IoT Security Evolution: Challenges and Countermeasures Review

Ali M A Abuagoub

Department of Computer Engineering, College of Computer Engineering and Sciences,
Prince Sattam bin Abdulaziz University, Kingdom of Saudi Arabia

***Abstract*:** Internet of Things (IoT) architecture, technologies, applications and security problems have been recently addressed by a number of researchers. Basically, IoT adds internet connectivity to a system of intelligent devices, machines, objects and/or people. Devices are allowed to automatically collect and transmit data over the Internet, which exposes them to serious attacks and threats. This paper provides an intensive review of IoT evolution with primary focusing on security issues together with the proposed countermeasures. Thus, it outlines the IoT security challenges as a future roadmap of research for new researchers in this domain.

***Keywords*:** IoT, security services, security mechanisms, security challenges.

1. Introduction

Today, Internet of Things (IoT) creates an architectural model from a huge amount of intelligent devices and smart tools which are connected with each other through cloud networking. IoT creates an environment for monitoring, collecting data and controlling systems. Recently, a number of projects and proposals on IoT applications have been discussed in the literature. Popular IoT-based smart applications include home, healthcare, industry, city, grid, building, appliances, wearables, car, communications, farming, factory/manufacturing, power/utilities, TV, retail, supply chain and robotics. Thus, the connectivity of IoT devices is steadily increasing, for instance the IoT will reach about 50 billion devices by 2020 as predicted in [1] or it will reach 75 billions by 2025 as reported in [2]. This expectation adds another dimension to the significance of IoT security [3]. For instance, everything like car, fridge, TV, console, and smartphone could be hacked, i.e., anybody can access and take some information and abused it. In IoT-based smart healthcare systems the compromise of a medical network sensor could lead to the loss of patient life(s). IoT-based devices in smart home are typically configured with built-in sensors for real-time monitoring, remote control, safety from intruders, gas/fire alarm, etc., thus the personal information could be leaked in absence of strong security. Security attacks in IoT-based smart industry may damage one of the devices of the IoT infrastructure or interrupt communication between two systems, which may affect other devices or systems and consequently leading to serious problems. Similarly, without secure IoT-based smart grid communications an attacker could spoof the identity of some one's smart meter. Also in IoT-based smart city the attacks or illegal access to information could cause physical disruptions in service availability.

Therefore, this paper reviews a number of recent research works that have been conducted in 2018-2019 with primary focusing on IoT security. In particular, its contributions can be pointed out as follows:

- Reviews of published research works' findings on IoT security, i.e., it summarizes major outcomes on IoT-based smart applications, security services and new approaches as countermeasures against security attacks.
- Highlights of IoT security challenges as a roadmap for future research directions.

The rest of the paper is organized as follows: Section 2 summarizes major research outcomes in IoT security together with the related application domains, security services, and new approaches as countermeasures that proposed to protect IoT application environments. Section 3 discusses IoT security challenges and open issues as a future roadmap of research for new researchers in this domain. Finally, Section 4 concludes the paper by outlining IoT security applications, countermeasures, services and challenges.

2. Related Research Works

This section summarizes studies that have been recently proposed within the IoT security domain. In particular, it highlights the main IoT-based smart applications for a number of researches as presented in the literature. Figure 1 shows dominant application sectors, which have been recently addressed by various researchers, from IoT security perspectives. These applications include: smart health, smart home, smart industry, smart grid, and smart city. Critical IoT security threats and some proposed solutions were reviewed in [4-6]. Common IoT security architectures, frameworks and platforms were presented in [7-11]. Further analysis of IoT security issues can be found in [3, 12-18].

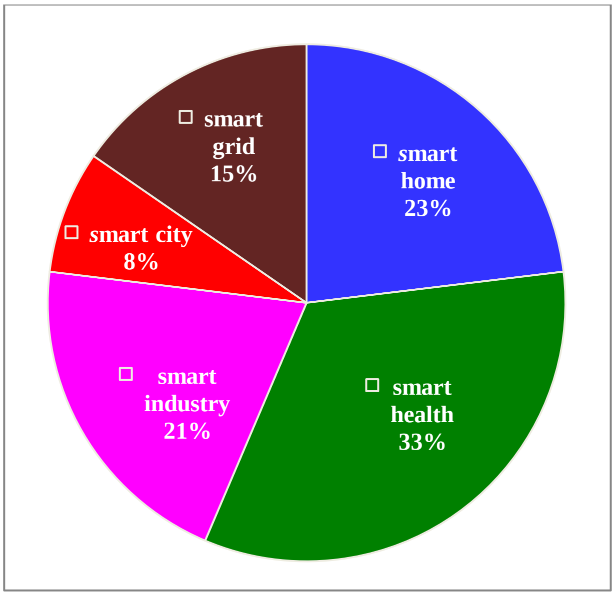

Figure 1. IoT security application domains

2.1 IoT security services

This subsection presents security services which have been explicitly mentioned in different studies that concern with IoT security. Table 1 records combinations of these security services with their references, whereas Figure 2 indicates that authentication has gained a great consideration within IoT security field, followed by privacy, access control, confidentiality and secure communication, respectively.

Table 1. Common security services

Security services	References
Authentication and trust management between IoT devices.	[19 - 34]
Support of confidentiality and privacy in IoT environment.	[35 - 53]
Control and verification of identification, authorization and access to IoT devices.	[1, 54 - 64]
Security of communication for IoT applications.	[65 - 71]
Prevention and detection of intrusions and attacks in IoT devices.	[72 - 82]
Enhancement of integrity and availability for IoT applications.	[83 - 87]

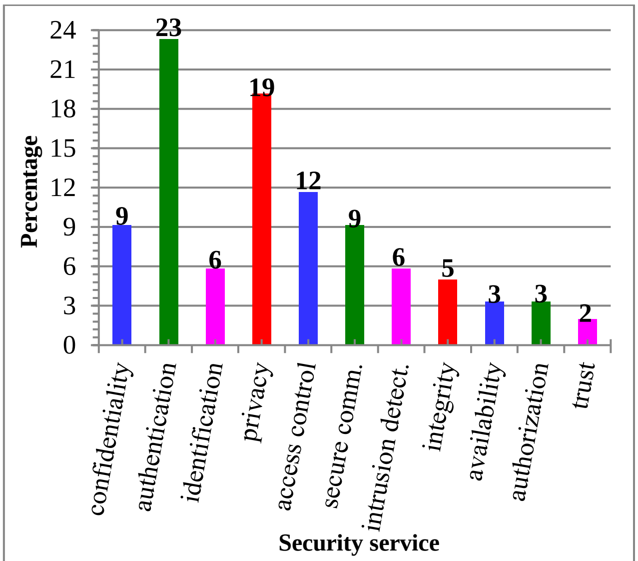

Figure 2. IoT security services

2.2 Recent security approaches

This section describes new technologies, techniques and concepts which have been recently introduced as new approaches to enhance IoT security, for instance blockchain (BC) in [88 - 96], cloud-fog in [57, 97 - 111], software-define network (SDN) and network-function virtual (NFV) in [112 - 116], physical unclonable function (PUF) in [117 - 119], machine learning (ML) in [115, 118, 120 - 122], lightweight algorithms in [103, 119, 121, 123 - 129], neural network (NN) in [130 - 132], and security fusion as a service (SFaaS) in [73]. Fingerprinting of IoT devices was studied in [133, 134], while authors in [135, 136] proposed solutions for supporting multimedia data in secure IoT environment. Figure 3 shows percentages the most promising approaches as proposed by different researchers to enhance IoT security. Thus, contributions of these approaches as new countermeasures can be ordered, from high to low, as follows: cloud-fog, lightweight algorithms, blockchain, machine learning, SDN/NFV, PUF and NN. The following subsections summarize recent studies on these approaches.

