International Journal of Scientific Engineering and Science
Volume 3, Issue 10, pp. 42-47, 2019. ISSN (Online): 2456-7361

A Concise Survey on Evolving IoT Security Technologies

Samson Hansen Sackey[1], Samuel Nartey Kofie[1], Joseph Henry Anajemba[1], Godwin Kobby Gapko[1], Abdul Karim Armah[2]
[1]College of Internet of Things Engineering, Hohai University, 213022, China
[2]School of Managerial Engineering, Zhengzhou University, Zhengzhou, 450001, China

Abstract— *Due to the numerous IoT (Internet of Things) devices in existence, the need to interconnect every device to the internet is very necessary. However, as there is increase in connected devices, the concentration of the IoT structure needs to be strengthened. Hence, the need to discuss security technologies. Furthermore, we give an account of the IoT security challenges and open solutions recognized with respect to the IoT layered structure. In this paper, we explain a breakdown of evolving IoT security technologies for the Internet of Things.*

Keywords— *Internet of Things (IoT), IoT Structure, IoT Security, Wireless Sensor Networks.*

I. INTRODUCTION

The mode of which we relate with our neighboring environment has changed which is however an influence sparked by the forth coming of the internet [27]. A network of physical objects (vehicles, buildings, devices, and other things) that are embedded with software, electronics, sensors, and network connectivity to assemble and interchange data is mainly well-known to be the Internet of Objects [11]. Internet of Objects is as well acknowledged to be the Internet of Things (IoT). IoT was initially in existence before the millennium years [15]. Primarily, there is data transmission, self-regulation and safe communication in the IoT periphery which exist between real world devices and applications [2], [25], [26]. Even though this awareness is drawing attention, at last everything and everyone will sooner or later be linked [1]. The IoT still faces challenges when it comes to the development of diverse applications and services in super large network hierarchy, network scale diversity and large number of events generated [12],[13]. The experience of radio frequency identification (RFID) technology has massive control in the theory of internet of things, which is now broadly used for tracking objects, animals, and people. In fact, not limiting to sensing abilities and deployment controllability that are more challenging application setups required [3].

In IoT fundamentals, we foremost identify things by its distinctive address given to it. Information collected is then disseminated back to the data cloud through specific IoT devices. Communication fundamentals such as Wi-Fi, IEE 802.15.4, Bluetooth, Z-wave helps strengthen the transmission protocols in IoT [33]. IoT software exploits its hardware through microprocessors, system-on-chips, microcontrollers etc. for processing. The services in IoT includes Information Aggregation Services, Identity-related Services, Ubiquitous Services and Collaborative-Aware Services. The above services are very beneficial when considering IoT applications such as smart grid, smart building, smart healthcare, smart agriculture, smart city and smart home [16], [28], [29], [30], [31], [32]. Figure 1 shows the six fundamentals of IoT.

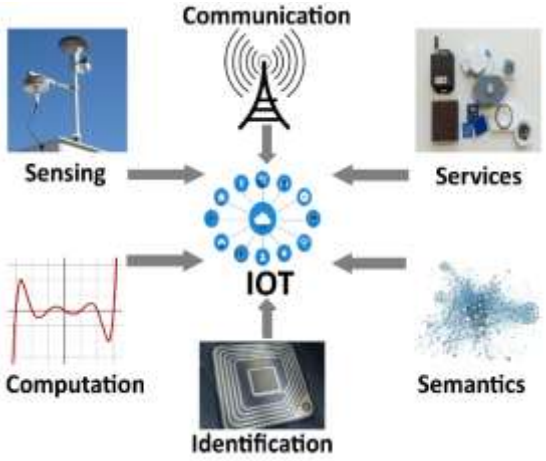

Fig. 1. The fundamentals of IoT

Almost every IoT devices is ought to be 100 percent insured for security complications. The three regions which provides IoT its secure mechanisms can be found in the trapezium in Fig. 2 below. Data availability originates when information demands to be dealt with by a user via smart devices and services. The user fails to retrieve information as a result of Denial of service (DoS) [39]. Therefore, prevention services for example firewalls fights to stop such risks from third users [19]. Data confidentiality ensures that new structures are put in place to avert unlawful users. Generally, when considering data encryption, it is the process whereby data is encrypted into a ciphertext. Two-step verification, it access data only and only if, it has passed authentication test which was provided by the IoT structure such as Biometric Verification [17]. Finally, data integrity is necessary because it protects user information from cybercriminals during IoT communication by securing end-to-end protection. In this case, data is impossible to be altered [18], [21].

