Sahmi I., Mazri T., Hmina N. (2019) Security Study of Different Threats in Internet of Things. In: Ben Ahmed M., Boudhir A., Younes A. (eds) Innovations in Smart Cities Applications Edition 2. SCA 2018. Lecture Notes in Intelligent Transportation and Infrastructure. Springer, Cham.

[88] Al-Gburi A., Al-Hasnawi A., Lilien L. (2018) Differentiating Security from Privacy in Internet of Things: A Survey of Selected Threats and Controls. In: Daimi K. (eds) Computer and Network Security Essentials. Springer, Cham.

[89] Hu Q., Lv S., Shi Z., Sun L., Xiao L. (2017) Defense Against Advanced Persistent Threats with Expert System for Internet of Things. In: Ma L., Khreishah A., Zhang Y., Yan M. (eds) Wireless Algorithms, Systems, and Applications. WASA 2017. Lecture Notes in Computer Science, vol 10251. Springer, Cham.

[90] Elrawy, M., Awad, A. & Hamed, H. J Cloud Comp (2018) 7: 21. https://doi.org/10.1186/s13677-018-0123-6.

[91] Zaidan, A. A., Zaidan, B. B., Qahtan, M. Y. et al. Telecommun Syst (2018) 69: 1. https://doi.org/10.1007/s11235-018-0430-8.

[92] Alabady, S. A., Al-Turjman, F. & Din, S. Int J Parallel Prog (2018). https://doi.org/10.1007/s10766-018-0580-z.

[93] Ko, E., Kim, T. & Kim, H. J Ambient Intell Human Comput (2018) 9: 1167. https://doi.org/10.1007/s12652-017-0581-6.

[94] Ferreira, H. G. C. & de Sousa Junior, R. T. Cluster Comput (2017) 20: 651. https://doi.org/10.1007/s10586-017-0729-3.

[95] Yan, BN., Lee, TS. & Lee, TP. Scientometrics (2015) 105: 1285. https://doi.org/10.1007/s11192-015-1740-1.

[96] Mohab Aly, Foutse Khomh, Mohamed Haoues, Alejandro Quintero, Soumaya Yacout, Enforcing security in Internet of Things frameworks: A Systematic Literature Review, Internet of Things, Volume6, 2019, 100050, ISSN25426605, https://doi.org/10.1016/j.iot.2019.100050.

[97] N. N. Srinidhi, S. M. Dilip Kumar, K. R. Venugopal, Network optimizations in the Internet of Things: Areview, Engineering Science and Technology, an International Journal, Volume 22, Issue 1, 2019, Pages 1-21, ISSN 2215-0986.

[98] R. Tanuja, Y. Shruthi, S. Manjula, K. Venugopal, L. Patnaik, Token basedprivacy preserving access control in wireless sensor networks, inInternational Conference on Advanced Computing and Communications (ADCOM), 2015, pp. 45–50.

[99] S. Raza, L. Wallgren, T. Voigt, SVELTE: real-time intrusion detection in theinternet of things, Ad Hoc Networks 11 (8) (2013) 2661–2674.

[100] H. Perrey, M. Landsmann, O. Ugus, T. C. Schmidt, M. Wahlisch, TRAIL: topologyauthentication in RPL, arXiv (2016). preprint arXiv: 1312.0984.

[101] P. Pongle, G. Chavan, Real time intrusion and wormhole attack detection ininternet of things, Int. J. Comput. Appl. (9) (2015) 121.

[102] Q. M. Ashraf, M. H. Habaebi, G. R. Sinniah, J. Chebil, Broadcast BasedRegistration Technique for Heterogenous Nodes in the IoT., 2014.

[103] P. Kasinathan, C. Pastrone, M. A. Spirito, M. Vinkovits, Denial-of-servicedetection in 6lowpan based internet of things, in IEEE 9th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), 2013, pp. 600–607.

[104] D. Yin, L. Zhang and K. Yang, "A DDoS Attack Detection and Mitigation With Software-Defined Internet of Things Framework," in IEEEAccess, vol. 6, pp. 2469424705, 2018. doi: 10.1109/ACCESS.2018.2831284.

[105] G. Lessa dos Santos, V. T. Guimarães, G. da Cunha Rodrigues, L. Z. Granville and L. M. R. Tarouco, "A DTLS-based security architecture for the Internet of Things," *2015 IEEE Symposium on Computers and Communication (ISCC)*, Larnaca, 2015, pp. 809-815. doi: 10.1109/ISCC.2015.7405613.

[106] D. Singh, G. Tripathi and A. Jara, "Secure layers-based architecture for Internet of Things," *2015 IEEE 2nd World Forum on Internet of Things (WF-IoT)*, Milan, 2015, pp. 321-326. doi: 10.1109/WF-IoT.2015.7389074.

[107] J. Qian, H. Xu and P. Li, "A Novel Secure Architecture for the Internet of Things," *2016 International Conference on Intelligent Networking and Collaborative Systems (INCoS)*, Ostrawva, 2016, pp. 398-401. doi: 10.1109/INCoS.2016.36.

[108] Weizhe Zhang, Baosheng Qu, "Security Architecture of the Internet of Things Oriented to Perceptual Layer", *International Journal on Computer Consumer and Control (IJ3C)*, vol. 2, no. 2, 2013.

[109] Yuan Huang, Yigang He, Qiwu Luo, Luqiang Shi, and Yuting Wu, Channel Estimation in MIMO–OFDM Systems Based on a New Adaptive Greedy Algorithm, IEEE WIRELESS COMMUNICATIONS LETTERS, VOL. 8, NO. 1, FEBRUARY 2019 29-32.

[110] Farhan Ali and He Yigang. 2019. Spectrum for Next Generation Technologies. In *Proceedings of the 2019 8th International Conference on Software and Information Engineering* (ICSIE '19). ACM, New York, NY, USA, 188-191. DOI: https://doi.org/10.1145/3328833.3328884.

[111] Farhan Ali, He Yigang, and Ruan Yi, "A Novel Security Architecture of Internet of Things," *International Journal of Computer Theory and Engineering* vol. 11, no. 5, pp. 89-96, 2019. DOI: 10.7763/IJCTE.2019. V11.1249.