2.2.1 Blockchain-based IoT Security

This subsection highlights some studies that significantly contributed in enhancing IoT security based on blockchain approach. Various designs and implementations of blockchain-based IoT security proposals were introduced in [88, 90, 95, 96]. Recently, few researchers analyzed and discussed some blockchain-based IoT security problems [89, 91 - 94].

2.2.2 IoT Security Based on AI Techniques

Machine learning techniques for IoT security were introduced in [120, 122, 137]. Analysis and implementation of neural network-based IoT security algorithms were presented in [118, 130 - 133]. Biometric and fingerprinting techniques for IoT applications were developed in [121, 134].

2.2.3 Security of Cloud–based IoT Environment

Security and privacy schemes for fog computing-based IoT services were proposed in [101, 105, 107, 110, 138, 139]. Authentication schemes for IoT cloud environment were developed in [98, 100, 104, 106]. In [99, 102, 108, 110, 135, 139] some security schemes were proposed for controlling data access in IoT cloud. Design and implementation of schemes for trusting and securing communication in cloud-based IoT environment can be found in [97, 111].

2.2.4 IoT Security Schemes

This subsection mentions studies which proposed and implemented different lightweight algorithms or schemes for securing IoT systems. A number of schemes or methods have been proposed for minimizing security vulnerabilities and threats in IoT devices [103, 124, 126, 127, 129, 136, 140 - 145], and for resource-constrained IoT platforms [125, 146 - 148]. Performance analyses and evaluations of IoT security solutions were provided in [119, 123, 128, 149 - 153].

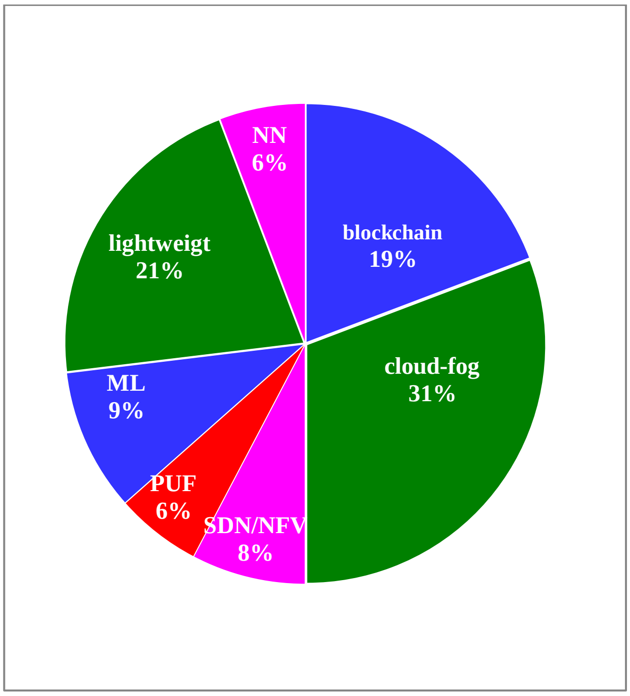

Figure 3. IoT security approaches

2.2.5 IoT Security Using SDN/NFV/PUF

IoT frameworks were designed in [112, 116] using software-define network (SDN) and network-function virtual (NFV), coupled with existing IoT security approaches. A Physical Unclonable Function (PUF) design based on piezo sensors in IoT devices was proposed as a cybersecurity solution [117]. Security features introduced by SDN/NFV against expected threats were analyzed in [113]. A fog-assisted SDN/IDPS system for securing IoT networks was proposed in [114].

3. Challenges and Future Directions

Although a number of studies have been conducted so far in the literature, to protect IoT applications, still there is a big security hole in IoT environment. IoT security issues and challenges have been analyzed in [12, 13, 16, 18, 21, 23, 29, 68, 115, 150, 153]. In [3, 6, 7, 9, 11, 15 - 17, 20, 37, 100] the authors reviewed recent IoT security research projects, tools, modelers and simulators. Researchers in [26, 28, 34, 65, 106, 142] tried to deploy the available cryptographic algorithms with slight enhancements for IoT security, whereas hardware ciphers have been addressed by authors in [13, 51, 60, 79, 125].

This section provides a number of IoT security challenges, as defined by other researchers, which can be considered as open issues for future research directions.

A. *Limitation* or constraints of device resources [1, 13, 17, 21, 23, 58, 90, 92, 93, 138, 154]: Manufacturers normally produce most of IoT equipment with low memories, computation capabilities, communication bandwidths and power supplies; on the other hand, classical security algorithms do not work well on IoT devices with limited capabilities [23]. Under tight IoT resource constraints the implementation of blockchain is required as a cost-effective solution [90]. In [13] limited computational resources were tackled by in-memory and near-memory computing. Storage capacity for sensors and actuators is limited, but in [92] the authors argued that the storage size can be increased if blockchain is used with IoT. In healthcare environment devices have less computation capabilities, memories and batteries which is a critical challenge for most of cryptographic solutions [17]. Similarly there are resource limitations for IoT devices and actuators in manufacturing [17]. Resource limitation is a challenge to protect communication in IoT environment [93]. Devices of small sizes with limited energies, memories, and processing capabilities is a real challenge for modeling access control in IoT environment [1]. Thus, deployment of IoT security still faces the biggest challenge of device resource constraints.

B. *Heterogeneity* and variation of devices, communication standards and information system technologies [17, 20, 23, 64, 92, 93, 100, 153]: IoT systems are diverse and connected over vast network with variation in computing capabilities for running encryption algorithms [92]. In [17] the authors discussed the heterogeneity as a challenge for different applications including: communication and information technologies in smart grids, network protocols and communication media in hospitals, heterogeneous elements in transportation, and heterogeneous smart devices in smart cities. Heterogeneity in cloud-based IoT environment is a challenge [100]. Implementation of a multi-layer security framework is critically needed for IoT environment to cope with various devices [93]. Heterogeneities of IoT devices and communication methods stand against deployment of traditional security solutions in IoT systems [23]. Therefore, heterogeneity of devices still represents a serious challenge to the IoT security.

C. *Scalability* of devices, application coverage and authentication schemes [1, 17, 23, 57, 64, 92, 100, 153]: This includes scalability, performance and integration of IoT technologies into the existing systems [57]. In [17] the researchers argued that scalability is a serious challenge for securing various IoT applications such as electrical energy consumption growth in smart grids, huge amount of IoT components in smart cities, and IoT systems grow continuously in manufacturing. Scalability in cloud-based IoT environment is a challenge for implementing authentication schemes [100]. In general scalability leads to great difficulties in key management and administration of large amount of devices [23]. Extension of IoT networks in terms of devices and sizes are critically important for designing a model for accessing the IoT system [1]. Thus, scalability of IoT systems remains a challenging to the adoption of effective IoT security mechanisms.

D. *Mutual* or common *authentication* [5, 9, 13, 20, 77, 100, 153]: Some researchers tried to protect authentication, however in a typical IoT network some issues still exist [9]. Security of cloud-based IoT authentication schemes against various attacks is a challenge [100]. Public key infrastructure and identity management system are main challenges to fully achieve mutual authentication [5].

E. *Trust management* [9, 12, 14, 23, 36, 93]: Trust is a very important technique that ensures credibility of dynamic IoT devices [14]. In [12] a gateway was proposed for analyzing and managing the security of the local IoT environment. Many unsuccessful techniques have been proposed for privacy and trust in IoT evironment [9]. It is challenging to provide trust management for a great amount of IoT devices [93]. As a result of the absence of central administration for IoT infrastructure the trust management still remains as a significant challenge [23].

F. *Standardization* of protocols for IoT devices [10, 17, 21, 57, 77, 92]: Formation of an international body is critically needed for enforcing security standards in IoT products [77]. Global standards are required for IoT architecture, device interconnection and service integration [57]. Still there is no technical standards for data storing, communicating and processing [90]. There is no protocol standard for IoT-based SCADA systems in manufacturing [17].