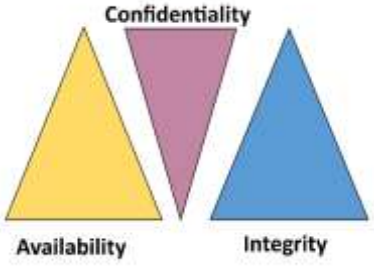

Fig. 2. IoT security ethics

In this context, smart households, industrial automation, Wireless Sensor Networks (WSNs), machine-to-machine (M2M) communications, and device-to-device (D2D) technologies, aided living, e-health, transportation, improved learning are only a few examples of possible application scenarios in which the new prototype will play a leading part in the near future [4],[14],[20], [22],[23]. The major enterprises in IoT are Amazon, AT&T, Cisco, Dell, GE Predix, Google, Hitachi Data systems, Microsoft, and Samsung Bosch. The contribution to this paper are as follows: (a) the inspiring wide variety of innovative IoT security technologies are discussed and (b) the basic challenges and solutions faced in IoT securities are indicated.

The remaining part of this paper is organized as follows. Section II describes briefly the structural interpretation of IoT. Section III forecasts possible evolving security technologies of IoT. Section IV describes key challenges and solutions in the applications of IoT security. Finally, Section V concludes the paper.

II. EVALUATION

The definition of IoT has been introduced several years ago from numerous different viewpoints and also from the large research community. For the obvious reason, the description of this type of configuration is rarely divided between two terms- The Internet and objects. Specifically, each layer comprises of protocols, devices, and modules that work effectively in converting data to information, and then to comprehensive analyses [45].

A. Device Layer:

The device layer which lies at the low part of the layer is also known as the perception layer. It is made up of devices like sensors, barcode readers, smart meters, Bluetooth, wearables, NFC (near-field communication), smartphones, low-power personal area networks, radio frequency identification (RFID), drones and others [5]. This layer is domineering because it represents the basis on which the outside world connects with.

B. Data Ingestion and Transformation Layer:

The Data ingestion and transformation layer is the central layer. However, the transformed data from the device layer goes via communication networks such as the internet, satellite, mobile networks, wireless network etc. are the few examples on which other practices establishes their standard [34]. This class of data can be obtained from sensors, wearables, actuators, connected machines, RFID, barcode, drones, GPS, smartphones, smart meters usually through wireless communications, wireless sensor networks which represents an indispensable part [10], [36]. The IEEE 802.15.4 protocol is observed to be very notable as it is the foundation for many WSN technologies [54].

C. Data Processing Layer:

Data compiled by the device layer which is preserved, analyzed and processed reaches this layer through the central layer [35]. The meaningful visualizations such as data retrieval and storage are few that provide the way forward for data management and decision support which are elementary tasks for this layer. Nonetheless, most data transformation analysis is carried out in real-time streaming analytics. Moreover, we can put to use some technologies for node localization, ticketing reporting, policy making, device provisioning, network communication, global maps and database intelligence which employs in usage of cloud computing and big data.

D. Applications Layer:

This layer lies on top of the IoT structure. It bridges the interval between the customers and the device layer. It also assists the customers access some restricted services [45], [46]. There are chains of intelligent applicative aims which ranges from transposition, employee safety, risk monitoring, fraud and warranty analytics, predictive analytic, and medical monitoring. These sort of reports can be applied in diverse fields such as logistics, healthcare, agriculture, buildings, retail, smart grid, oil mining and others.

Fig. 3. The IoT Structure by layers

III. EVOLVING SECURITY TECHNOLOGIES

The IoT can retrieve its security technologies in virtually every phase of our day-to-day natural life. Listed below are some identifiable standards [24].

Volume 3, Issue 10, pp. 42-47, 2019. ISSN (Online): 2456-7361

1. *IoT API Security:*

For efficient information flow within IoT devices, there is the need for authorization and authentication [38]. This is mostly done through recognized APIs which runs end-to-end within the devices. This (application programming interfaces) APIs allow authorized devices, developers and apps to communicate together, so that potential risks and attacks will be identified through such secured API. Few Wholesalers for the above involves Google, Muleosft, CA Technologies and Mashery.