G. *Identity verification* and integrity of IoT end devices [13, 36, 77, 88, 153]: Diversification of IoT devices resulted in complexity of identity verification [88]. A network identity verification method can be implemented in IoT environment to facilitate the exchange of information between devices [13].

H. *Privacy preservation* of data and information [9, 10, 13, 14, 17, 20, 21, 23, 36, 37, 57, 77, 100, 138, 153]: Privacy means the information of users that submitted to IoT applications is secure and cannot be accessible by others [9]. There is a lack of lightweight anti-malware solutions for IoT devices [14]. Although a number of researches considered privacy of users and data still there is a need for data privacy at different states including collection, aggregation, sharing and management [77]. Disclosure or unauthorized access of home or cloud services can be prevented by developing reliable and well-balanced security frameworks [57]. Technical standards are necessary to be considered for implementing privacy protection mechanisms [10]. It is challenging to protect exchange of user data between local smart meters and remote control center in smart grids [17]. Protecting vehicle drivers from different network attacks is challenge for smart transportation systems [17]. Privacy of data maintained in cloud-based IoT environment is a challenge [100]. Higher privacy requires weaker identity while strong security demands strong identity, thus a tradeoff between privacy and security is an open issue [23].

I. *Modeling* of IoT network traffic, threats and attacks [3, 37, 75, 90, 115, 153]: Although IoT traffic characterization, filtration and sampling are more complicated they are important to identify malicious nodes and to improve the effectiveness of trust computation [75]. Threat modeling is useful for effective IoT security mitigation [3]. Realistic attack models are necessary to detect cyber criminals that arise from interconnection of smart IoT devices [75]. Consistent formalization of inputs (data and attacks) and outputs (processed data) is needed for ML algorithm to properly work in IoT environment [115].

J. *Integration* of security mechanisms in IoT protocols and architectures [12, 23, 37, 57, 58]: It includes integration of security mechanisms in existing IoT platforms [12]. Integration of IoT with the open physical world may expose IoT applications to security compromising [23].

K. *Access control* and privilege management based on locations and rights [1, 5, 13, 21, 36, 57, 90]: Access control is essential specially for IoT devices which may be located on open areas and physically under control of opponents [90]. Contract management plays a centralized role for IoT systems in the future generations [5]. Delegation of authority to IoT devices has to be considered by an access model to enable usability and flexibility of IoT systems [1].

L. *Lightweight* cryptographic algorithms and effective key management [13, 14, 36, 58, 77]: Resource constraints of IoT devices as a challenge raises the requirements for designing lightweight algorithms to protect data confidentiality and integrity in IoT environment [14] and to support real-time fog-based IoT services [77].

M. *Intrusion detection* and prevention [20, 21, 36, 88]: It includes abnormal network traffic monitoring [88]. Adoption of intrusion detection and prevention is a challenge to avoid IoT botnet and DDoS [36].

N. *Mobility* of devices, data management and routing protocols [14, 17, 21, 75, 100, 153]: Although routing protocols are insecure providing protection against routing threats is critically important in IoT environment [14]. Most of healthcare devices are embedded in human bodies, which makes security solutions for mobility is a serious challenge [17]. Security solutions are highly challenging for smart vehicles in high mobility environment [17]. Smart devices often generate huge traffic in modern cities and consequently raise several challenges to the data management [17].

O. Hardware/firmware *vulnerabilities* and consumer illiteracy with IoT devices [14, 17, 21, 23, 84, 90, 92, 93, 115]: Hardware security of most IoT devices is neglected by manufacturers [14]. IoT technology is still new, which means that its skilled force is very much limited and extremely less when it is integrated with blockchain [92]. Vulnerabilities related to information system technology can be found in smart grids as open systems subjected to a number of attacks [17]. Manufacturing systems including SCADA systems are vulnerable to several type of attacks [17]. Hardware level security is necessary for IoT systems to detect and alleviate vulnerabilities [93]. Breach of IoT security is mostly caused by less security preparation including user mindsets, design and manufacture of devices [23]. Security-by-design approach can be applied to software and hardware development to free systems from vulnerabilities [115].

P. *Interoperability* of security protocols and *interaction* between users and policies: Interoperability of security protocols implemented at different layers is a critical challenge to standardize an IoT security mechanism [93]. Interoperability of access policies with multiple users and organizations is a challenge for an access control model [1]. Thus, interoperability and interaction between protocols, users and policies are still challenges to the development of any IoT security model.

Q. *Decentralized* IoT security based on blockchain as a reliable platform [77, 90, 10, 91, 93, 115]: Further research is needed to adopt blockchain as a reliable and secure IoT platform [77]. Blockchain can reduce hard and soft compromising of physically accessible IoT devices [90]. However, blockchain vulnerabilities are challenges which need providing of effective security mechanisms [93]. Adoption of blockchain for decentralized IoT security can provide a privacy-preserving [115].

Figure 4 reflects the significance of each security challenge as compared with others. These security challenges can be ordered in the following list based on their critical roles in IoT environment:

1. Privacy preservation of data and information.
2. Limitation or constraints of device resources.
3. Hardware/firmware vulnerabilities and consumer illiteracy with IoT devices.
4. Heterogeneity and variation of devices, communication standards and information system technologies.
5. Scalability of devices, application coverage and authentication schemes.
6. Mutual or common authentication.
7. Access control and privilege management based on locations and rights.
8. Trust management.
9. Standardization of protocols for IoT devices and processing.
10. Modeling of IoT network traffic, threats and attacks.
11. Mobility of devices, data management and routing protocols.
12. Decentralization of IoT security based on blockchain as a reliable platform.
13. Identity verification and integrity of IoT end devices.
14. Integration of security mechanisms in IoT protocols and architectures.
15. Lightweight cryptographic algorithms and effective key management.
16. Intrusion detection and prevention.
17. Interoperability of security protocols and interaction between users and policies.

Thus, the above list summarizes the most important IoT security challenges, which can be adopted as open issues for future research directions.

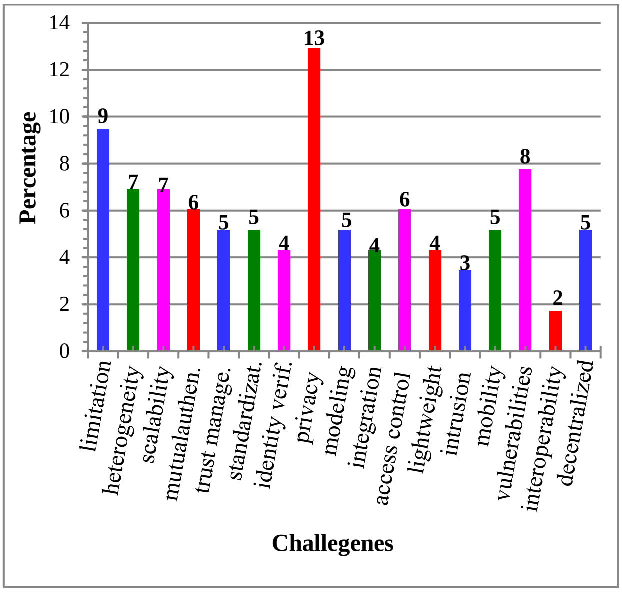

Figure 4. IoT security challenges

4. Conclusion

Today, Internet of Things (IoT) applications are growing very fast. However, IoT devices are insecure due to a number of reasons including constrained resources, heterogeneity, scalability and lack of standards. This paper has studied a large no of IoT research works with a primary focusing on IoT security. Thus, it presents the main IoT application domains from security perspectives including industry, healthcare, home, city, grid, communications, building, car, factory, TV, supply chain, storehouse, social IoT(S-IoT), and transportation. Also the paper highlights new approaches as countermeasures, proposed by the researchers to enhance IoT security, such as cloud-fog, lightweight algorithms, blockchain, machine learning, SDN/NFV, PUF and NN. In contrast the paper points out the following IoT security services: authentication, privacy, access control, confidentiality and secure communication. Finally, the paper outlines IoT security challenges as a future roadmap of research for new researchers in this domain. Challenges and open issues include privacy, limitation of resources, vulnerabilities, heterogeneity, scalability, mutual authentication, access control, trust management, standardization, modeling, mobility, decentralization, identity verification, integration, lightweight algorithms, intrusion detection and interoperability.

Acknowledgement

This research work was supported by the Deanship of Scientific Research at Prince Sattam Bin Abdulaziz University.

References

[1] H. F. Atlam, R. J. Walters, G. B. Wills, and J. Daniel, Fuzzy Logic with Expert Judgment to Implement an Adaptive Risk-Based Access Control Model for IoT, *Mobile Networks and Applications*, January, 2019.

[2] M. Schunter, and A. Wespi, Editorial: Special issue on IoT security and privacy, *Computer Networks*, Vol. 6, No.17, December, 2018.

[3] M. b. M. Noor, and W.H. Hassan, Current research on Internet of Things (IoT) security: A survey, *Computer Networks*, Vol. 8, No. 29, pp. 283–294, December, 2018.

[4] M. F. Elrawy, A. I. Awad, and H. F. A. Hamed, Intrusion detection systems for IoT-based smart environments: a survey, *Journal of Cloud Computing: Advances, Systems and Applications*, Vol. 7, No. 1, pp. 1-20, December, 2018.

[5] F. Marinoa, C. Moiso, and M. Petracca, Automatic contract negotiation, service discovery and mutual authentication solutions: A survey on the enabling technologies of the forthcoming IoT ecosystems, *Computer Networks*, Vol. 148, pp. 176–195, 2019.

[6] I. Stellios, P. Kotzanikolaou, M. Psarakis, C. Alcaraz, and J. Lopez, A Survey of IoT-Enabled Cyberattacks: Assessing Attack Paths to Critical Infrastructures and Services, *IEEE Communications Surveys & Tutorials*, Vol. 20, No. 4, pp. 3453- 3495, 4th Quarter, 2018.

[7] D. D. López, M. B. Uribe, C. S. Cely, D. T. Murgueitio, E. G. Garcia, P. Nespoli, and F. G. Mármol, Developing Secure IoT Services: A Security-Oriented Review of IoT Platforms, *Symmetry*, Vol. *10, No.* 669, November, 2018.

[8] R. Malik, K. Solanki, and S. Dalal, Literature Review on Security Aspects of IOT, *International Journal of Advanced Research in Computer Science*, Vol. 12, No. 2, pp. 131-134, March-April, 2018.

[9] M. Burhan, R. A. Rehman, B. Khan, and B-S. Kim, IoT Elements, Layered Architectures and Security Issues: A Comprehensive Survey, *Sensors*, Vol. 18, No. 2796, August, 2018.

[10] J. Hou, L. Qu, and W. Shi, A survey on internet of things security from data perspectives, *Computer Networks*, Vol. 7, No. 41, pp. 295–306, December, 2018.

[11] M. Ammar, G. Russello, and B. Crispo, Internet of Things: A survey on the security of IoT frameworks, *Journal of Information Security and Applications*, Vol. 38, pp. 8-27, 2018.

[12] R. Román-Castro, J. López, and S. Gritzalis, Evolution and Trends in IoT Security, *Computer IEEE Computer Society*, pp. 16-25, July, 2018.

[13] M. Kesavan, and J. Prabhu, A Survey, Design and Analysis of IoT Security and QoS Challenges, *International Journal of Information System Modeling and Design*, Vol. 9, No. 3, pp. 48-66, July-September, 2018.

[14] M. Frustaci, P. Pace, G. Aloi, and G. Fortino, Evaluating Critical Security Issues of the IoT World: Present and Future Challenges, *IEEE Internet of Things Journal*, Vol. 5, No. 4, pp. 2483- 2495, August, 2018.

[15] A. Colakovic, and M. Hadžialic, Internet of Things (IoT): A review of enabling technologies, challenges, and open research issues, *Computer Networks*, Vol. 144, pp. 17–39, July, 2018.

[16] P. Asghari, A. M. Rahmani, and H. H. S. Javadi, Internet of Things applications: A systematic review, *Computer Networks*, Vol. 148, pp. 241–261, December, 2018.

[17] D. E. Kouicem, A. Bouabdallah, and H. Lakhlef, Internet of things security: A top-down survey, *Computer Networks,* Vol. 141, pp. 199–221, March, 2018.

[18] A. R. Sfar, E. Natalizio, Y. Challal, and Z. Chtourou, A roadmap for security challenges in the Internet of Things, *Digital Communications and Networks,* Vol. 4, pp. 118–137, 2018.

[19] S. N. Matheu-García, J. L. Hernández-Ramosa, A. F. Skarmetaa, and G. Baldinic, Risk-based automated assessment and testing for the cybersecurity certification and labelling of IoT devices, *Computer Standards & Interfaces,* Vol. 62, pp. 64–83, 2019.

[20] A. Gupta, A. Anpalagan, G. H.S. Carvalho, A. S. Khwaja, L. Guan, and I. Woungang, Prevailing and emerging cyber threats and security practices in IoT-Enabled smart grids: A survey, *Journal of Network and Computer Applications,* Vol. 132, pp. 118–148, February, 2019.

[21] K. Kimani, V. Oduol, and K. Langat, Cyber security challenges for IoT-based smart grid networks, *International Journal of Critical Infrastructure Protection*, Vol. 25, pp. 36–49, January, 2019.

[22] S. Pérez, D. Garcia-Carrillo, R. Marín-López, J. L. Hernández-Ramos, R. Marín-Pérez, and A. F. Skarmeta, Architecture of security association establishment based on bootstrapping technologies for enabling secure IoT infrastructures, *Future Generation Computer Systems,* Vol. 95, pp. 570–585, January, 2019.

[23] K. Sha, W. Wei, T. A. Yang, Z. Wangb, and W. Shi, On security challenges and open issues in Internet of Things, *Future Generation Computer Systems,* Vol. 83, pp. 326–337, 2018.

[24] D. D. López, M. B. Uribe, C. S. Cely, A. V. Torres, N. M. Guataquira, S. M. Castro, P. Nespoli, and F. G. Mármol, Shielding IoT against Cyber-Attacks: An Event-Based Approach Using SIEM, *Wireless Communications and Mobile Computing*, October, 2018.

[25] T. Perković, M. Čagalj, and T. Kovačević, LISA: Visible light based initialization and SMS based authentication of constrained IoT devices, *Future Generation Computer Systems,* Vol. 97, pp. 105–118, March, 2019.

[26] T. Kudithi, and R. Sakthivel, "High-performance ECC processor architecture design for IoT security applications, *Journal of Supercomputing,* Vol. 75, pp. 447–474, January, 2019.

[27] M. Alshahrani, and I. Traore, Secure mutual authentication and automated access control for IoT smart home using cumulative Keyed-hash chain, *Journal of Information Security and Applications,* Vol. 45, pp. 156–175, February, 2019.

[28] A. Lohachab, and Karambir, ECC based inter-device authentication and authorization scheme using MQTT for IoT networks, *Journal of Information Security and Applications,* Vol. 46, pp. 1–12, 2019.

[29] N. Miloslavskaya, and A. Tolstoy, Internet of Things: information security challenges and solutions, *Cluster Computing,* Vol. 22, pp. 103–119, 2019.