2. *IoT Security and Risk Management:*

By the year 2025 and beyond, IoT devices will be able to sense forthcoming danger on their own. Therefore, events that fall outside the designed policy will be a failed trial. The number of false positive alerts can be reduced through highly developed predictive strategies. Canary Smart Security System combines video, audio, motion detection, night vision, temperature, a siren, air quality sensors into a piece of device that can be guarded from your phone. The emerging Artificial Intelligence (AI) is a momentous initiation in unification with the support of improved algorithms to overcome conventional attack strategies. Kaspersky, Cisco, and Senrio are Traders in such products.

3. *IoT Verification:*

Some kits are useful in verifying and monitoring millions of devices. IoT verification has been strengthen since the involvement of connected cars (multiple-users-single-device), biometrics, digital certificates and two-factor authentication. There are two ways by which authentication can be done, whether by entering credential or by the use of embedded IoT sensors for human identification [47]. The Piper in Figure 4(a) can be used for both security functions and home monitoring. The Retailers includes Device Authority, Gemalto, and Baimos Technologies.

4. *IoT Encoding:*

There are devices that check software updates, diagnostics, crash analysis, physical management, and security management. Data integrity arises when encrypted data is publicized back and forth the IoT system. It however utilities robust cryptographic techniques to prevent data hackers and etc. Cryptographic techniques includes Advanced Encryption Standard (for confidentiality), Diffie-hellman (for key agreement), Elliptic curve cryptography (for digital signatures key transportation) and SHA-256 (for integrality). Security could be breached if poor key management is considered instead of full encryption key lifecycle management processes. Entrust Datacard, Lynx Software Technologies, and Symantec are Merchants.

5. IoT Network Security

Technologies will be mandatory to protect and secure connected IoT devices. IoT network prevents intrusion and detects strong antivirus and antimalware solutions against obstructions such as denial-of-sleep attacks that deteriorates batteries. IoT devices make use of sophisticated security processors which increases complexity than traditional network securities practices. August smart lock routinely operates to unlock your household when you arrive or leave. Figure 4(e) supports the (Advanced Encryption Standard) AES-128 Security Module and Cisco Meraki MX64W (Figure 4(f)). Darktrace, Bayshore Networks, and Cisco are few suppliers of such services.

Fig. 4. Extended security based IoT Technologies

6. IoT PKI:

IoT devices make use of processors, certificates and designs to check whether they are capable to resist strong encryption and security to ensure actively enabled third party PKI software suites. It functions with other automated devices for security conservation through digital certificates by providing assistance for management, private key generation, invalidation and distribution. Public key Infrastructure (PKI) can sometimes be restricted by IoT devices due to the complicated hardware specifications it possesses. Vendors of such products includes WISekey, DigiCert, and Hewlett Packard Enterprise (HPE).

7. IoT Distribution:

Due to unexpected cyberattacks by hackers, the regular allocation of randomize IoT software and hardware updates is very substantial [38]. Such software are controlled by experts in this area. Sporadically, simplified patches are done to the software to restore critical gaps for high throughput. Cisco's Connected Factory encourages companies to incorporate IoT technologies in manufacturing industries for efficient monitoring of equipment.

8. IoT System Improvement:

If IoT security technologies are improved, the end-to-end network topology will be perceived to be a full active system. Security involves a robust design which should be in existence

permanently but it's difficult if there are built-in smart sensors. Most system designers face issues during the post-implementation phase. Furthermore, softwares and hardwares are taken into consideration in securing such systems. It should be obligatory that, together with authorized developers, devices, and applications, no other should be permitted for communication within these secured devices [50].

9. IoT Interface Preservation:

Low-level device control through APIs are handled by designers beyond communication systems (WiMAX), device monitoring (HTTP-CoAP proxy), security devices, and firmware modification. Maintaining these interfaces in order to successfully go beyond encryption, it must undergo thorough authorization and authentication.

The IoT technologies for security will constantly evolve with time but still faces numerous challenges and sufficient continuum for connecting huge number of tagged objects or sensors etc.

IV. Challenges and Solutions

The IoT has much impact in the internet world and therefore can be resourceful to the vast economic benefits that comes with it but it also expressions it challenging outcomes [9], [24], [55]. A few of them are concisely defined below.

1. *RFID Congestion:*

RFID is the oldest inspiring evolving technology which make use of radio waves frequency. Therefore, countless security flaws that strikes different systems also affects RFID technology too [51]. The damage brought about by RF congestion is similar to the involvement of communication between RFID tag and reader by adding noise signals. When RFID tags are unable to be identified, the Physical Unclonable Function (PUF) approach is used to recognize which chip is safe.