[30] H. Hamidi, An approach to develop the smart health using Internet of Things and authentication based on biometric technology, *Future Generation Computer Systems,* Vol. 91, pp. 434–449, 2019.

[31] M. Suárez-Albela, P. Fraga-Lamas, L. Castedo, and T. M. Fernández-Caramés, Clock Frequency Impact on the Performance of High-Security Cryptographic Cipher Suites for Energy-Efficient Resource-Constrained IoT Devices, *Sensors,* Vol *19, No.* 15, 2019.

[32] J. Ni, X. Lin, and X. S. Shen, Efficient and Secure Service-Oriented Authentication Supporting Network Slicing for 5G-Enabled IoT, *IEEE Journal on Selected Areas In Communications*, Vol. 36, No. 3, pp. 644-657, March, 2018.

[33] Y. Zhou, T. Liu, F. Tang, and M. Tinashe, An Unlinkable Authentication Scheme for Distributed IoT Application, *IEEE Access,* Vol. 7, pp. 14757- 14766, February, 2019.

[34] Z. Liu, and H. Seo, IoT-NUMS: Evaluating NUMS Elliptic Curve Cryptography for IoT Platforms, IEEE Transactions on Information Forensics and Security, Vol. 14, No. 3, pp. 720- 729, March, 2019.

[35] J.–Z. Chen, Embedding the MRC and SC Schemes into Trust Management Algorithm Applied to IoT Security Protection, *Wireless Personal Communications,* Vol. 99, pp. 461–477, January, 2018.

[36] W. Zhou, Y. Jia, A. Peng, Y. Zhang, and P. Liu, The Effect of IoT New Features on Security and Privacy: New Threats, Existing Solutions, and Challenges Yet to Be Solved, *IEEE Internet of Things Journal*, January, 2018.

[37] M. Talal, A. A. Zaidan, B. B. Zaidan, A. S. Albahri, A. H. Alamoodi, O. S. Albahri, M. A. Alsalem, C. K Lim, K. L. Tan, W. L. Shir, and K. I. Mohammed, Smart Home-based IoT for Real-time and Secure Remote Health Monitoring of Triage and Priority System using Body Sensors: Multi-driven Systematic Review, *Journal of Medical Systems,* Vol. 43, No. 42, January, 2019.

[38] J. L. Hernández-Ramos, S. Pérez, C. Hennebert, J. B. Bernabé, B. Denis, A. Macabies, and A. F. Skarmeta, Protecting personal data in IoT platform scenarios through encryption-based selective disclosure, *Computer Communications,* Vol. 130, pp. 20–37, 2018.

[39] Z. Wang, A privacy-preserving and accountable authentication protocol for IoT end-devices with weaker identity, *Future Generation Computer Systems,* Vol. 82, pp. 342–348, 2018.

[40] V. Sharma, I. You, D. N. K. Jayakody, and M. Atiquzzaman, Cooperative trust relaying and privacy preservation via edge-crowdsourcing in social Internet of Things, *Future Generation Computer Systems,* Vol. 92, pp. 758–776, 2019.

[41] S. V. Limkar, and R. K. Jha, Computing over encrypted spatial data generated by IoT, *Telecommunication Systems,* Vol. 70, pp. 193–229, 2019.

[42] H. Wanga, G. Hana, L. Zhoua, J. A. Anserea, and W. Zhang, A source location privacy protection scheme based on ring-loop routing for the IoT, *Computer Networks,* Vol. 148, pp. 142–150, 2019.

[43] D. Kim, K. Park, Y. Park, and J-H. Ahn, Willingness to provide personal information: Perspective of privacy calculus in IoT services, *Computers in Human Behavior*, Vol. 92, pp. 273–281, 2019.

[44] R. Hamza, Z. Yan, K. Muhammad, P. Bellavista, and Faiza Titouna, A privacy-preserving cryptosystem for IoT E-healthcare, *Journal of Information Sciences*, Vol. 17, No. 28, February, 2019.

[45] T. Li, C. Gao, L. Jiang, W. Pedrycz, and J. Shen, Publicly verifiable privacy-preserving aggregation and its application in IoT, *Journal of Network and Computer Applications*, Vol. 126, pp. 39–44, 2019.

[46] H. Yana, Z. Chena, and C. Jia, SSIR: Secure similarity image retrieval in IoT, *Journal of Information Sciences*, Vol. 479, pp. 153–163, 2019.

[47] Y.-N. Liu, Y.-P. Wang, X.-F. Wang, Z. Xia, and J.-F. Xu, Privacy-preserving raw data collection without a trusted authority for IoT, *Computer Networks*, Vol. 148, pp. 340–348, 2019.

[48] K. Li, L. Tian, W. Li, G. Luo, and Z. Cai, Incorporating social interaction into three-party game towards privacy protection in IoT, *Computer Networks*, Vol. 150, pp. 90–101, 2019.

[49] J. Jang, I.Y Jung, and J. H. Park, An effective handling of secure data stream in IoT, *Applied Soft Computing*, Vol. 68, pp. 811–820, 2018.

[50] G. Chu, N. Apthorpe, and N. Feamster, Security and Privacy Analyses of Internet of Things Children's Toys, *IEEE Internet of Things Journal*, Vol. 6, No.1, pp. 978-985, February, 2019.

[51] H. Tao, M. Z. A. Bhuiyan, A. N. Abdalla, M. M. Hassan, J. M. Zain, and T. Hayajneh, Secured Data Collection with Hardware-based Ciphers for IoT-based Healthcare, *IEEE Internet of Things Journal*, Vol. 6, No. 1, pp. 410-420, February, 2019.

[52] L. Jiang, T. Li, X. Li, M. Atiquzzaman, H. Ahmad, and X. Wang, Anonymous Communication via Anonymous Identity-Based Encryption and Its Application in IoT, *Wireless Communications and Mobile Computing*, Vol. 2018, November, 2018.

[53] J. M. de Fuentes, L. Gonzalez-Manzano, A. Solanas, and F. Veseli, Attribute-Based Credentials for Privacy-Aware Smart Health Services in IoT-Based Smart Cities, *Computer IEEE Computer Society*, Vol. 51, pp. 44-53, 2018.

[54] Q. Huang, L. Wang, and Y. Yang, DECENT: Secure and fine-grained data access control with policy updating for constrained IoT devices, *World Wide Web Journal*, Vol. 21, pp. 151–167, January, 2018.

[55] F. D. Hudson, Enabling Trust and Security: TIPPSS for IoT, *IT Professional IEEE Computer Society*, pp. 15-18, April, 2018.

[56] B. Lu, L. Wang, J. Liu, W. Zhou, L. Guo, M.-H. Jeong, S. Wang, and G. Han, LaSa: Location Aware Wireless Security Access Control for IoT Systems, *Mobile Networks and Applications*, June, 2018.

[57] M. Tao, J. Zuo, Z. Liu, A. Castiglione, and F. Palmieri, Multi-layer cloud architectural model and ontology-based security service framework for IoT-based smart homes, *Future Generation Computer Systems*, Vol. 78, pp. 1040–1051, 2018.

[58] R.-H. Hsu, J. Lee, T. Q. S. Quek, and J-C. Chen, Reconfigurable Security: Edge-Computing-Based Framework for IoT, *IEEE Network*, pp. 92-99, October, 2018.

[59] H. Yan, Y. Wang, C. Jia, J. Li, Y. Xiang, and W. Pedrycz, IoT-FBAC: Function-based access control scheme using identity-based encryption in IoT, *Future Generation Computer Systems*, Vol. 95, pp. 344–353, January, 2019.

[60] Z. Zhoua, W. Zhang, S. Li, and N. Yu, Potential risk of IoT device supporting IR remote control, *Computer Networks*, Vol. 148, pp. 307–317, 2019.

[61] Y. Yang, X. Zhenga, W. Guoa, X. Liua, and V. Chang, Privacy-preserving smart IoT-based healthcare big data storage and self-adaptive access control system, *Journal of Information Sciences*, Vol. 479, pp. 567–592, 2019.

[62] N. Akatyev, and J. I. James, Evidence identification in IoT networks based on threat assessment, *Future Generation Computer Systems*, Vol. 93, pp. 814–821, 2019.

[63] U. Sarfraz, M. Alam, S. Zeadally, and A. Khan, Privacy aware IOTA ledger: Decentralized mixing and unlinkable IOTA transactions, *Computer Networks*, Vol. 148, pp. 361–372, 2019.

[64] R. Hodgson, Solving the security challenges of IoT with public key cryptography, *Network Security*, pp. 17-19, January, 2019.

[65] M. Suárez-Albela, P. Fraga-Lamas, and T. M. Fernández-Caramés, A Practical Evaluation on RSA and ECC-Based Cipher Suites for IoT High-Security Energy-Efficient Fog and Mist Computing Devices, *Sensors*, Vol 18, No. 11, 3868, November, 2018.

[66] M. Sinda, T. Danner, S. O'Neill, A. Alqurashi, and H-K Kim, Improving the Bluetooth Hopping Sequence for Better Security in IoT Devices, *International Journal of Software Innovation*, Vol. 6, No. 4, pp. 117-131, December, 2018.

[67] S. Plaga, N. Wiedermann, S. D. Anton, S. Tatschner, H. Schotten, and T. Newe, Securing future decentralised industrial IoT infrastructures: Challenges and free open source solutions, *Future Generation Computer Systems*, Vol. 93, pp. 596–608, 2019.

[68] C.-Y. Chen, M. Hasan, and S. Mohan, Securing Real-Time Internet-of-Things, *Sensors* Vol. 18, No. 4356, pp. 1-21, December, 2018.

[69] S. Tonyali, K. Akkaya, N Saputro, A. S. Uluagac, and M. Nojoumian, Privacy-preserving protocols for secure and reliable data aggregation in IoT-enabled Smart Metering systems, *Future Generation Computer Systems*, Vol. 78, pp. 547–557, 2018.

[70] S. Anandhi, R. Anitha, and V. Sureshkumar, IoT Enabled RFID Authentication and Secure Object Tracking System for Smart Logistics, *Wireless Personal Communications*, Vol. 104, pp. 543–560, 2019.

[71] D.-S. Agha, F. H. Khan, R. Shams, H. H. Rizvi, and F. Qazi, A Secure Crypto Base Authentication and Communication Suite in Wireless Body Area Network (WBAN) for IoT Applications, *Wireless Personal Communications*, Vol. 103, pp. 2877–2890, 2018.

[72] A. Nieto, A. Acien1, and G. Fernandez, Crowdsourcing Analysis in 5G IoT: Cybersecurity Threats and Mitigation, *Mobile Networks and Applications*, October, 2018.

[73] C.-T. Kuo, P.-W. Chi, V. Chang, and C.-L. Lei, SFaaS: Keeping an eye on IoT fusion environment with security fusion as a service, *Future Generation Computer Systems*, Vol. 86, pp. 1424–1436, January, 2018.

[74] E. Benkhelifa, T. Welsh, and W. Hamouda, A Critical Review of Practices and Challenges in Intrusion Detection Systems for IoT: Toward Universal and Resilient Systems, *IEEE Communications Surveys & Tutorials*, Vol. 20, No. 4, pp. 3496-3509, Fourth-Quarter, 2018.

[75] W. Meng, Intrusion Detection in the Era of IoT: Building Trust via Traffic Filtering and Sampling, *Computer Published by the IEEE Computer Society*, pp. 36-43, July, 2018.

[76] X. Su, Z. Wang, X. Liu, C. Choi, and D. Choi, Study to Improve Security for IoT Smart Device Controller: Drawbacks and Countermeasures, *Security and Communication Networks*, May, 2018.

[77] I. Makhdoom, M. Abolhasan, J. Lipman, R. P. Liu, and W. Ni, Anatomy of Threats to the Internet of Things, *IEEE Communications Surveys and Tutorials*, 2018.

[78] B. Yigit, G. Gür, F. Alagöz, and B. Tellenbach, Cost-aware securing of IoT systems using attack graphs, *Ad Hoc Networks*, Vol. 86, pp. 23–35, January, 2019.

[79] B. Xu, W. Wang, Q. Hao, Z. Zhang, P. Du, T. Xia, H. Li, and X. Wang, A Security Design for the Detecting of Buffer Overflow Attacks in IoT Device, *IEEE Access*, Vol. 6, pp. 72862-72869, December, 2018.

[80] U. D. Gandhi, P. M. Kumar, R. Varatharajan, G. Manogaran, R. Sundarasekar, and S. Kadu, HIoTPOT: Surveillance on IoT Devices against Recent Threats, Wireless Personal Communications, Vol. 103, pp. 1179–1194, 2018.

[81] D. Choi, and K. Lee, An Artificial Intelligence Approach to Financial Fraud Detection under IoT Environment: A Survey and Implementation, *Security and Communication Networks*, September, 2018.]

[82] A. Mehmood, M. Mukherjee, S. H. Ahmed, H. Song, and K. M. Malik, NBC-MAIDS: Naive Bayesian classification technique in multi-agent system-enriched IDS for securing IoT against DDoS attacks, *Journal of Supercomputing*, Vol. 74, pp. 5156–5170, May, 2018.

[83] B. Ali, and A. I. Awad, Cyber and Physical Security Vulnerability Assessment for IoT-Based Smart Homes, *Sensors*, Vol. 18, No. 817, March, 2018.

[84] S. Cha, S. Baek, S. Kang, and S. Kim, Security Evaluation Framework for Military IoT Devices, *Security and Communication Networks*, July, 2018.

[85] C. Toma, and M. Popa, IoT Security Approaches in Oil & Gas Solution Industry 4.0, *Informatica Economică*, Vol. 22, No.3, pp. 46-61, 2018.

[86] Z. Guan, Y. Zhang, L. Wu, J. Wu, J. Li, Y. Ma, and J. Hu, APPA: An anonymous and privacy preserving data aggregation scheme for fog-enhanced IoT, *Journal of Network and Computer Applications*, Vol. 125, pp. 82–92, 2019.

[87] Y. Zhang, R. H. Deng, G. Han, and D. Zheng, Secure smart health with privacy-aware aggregate authentication and access control in Internet of Things, *Journal of Network and Computer Applications*, Vol. 123, pp. 89-100, September, 2018.

[88] Y. Qian , Y. Jiang , J. Chen , Y. Zhang , J. Song , M. Zhou, and M. Pustišek, Towards decentralized IoT security enhancement: A blockchain approach, *Computers and Electrical Engineering*, Vol. 72, pp. 266–273, September, 2018.

[89] I. Makhdoom, M. Abolhasan, H. Abbas, and W. Ni, Blockchain's adoption in IoT: The challenges, and a way forward, *Journal of Network and Computer Applications*, Vol. 125, pp. 251–279, November, 2019.

[90] M. Banerjee, J. Lee, and K-K R. Choo, A blockchain future for internet of things security: a position paper, *Digital Communications and Networks*, Vol. 4, pp. 149–160, 2018.

[91] D. Minoli, and B. Occhiogrosso, Blockchain mechanisms for IoT security, *Internet of Things*, Vol. 1, No. 2, pp. 1–13, June, 2018.

[92] N. M. Kumar, and P. K. Mallick, Blockchain technology for security issues and challenges in IoT, *Procedia Computer Science*, Vol. 132, pp. 1815–1823, 2018.

[93] M. A. Khan, and K. Salah, IoT security: Review, blockchain solutions, and open challenges, *Future Generation Computer Systems*, Vol. 82, pp. 395-411, 2018.