2. *Unapproved Tag Deactivating:*

RFID, 2D-barcodes, sensors, and Ultra High Frequency RFID reader are necessary for everyday identification and therefore the tags needs to contain data of a specific entry. Whenever RFID tags are deactivated, it is known as Denial-of-Service (DoS) attack where this tags are inaccessible from public space [39]. IoT systems that stand for integrity may be penetrated due to critical attacks. To countermeasure this problem, a combined distinctive identification service weighted in the cloud is applied. OAuth protocol regulators the series of authentication certification coming through the system [53].

3. *Security Attacks:*

Peer-to-peer connection constructs redundant isolated nodes that are simultaneous to each other [7]. Node distribution tends to superpose all other different distant computing portion. Security attacks in IoT causes high threat to independent systems linked with each other. Because of several IoT operations, intruders can cause damage to these devices i.e. we must avert these intruders from further undependable events [52]. IoT devices are guaranteed to customize symmetric encryption technologies to better its outcomes [37], [41], [42], [43], [44].

4. *Unauthorized Access:*

For that reason, preserving privacy should play a key role in the IoT architecture [8].Implemented APIs are cyclically taken advantage of by other users and makes it vulnerable to attacks during connection from the server. For preventing unauthorized access, recent approaches have been carried out which computes IoT effective placement strategy. However, security is coordinated through allowing different functions for diverse purposes in well-timed standard.

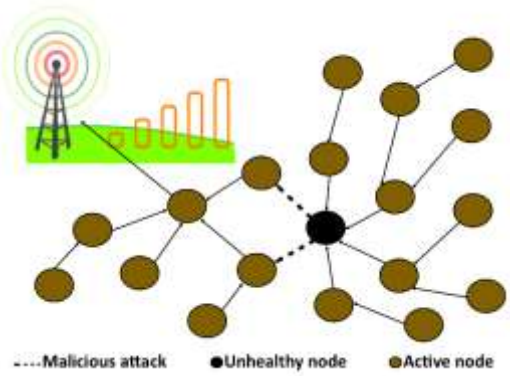

Fig. 5. The Network Topology Destruction

5. *Topology Destruction:*

Excessive advertisement of nodes in a connected network through high quality routing is a way attackers intrude. After full network connection is attained, data flows straight through the router which end up settling or departing [40]. Moreover, storage allocation is made for other data to be reserved in the data centers as well as the energy reserves. Figure 5 shows the network topology destruction. This situation is handled by directing all traffic and communication settings better for assessment.

6. *Sleep Deprivation Attack*:

Therefore, the deployment of sensors to a perilous area is very important in order to make acute decision in detecting malicious activities quickly. Nodes stay alive for stronger network connection through battery renewal in order to minimize power consumption. Sending redundant control traffic packets tends to exhaust the battery life of nodes.

7. *Sniffing Attack:*

A firm attacker gets into the IoT application devices by collecting information from the various layers in order to exploit the system. The attacker stays undetectable to be sensed for a long time and acquires all the delicate information. This encounter can be dominated by introducing Multilayer perception (MLP) which is a supervised Artificial Neural Network (ANN) set for categorizing threat preventive schemes especially for all forms of DDoS/DoS attacks.

8. *Cryptanalysis:*

The IoT will connect billions of objects to control flow of data and rejection of messages. With the backing of a cypher

text decoder, encrypted messages are retrieved by the attacker by using a set of encryption keys [41], [48], [49]. To secure RFID devices, integrated light weight authentication designs are applied, which are difficult to achieve by the use of cryptographic algorithms.

9. Botnets:

In adverse cases, devices in a network are relayed, otherwise, there may be complications such as malware to prevent the spread of accurate messages. IoT devices are taken control of if the botnet is realized in the network. A Distributed Denial-of-Service (DDOS) attack can be identified when an IoT device is affected.

V. CONCLUSIONS

This paper contributes widely concerning study on developing future IoT security technologies. Sensor devices function autonomously in making big advancements especially in safeguarding our environment. IoT security technologies exhibits threats challenges and potential solutions needed to be implemented. This security attacks creates huge problems within the whole network if measures are not set into order. The continuous increase in the interest of IoT innovations has seen several research being conducted. The present-day evolving things reviewed above are highly promising to influence the world for many years to come.

REFERENCES

[1] J. Zheng, D. Simplot-Ryl, C. Bisdikian, and H. Mouftah, "The Internet of Things," in *IEEE Communications Magazine, Volume: 49, Issue: 11, pp: 30-31*, 2011.
[2] T. Fan and Y. Chen, "A Scheme of Data Management in the Internet of Things," in *2nd IEEE International Conference on Network Infrastructure and Digital Content*, 2010.
[3] R. Khan, S.U. Khan, R. Zaheer, and S. Khan, "Future Internet: The Internet of Things Architecture, Possible Applications and Key Challenges," In *10th International Conference on Frontiers of Information Technology (FIT)*: Proceedings (pp. 257-260). *Institute of Electrical and Electronics Engineers Inc*., 2012.
[4] D. Bandyopadhyay and J. Sen, "Internet of Things: Applications and Challenges in Technology and Standardization," in *Wireless Peers Comm.* 58:49–69, 2011.
[5] S. H. Sackey, G. K. Gapko, S. N. Kofie, A. K. Armah, "Inspiring Evolving Technologies in Internet of Things", *Pacific International Journal*, vol. 2, no. 2, pp. 41-47, 2019.
[6] M. R. Palatella, N. Accettura, X. Vilajosana, T. Watteyne, L. A. Grieco, G. Boggia, and M. Dohler, "Standardized Protocol Stack for the Internet of (Important) Things", *IEEE Communications Surveys & Tutorials*, Vol. 15, No. 3, 3rd Quarter, 2013.
[7] Li B, Li Y. "Internet of things drives supply chain innovation: A research framework". *International Journal of Organizational Innovation*. 9(3):71-92, 2017.
[8] I. Andrea, C. Chrysostomou, G. Hadjichristofi, "Internet of Things: Security vulnerabilities and challenges", in: *Computers and Communication (ISCC), IEEE Symposium*, pp. 180-187, 2015.
[9] G. Gang, L. Zeyong, and J. Jun, "Internet of Things Security Analysis," in *International Conference on Internet Technology and Applications (iTAP)*, 2011.
[10] T. Winter, P. Thubert, A. Brandt, J. Hui, R. Kelsey, K. Pister, R. Struik, J. P. Vasseur, and R. Alexander, "RPL: IPv6 routing protocol for low-power and lossy networks", *RFC6550, IETF*, 2012.
[11] F. Ganz, D. Puschmann, P. Barnaghi, and F. Carrez, "A Practical Evaluation of Information Processing and Abstraction Techniques for the Internet of Things", *IEEE Internet Things J*. 2 340–354, 2012.
[12] M.A. Razzaque, M. Milojevic-Jevric, A. Palade, and S. Cla, "Middleware for internet of things: A survey", *IEEE Internet Things J*. 3 70–95, 2016.
[13] Y. Ai, M. Peng, and K. Zhang, "Edge cloud computing technologies for internet of things: A primer", *Digital Communications and Networks*, 2017.
[14] A. AI-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayysah, "Internet of Things: A Survey on Enabling Technologies, Protocols and Applications", *IEEE Communication Surveys and Tutorials* Vol. 17, No.4. pp. 2347-2376, Fourth Quarter, 2015.
[15] R. H. Weber, "Internet of Things–New security and privacy challenges," *Computer law & security review*, vol. 26, no. 1, pp. 23-30, 2010.
[16] A. Al-Fuqqaha, M. Mohammadi, "Internet of Things: A Survey on Enabling Technologies, Protocols and Applications", *IEEE Communication Surveys and Tutorials*, Vol. 17, No. 4,pp. 2347-2376, Fourth Quarter, 2015.
[17] D. Miorandi, S. Sicari, F. De Pellegrini and I. Chlamtac, "Internet of Things: Vision, applications and research challenges," *In: Ad Hoc Networks*, pp.1497-1516, 2012.