[94] W. Li, S. Tug, W. Meng, and Y. Wang, Designing collaborative blockchained signature-based intrusion detection in IoT environments, *Future Generation Computer Systems*, Vol. 96, pp. 481–489, 2019.

[95] M. T. Hammi, B. Hammi, P. Bellot, and A. Serhrouchni, Bubbles of Trust: A decentralized blockchain-based authentication system for IoT, *Computers & Security*, Vol. 78, pp. 126–142, 2018.

[96] S.-K. Kim, U.-M. Kim, and J.-H. Huh, A Study on Improvement of Blockchain Application to Overcome Vulnerability of IoT Multiplatform Security, *Energies*, Vol. 12, No. 402, January, 2019.

[97] B. Mukherjee, S. Wang, W. Lu, R. Lal`Neupane, D. Dunn, Y. Ren, Q. Su, and P. Calyam, Flexible IoT security middleware for end-to-end cloud–fog communication, *Future Generation Computer Systems*, Vol. 87, pp. 688–703, February, 2018.

[98] M. Wazida, A. K. Das, and A. V. Vasilakosc, Authenticated key management protocol for cloud-assisted body area sensor networks, *Journal of Network and Computer Applications*, Vol. 123, pp. 112–126, 2018.

[99] C. Stergioua, K. E. Psannisa, B. B. Guptab, and Y. Ishibashic, Security, privacy & efficiency of sustainable Cloud Computing for Big Data & IoT, *Sustainable Computing: Informatics and Systems*, Vol. 19, pp. 174–184, 2018.

[100] M. Wazida, A. Kumar Das, R. Hussainc, G. Succi, and J. J.P.C. Rodrigues, Authentication in cloud-driven IoT-based big data environment: Survey and outlook, *Journal of Systems Architecture*, Vol. 22, No. 18, January, 2019.

[101] B. P. Kavin, and S. Ganapathy, A secured storage and privacy-preserving model using CRT for providing security on cloud and IoT-based applications, *Computer Networks*, Vol. 151, pp. 181–190, January, 2019.

[102] J. Haoa, C. Huang, J. Ni, H. Ronga, M. Xiana, and X. Shenb, Fine-grained data access control with attribute-hiding policy for cloud-based IoT, *Computer Networks*, Vol. 153, pp. 1–10, February, 2019.

[103] L. Zhou, X. Li, K.-H. Yeh, C. Su, and W. Chiu, Lightweight IoT-based authentication scheme in cloud computing circumstance, *Future Generation Computer Systems*, Vol. 91, pp. 244–251, 2019.

[104] R. Amin, N. Kumar, G.P. Biswas, R. Iqbal, and V. Changd, A lightweight authentication protocol for IoT-

enabled devices in distributed Cloud Computing environment, *Future Generation Computer Systems*, Vol. 78, pp. 1005–1019, 2018.

[105] S. Belguitha, N. Kaaniche, M. Laurent, A. Jemai, and R. Attia, PHOABE: Securely outsourcing multi-authority attribute based encryption with policy hidden for cloud assisted IoT, *Computer Networks,* Vol. 133, pp. 141–156, 2018.

[106] B.-W. Jin, J.-O. Park, and H.-J. Mun, A Design of Secure Communication Protocol Using RLWE-Based Homomorphic Encryption in IoT Convergence Cloud Environment, *Wireless Personal Communications*, Vol. 105, pp. 599–618, 2019.

[107] X. Li, X. Jin, Q. Wang, M. Cao, and X. Chen, SCCAF: A Secure and Compliant Continuous Assessment Framework in Cloud-Based IoT Context, *Wireless Communications and Mobile Computing,* October, 2018.

[108] S. Xu, G. Yang, Y. Mu, and X. Liu, A secure IoT cloud storage system with fine-grained access control and decryption key exposure resistance, *Future Generation Computer Systems,* February, 2019.

[109] Z. Xu, R. Gu, T. Huang, H. Xiang, X. Zhang, L. Qi, and X. Xu, An IoT-Oriented Offloading Method with Privacy Preservation for Cloudlet-Enabled Wireless Metropolitan Area Networks, *Sensors*, Vol. 18, No. 30, September, 2018.

[110] J.-S. Fu, Y. Liu, H.-C. Chao, B. K. Bhargava, and Z.-J. Zhang, Secure Data Storage and Searching for Industrial IoT by Integrating Fog Computing and Cloud Computing, *IEEE Transactions on Industrial Informatics*, Vol. 14, No. 10, pp. 4519-4528, October, 2018.

[111] X. Li, Q. Wang, X. Lan, X. Chen, N. Zhang, and D. Chen, Enhancing Cloud-Based IoT Security Through Trustworthy Cloud Service: An Integration of Security and Reputation Approach, *IEEE Access,* Vol. 7, pp. 9368- 9383, January, 2019.

[112] A. M. Zarca, J. B. Bernabe, I. Farris, Y. Khettab, T. Taleb, and A. Skarmeta, Enhancing IoT security through network softwarization and virtual security appliances, *International Journal of Network Management*, May, 2018.

[113] I. Farris, T. Taleb, Y. Khettab, and J.S. Song, A Survey on Emerging SDN and NFV Security Mechanisms for IoT Systems, *IEEE Communications Surveys and Tutorials*, Vol. 21, pp. 812-837, 2019.

[114] Q. Shafi, A. Basit, S. Qaisar, A. Koay, and I. Welch, Fog-Assisted SDN Controlled Framework for Enduring Anomaly Detection in an IoT Network, *IEEE Access*, Vol. 6, pp. 73713-7372, December, 2018.

[115] F. Restuccia, S. D'Oro, and T. Melodia, Securing the Internet of Things in the Age of Machine Learning and Software-Defined Networking, *IEEE Internet of Things Journal*, Vol. 5, No. 6, pp. 4829-4842, December, 2018.

[116] A. M. Zarca, D. Garcia-Carrillo, J. B. Bernabe, J. Ortiz, R. Marin-Perez, and A. Skarmeta, Enabling Virtual AAA Management in SDN-Based IoT Networks, *Sensors, Vol. 19*, No. 295, January, 2019.

[117] C. Labrado, and H. Thapliyal, Design of a Piezoelectric Based Physically Unclonable Function for IoT Security, *IEEE Internet of Things Journal,* 2018.

[118] B. Chatterjee, D. Das, S. Maity, and S. Sen, RF-PUF: Enhancing IoT Security through Authentication of Wireless Nodes Using In-situ Machine Learning, *IEEE Internet of Things Journal*, 2018.

[119] Y. Bendavid, N. Bagheri, M. Safkhani, and S. Rostampour, IoT Device Security: Challenging - A Lightweight RFID Mutual Authentication Protocol Based on Physical Unclonable Function, *Sensors*, Vol. 18, No. 4444, December, 2018.

[120] L. Xiao, X. Wan, X. Lu, Y. Zhang, and D. Wu, IoT Security Techniques Based on Machine Learning-How do IoT devices use AI to enhance security, *IEEE Signal Processing Magazine*, pp. 41-49, September, 2018.

[121] P. Punithavathi, S. Geetha, M. Karuppiah, S. H. Islam, M. M. Hassan, and K-K. R. Choo, A lightweight machine learning-based authentication framework for smart IoT devices, *Journal of Information Sciences*, Vol. 484, pp. 255–268, 2019.

[122] K. A.P. da Costa, J. P. Papa, C. O. Lisboa, R. Munoz, V. H. C. de Albuquerque, "Internet of Things: A survey on machine learning-based intrusion detection approaches", *Computer Networks*, Vol. 151, pp. 147–157, 2019.

[123] M. Qasaimeh, R. S. Al-Qassas, and S. Tedmori, Software randomness analysis and evaluation of lightweight ciphers: the prospective for IoT security, *Multimedia Tools and Applications,* Vol. 77, pp. 18415–18449, February, 2018.