[18] R. Mahmoud et al., "Internet of things (IoT) security: Current status, challenges and prospective measures", *Internet Technology and Secured Transactions (ICITST), 10th International Conference IEEE*, 336-341, 2015.
[19] M. U. Farooq, M. Waseem, A. Khairi, S. Mazhar, "A critical analysis on the security concerns of internet of things (IoT)", *International Journal of Computer Applications*, 111(7), 2015.
[20] J. Wan, H. Yan, H. Suo, and F. Li, "Advances in Cyber-Physical Systems Research," *TIIS*, vol. 5, no. 11, pp. 1891-1908, 2011.
[21] M. Chen, J. Wan, and F. Li, "Machine-to-machine communications: Architectures, standards and applications," *Ksii trans. on internet & info. Systems*, vol. 6, no. 2, 2012.
[22] Y. C. Pranaya, M. Naga Himarish, M. Nisar Baig, and M. Riyaz Ahmed. "Cognitive Architecture based Smart Homes for Smart Cities", *International Conference on Trends in Electronics and Informatics*, 11-12, 2018.
[23] Pranaya, Y. C., Manne Naga Himarish, Mohammed Nisar Baig, and Mohammed Riyaz Ahmed. "Cognitive architecture based smart grids for smart cities." *In Power Generation Systems and Renewable Energy Technologies (PGSRET), 3rd Int. Conf. on*, pp. 44-49, 2017.
[24] Naik, Swapnil, and Vikas Maral. "Cyber security—IoT." *In Recent Trends in Electronics, Information & Communication Technology (RTEICT), 2nd IEEE International Conference on*, pp. 764-767, 2017.
[25] Vashi, Shivangi, Jyotsnamayee Ram, Janit Modi, Saurav Verma, and Chetana Prakash. "Internet of Things (IoT): A vision, architectural elements, and security issues." *In I-SMAC (IoT in Social, Mobile, Analytics and Cloud), (I-SMAC), International Conference on*, pp. 492-496, 2017
[26] Kaur, Navroop, and Sandeep K. Sood. "An energy-efficient architecture for the Internet of Things (IoT)." *IEEE Systems Journal vol. 11*, no. 2, pp. 796-805, 2017.
[27] J. Gubbi, R. Buyya, S. Marusic, M. Palaniswami, "Internet of Things (IoT): A vision, architectural elements, and future directions'', *Future Gener. Comput. Syst*., vol. 29, no.7, pp. 1645-1660, 2013.
[28] Al Rabaiei KA & Harous S, "Internet of things: Applications and challenges", *In Innovations in Information Technology (IIT), 12th International Conference on, 1-6, IEEE*, 2016.
[29] Bandyopadhyay D & Sen J., "Internet of things: Applications and challenges in technology and standardization", *Wireless Personal Communications* 58(1), 49-69, 2011.
[30] Miorandi D, Sicari S, De Pellegrini F & Chlamtac I, "Internet of things: Vision, applications and research challenges", *In Ad hoc net-works* 10(7), 1497-1516, 2012.
[31] X. Liu and O. Baiocchi, "A comparison of the definitions for smart sensors, smart objects and Things in IoT". *In Information Technology, Electronics and Mobile Comm. Conference (IEMCON), IEEE 7th Annual*, 1-4, 2016.
[32] Talavera JM, Tobón LE, Gómez JA, Culman MA, Aranda JM, Parra DT, Quiroz LA, Hoyos A & Garreta LE, "Review of IoT applications in agro-industrial and environmental fields", *Computers and Elec. in Agriculture*, vol. 142, 283-297, 2017
[33] M. James, C. Michael, B. Peter, W. Jonathan, D. Richard, B. Jacques, and A. Dan, "Unlocking the potential of the Internet of things", 2015.

[34] Darwish, Dina. "Improved Layered Architecture for Internet of Things." *International Journal of Computing Academic Research (IJCAR)* 4, no. 4: 214-223, 2015.
[35] Shen, Yulong, Tao Zhang, Yongzhi Wang, Hua Wang, and Xiao Hong Jiang. "MicroThings: A Generic IoT Architecture for Flexible Data Aggregation and Scalable Service Cooperation." *IEEE Communications Magazine* 55, no. 9, 86-93, 2017.
[36] Tsoukaneri, Galini, Massimo Condoluci, Toktam Mahmoodi, Mischa Dohler, and Mahesh K. Marina. "Group Communications in Narrowband-IoT: Architecture, Procedures, and Evaluation." *IEEE Internet of Things Journal*, 2018.
[37] R. Billure, V. M. Tayur and Mahesh V, "Internet of Things - a study on the security challenges," *IEEE International Advance Computing Conference (IACC)*, Banglore, pp. 247-252, 2015.
[38] Punia, Aanchal, Daya Gupta, and Shruti Jaiswal. "A perspective on available security techniques in IoT." *In Recent Trends in Electronics, Information & Communication Technology (RTEICT), 2nd IEEE International Conference on*, pp. 1553-1559, 2017.
[39] Deogirikar, Jyoti, and Amarsinh Vidhate. "Security attacks in IoT: A survey." *In I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (ISMAC), International Conference on*, pp. 32-37. IEEE, 2017.
[40] Pawar, Ankush B., and Shashikant Ghumbre. "A survey on IoT applications, security challenges and counter measures." *In Computing, Analytics and Security Trends (CAST), International Conference on*, pp. 294-299, 2016.
[41] Ahemd, Mian Muhammad, Munam Ali Shah, and Abdul Wahid. "IoT security: A layered approach for attacks & defenses." In *Communication Technologies (ComTech), International Conference on, pp. 104-110. IEEE*, 2017.
[42] E. Fernandes, A. Rahmati, K. Eykholt and A. Prakash, "Internet of Things Security Research: A Rehash of Old Ideas or New Intellectual Challenges?," *in IEEE Security & Privacy*, vol. 15, no. 4, pp. 79-84, 2017.
[43] K. Gupta and S. Shukla, "Internet of Things: Security challenges for next generation networks," *International Conference on Innovation and Challenges in Cyber Security (ICICCS-INBUSH), Noida*, pp. 315-318, 2016.
[44] M. M. Ahemd, M. A. Shah and A. Wahid, "IoT security: A layered approach for attacks & defenses," *International Conference on Communication Technologies (ComTech), Rawalpindi*, pp. 104-110, 2017.
[45] G. Yang, J. Xu, W. Chen, Z.-H. Qi, and H.-Y. Wang, "Security characteristic and technology in the internet of things," *Journal of Nanjing University of Posts and Telecommunications (Natural Nanjing University of Posts and Telecomm. (Natural*, vol. 30, no. 4, 2010.
[46] H. Suo, J. Wan, C. Zou, and J. Liu, "Security in the internet of things: a review," in *Computer Science and Electronics Engineering (ICCSEE), 2012 international conference on*, vol. 3, pp. 648-651, 2012.
[47] G. Misra, V. Kumar, A. Agarwal, and K. Agarwal, "Internet of Things (IoT)–A Technological Analysis and Survey on Vision, Concepts, Challenges, Innovation Directions, Technologies, and Applications (An Upcoming or Future Generation Computer Communication System Technology)," *American Journal of Electric and Electronic Engineering*, vol. 4, no. 1, pp. 23-32, 2016.
[48] Z. Hu, "The research of several key question of internet of things," in *Intelligence Science and Information Engineering (ISIE), International Conference on*, pp. 362-365: IEEE, 2011.
[49] P. Gaona-García, C. E. Montenegro-Marin, J. D. Prieto, and Y. V. Nieto, "Analysis of Security Mechanisms Based on Clusters IoT Environments," *Int'l Journal of Interactive Multimedia and Artificial Intelligence*, vol. 4, no. Special Issue on Advances and Applications in the Internet of Things and Cloud Computing, 2017.
[50] M. Langheinrich, "Privacy by design—principles of privacy-aware ubiquitous systems," in *International conference on Ubiquitous Computing*, pp. 273-291: Springer, 2001.
[51] D. C. Y. L. W. Meng, "Security Architecture and Key Technologies for IoT/CPS," *ZTE Technology Journal*, vol. 1, p. 013, 2011.
[52] P. Gaona-García, C. E. Montenegro-Marin, J. D. Prieto, and Y. V. Nieto, "Analysis of Security Mechanisms Based on Clusters IoT Environments," *International Journal of Interactive Multimedia and Artificial Inteligence*, vol. 4, no. Special Issue on Advances and Applications in the Internet of Things and Cloud Computing, 2017.
[53] S. Cirani, M. Picone, P. Gonizzi, L. Veltri, G. Ferrari, "Iot-oas: An oauth-based authorization service architecture for secure services in iot scenarios", *IEEE sensors journal*, 15(2):1224-34, 2015.
[54] R. T. Tiburski, L. A. Amaral, E. De Matos, F. Hessel. "The importance of a standard security architecture for SOA-based iot middleware". IEEE Communications Magazine, 53(12):20-6, 2015.
[55] P. N. Mahalle, B. Anggorojati, N. R. Prasad, and R. Prasad, "Identity authentication and capability based access control (iacac) for the internet of things," J. of Cyber Security and Mobility, vol. 1, 309-348, 2013.