[124] W. Feng, Y. Qin, S. Zhao, and D. Feng, AAoT: Lightweight attestation and authentication of low-resource things in IoT and CPS, *Computer Networks*, Vol. 134, pp. 167–182, February, 2018.

[125] R. Leveugle, A. Mkhinini, and P. Maistri, Hardware Support for Security in the Internet of Things - From Lightweight Countermeasures to Accelerated Homomorphic Encryption, *Information Journal,* Vol. 9, No. 114, May, 2018.

[126] S. F. Aghili, H. Mala, M. Shojafar, and P. Peris-Lopez, LACO: Lightweight Three-Factor Authentication, Access Control and Ownership Transfer Scheme for E-Health Systems in IoT, *Future Generation Computer Systems,* Vol. 96, pp. 410–424, 2019.

[127] S. F. Aghili, M. Ashouri-Talouki, and H. Mala, DoS, impersonation and de-synchronization attacks against an ultra-lightweight RFID mutual authentication protocol for IoT, Journal of Supercomputing, Vol. 74, pp. 509–525, 2018.

[128] K.-H. Wang, C.-M. Chen, W. Fang, and T.-Y. Wu, On the security of a new ultra-lightweight authentication protocol in IoT environment for RFID tags, *Journal of Supercomputing*, Vol. 74, pp. 65–70, 2018.

[129] B. J. Mohd, and T. Hayajneh, Lightweight Block Ciphers for IoT: Energy Optimization and Survivability Techniques, *IEEE Access,* Vol. 6, pp. 35966-35978, July, 2018.

[130] M. Xi, N. Lingyu, and S. Jiapen, IoT individual privacy features analysis based on convolutional neural network, *Cognitive Systems Research,* Vol. 57, pp. 126-130, 2019.

[131] X. Liu, C. Zhang , P. Liu, M. Yan, B. Wang, J. Zhang, and R. Higgs, Application of Temperature Prediction Based on Neural Network in Intrusion Detection of IoT, *Security and Communication Networks*, December, 2018.

[132] K. W. G. Cowdrey, and R. Malekian, Home automation - an IoT based system to open security gates using number plate recognition and artificial neural networks, *Multimedia Tools and Applications,* Vol. 77, pp. 20325–20354, 2018.
[133] K. Yang, Q. Li, and L. Sun, Towards automatic fingerprinting of IoT devices in the cyberspace, *Computer Networks,* Vol. 148, pp. 318–327, 2019.
[134] V. Thangavelu, D. M. Divakaran, R. Sairam, S. S. Bhunia, and M. Gurusamy, DEFT: A Distributed IoT Fingerprinting Technique, *IEEE Internet of Things Journal*, Vol. 6, No. 1, pp. 940 – 952, February, 2019.
[135] X. Hu, C. Tang, D. S. Wong, and X. Zheng, Efficient pairing-free PRE schemes for multimedia data sharing in IoT, *Multimedia Tools and Applications*, Vol. 77, pp. 18327–18354, 2018.
[136] H. Noura, A. Chehab, L. Sleem, M. Noura, R. Couturier, and M. M. Mansour, One round cipher algorithm for multimedia IoT devices, *Multimedia Tools and Applications,* Vol. 77, pp. 18383–18413, 2018.
[137] S.-J. Yang, and X. Huang, Certain types of M-fuzzifying matroids: A fundamental look at the security protocols in RFID and IoT, *Future Generation Computer Systems,* Vol. 86, pp. 582–590, April, 2018.
[138] R. Ullah, S. H. Ahmed, and B-S Kim, Information-Centric Networking With Edge Computing for IoT: Research Challenges and Future Directions, *IEEE Access*, Vol. 6, pp. 73465-73488, December, 2018.
[139] A. Viejo, and D. Sánchez, Secure and privacy-preserving orchestration and delivery of fog-enabled IoT services, *Ad Hoc Networks*, Vol. 82, pp. 113–125, 2019.
[140] C. Bodei, S. Chessa, and L. Galletta, Measuring security in IoT communications, *Theoretical Computer Science*, December, 2018.
[141] S. Choi, C. Yang, and J. Kwak, System Hardening and Security Monitoring for IoT Devices to Mitigate IoT Security Vulnerabilities and Threats, *Transactions on Internet and Information Systems*, Vol. 12, No. 2, pp. 906-918, February, 2018.
[142] S. Kim, and I.Y. Lee, IoT device security based on proxy re-encryption, *Journal of Ambient Intelligence and Humanized Computing,* Vol. 9, pp. 1267–1273, January, 2018.
[143] B. Maram, J. M. Gnanasekar, G. Manogaran, and M. Balaanand, Intelligent security algorithm for UNICODE data privacy and security in IOT Service, *12th IEEE Int. Conf. on Service-Oriented Computing and Applications*, Kaohsiung, Taiwan, 2019.
[144] S. Kaedi1, M. A. Doostari, and M. B. Ghaznavi-Ghoushchi, Low-complexity and differential power analysis (DPA)-resistant two-folded power-aware Rivest–Shamir–Adleman (RSA) security schema implementation for IoT-connected devices, *IET Computers & Digital Techniques Journal*, Vol. 12, No.6, pp. 279-288, 2018.
[145] G. George, and S. M. Thampi, A Graph-Based Security Framework for Securing Industrial IoT Networks from Vulnerability Exploitations, *IEEE Access*, Vol. 6, pp. 43586-43601, August, 2018.
[146] G. Margelis, X. Fafoutis, G. Oikonomou, R. Piechocki, T. Tryfonas, and P. Thomas, Efficient DCT-based secret key generation for the Internet of Things, *Ad Hoc Networks*, Vol. 23, No. 50, pp. 1-11, August, 2018.
[147] H. Kim, D. Kim, O. Yi, and J. Kim, Cryptanalysis of Hash Functions Based on Blockciphers Suitable for IoT Service Platform Security, *Multimedia Tools and Application,* March, 2018.
[148] J. Moon, I. Y. Jung, and J. H. Park, IoT application protection against power analysis attack, *Computers and Electrical Engineering Journal,* Vol. 67, pp. 566–578, March, 2018.
[149] M. Mangia, F. Pareschi, R. Rovatti, and G. Setti, Low-Cost Security of IoT Sensor Nodes with Rakeness-Based Compressed Sensing: Statistical and Known-Plaintext Attacks, *IEEE Transactions on Information Forensics and Security*, Vol. 13, No. 2, pp. 327-339, February, 2018.
[150] O. Mavropoulos, H. Mouratidis, A. Fish, and E. Panaousis, Apparatus: A framework for security analysis in internet of things systems, *Ad Hoc Networks*, Vol. 21, No. 13, pp. 1-11, August, 2018.
[151] S. Kwon, J. Jeong, and T. Shon, Toward Security Enhanced Provisioning in Industrial IoT Systems, *Sensors*, Vol. 18, No. 4372, December, 2018.
[152] M. A. A. da Cruz, J. J. P. C. Rodrigues, A. K. Sangaiah, J. Al-Muhtadi, and V. Korotaev, Performance evaluation of IoT middleware, *Journal of Network and Computer Applications,* Vol. 109, pp. 53–65, March, 2018.
[153] A. Tewari, and B. B. Gupta, Security, privacy and trust of different layers in Internet-of-Things (IoTs) framework, *Future Generation Computer Systems,* April, 2018.
[154] Y. Zhang, L. Xu, Q. Dong, J. Wang, D. Blaauw, and D. Sylvester, Recryptor: A Reconfigurable Cryptographic Cortex-M0 Processor With In-Memory and Near-Memory Computing for IoT Security, *IEEE Journal of Solid-State Circuits,* Vol. 53, No. 4, pp. 995-1005, April, 2018.