Survey of Security Threats in IoT and Emerging Countermeasures

Mimi Cherian(✉) and Madhumita Chatterjee(✉)

Pillai College of Engineering, Mumbai University, Navi Mumbai, India
{mcherian,mchatterjeee}@mes.ac.in

Abstract. In Internet of things there are many things connected through network which can be sensors, actuators or devices meant for collecting data and transmitting data. These collected data is used for optimizing the network performance, improving performance of products and services. In future it is predicted billions of devices will be connected in network for the working of IoT. Hence securing network and increasing its flexibility along with scalability will be mandatory requirement for the working of IoT. This paper is an attempt to do a broad survey of security issues in IoT and resolving it by exploring latest techniques like Software Defined Network, Blockchain and Machine Learning.

Keywords: Software Defined Network · Blockchain · Internet of Things · Security

1 Introduction

Emergence of Internet of Things (IoT) is one of the spectacular phenomenon in last few years. IoT means interconnection of heterogeneous entities where these entities can be a sensors, devices, humans or any thing that requests or provides services. Implementation of IoT architecture requires some modifications in traditional network. These modification includes converting an isolated device into a communicating device, need to improve the storage and computation power of small computing devices while their physical size is reduced drastically and development of various lightweight secure protocols for communication between different objects in IoT environment. The changes brought in traditional network to support working of IoT environment has its own side effects. The area for security attack in IoT domain is more and potential threats against security of these entities in the domain has grown drastically. IoT is implemented in domains like health monitoring, building automation and nuclear power grid. Securing the IoT domain is of great concern as its implementation is in critical environment that carries time sensitive data. Currently ongoing research topics are based on identifying the potential threats in IoT and their possible countermeasures. The survey paper aims to find all possible issues in IoT and its

S. M. Thampi et al. (Eds.): SSCC 2018, CCIS 969, pp. 591–604, 2019.
https://doi.org/10.1007/978-981-13-5826-5_46

various solutions, in which many recent solutions lead to exploring the potential of technologies like Software Defined Network(SDN) and BlockChain. The flow of paper will be as follows:-

- Reference model of IoT and its communication protocols.
- Survey of security issues in each layer and their existing solutions till now.
- Survey of techniques related to SDN and Blockchain as solution for IoT security issues.

1.1 IoT Reference Model

Initially IoT emerged with three layer layered architecture mainly have three layers like Perception layer, Transport layer and Application Layer [1–5]. The Data Processing layer which process the strategic decision making in cloud is considered as a part of either Application Layer else Network layer. Few researchers have divided the Application Layer and Data Processing Layer as separate layers thus leading to four layered IoT Architecture [6–9].

Recently Cisco has defined a seven layer IoT reference model (Fig. 1) that has the potential to be standardized [10]. The communication is bidirectional i.e if it is a control system then data and commands will flow from application layer to edge node layer while in monitoring system the flow of communication will be from edge node layer to application layer.

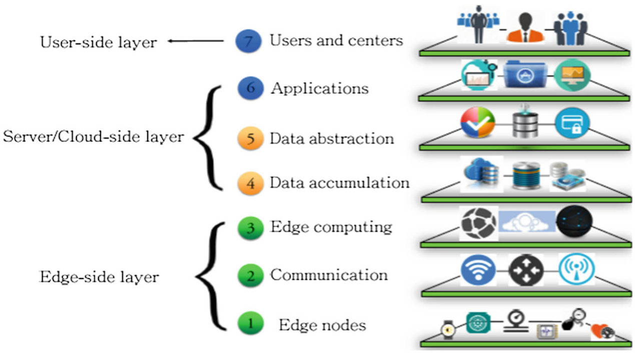

Fig. 1. Cisco defined IoT layers [10]

Working of Each Layer in IoT: Working of each layer in reference model is summarized as follows:-

- Edge side layer: It consist of computing nodes like RFID readers, sensors, actuators and controllers. In this layer expectation is to provide integrity and confidentiality of data collected and sent across.
  - Edge node: This is layer consists of different sensors and devices which monitors the network and collects data from different sources.

- Communication: The communication layer includes objects that can be used for communication between objects in first level, second level and third level. Information transmission takes place in this layer.
- Edge Computing: It is similar to Fog computing which initiates data processing. Edge computing reduces computation load in higher level and provide fast response. This computing layer consists of simple learning algorithm and data processing. Real time applications performs computation close to edge node close to network.

- Data Accumulation and Abstraction: The Data Accumulation layer allows to store data for future reference and strategic analysis. Its main activity is to convert the network packets into data and storing them in tables for selective sorting.
- Application and users Layer: It provides a application based platform for users to provide and interpret information. Users makes use of these application to make strategic decisions and analytical data.

1.2 IoT Communication Protocol

In IoT network the protocol stack has to be different from traditional OSI model as the IoT Environment devices are more resource constrained compared to traditional network. IoT Protocol are supposed to be lightweight protocols.

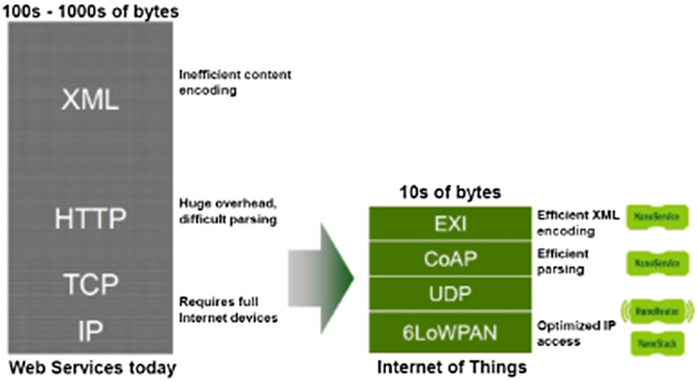

Fig. 2. IoT protocol stack

In Fig. 2 Protocol stack [11] the protocol stack used by IoT is described. It consists of following communication protocols :-

- 6LoWPAN is abbreviation for IPv6 over Low power Wireless Personal Area. 6LoWPAN protocol has a layer which helps to adapt the resource constrained devices with IP world thus enabling Internet to access the sensor devices.
- UDP: They are connectionless datagrams that also enable to transmit smaller packets and cycles with few overhead and has faster wake-up.

- CoAP is abbreviation for Constrained application protocol. It is a transfer protocol which is similar to HTTP, but COAP is designed such that it can help in communication for resource constrained devices. This protocols is used for communication between resource constrained IoT devices and resource rich devices based on internet. CoAP is a binary protocol that is transported over UDP. The semantics of CoAP were designed to closely model those of HTTP. Being a binary protocol reduces its data overhead while its use of UDP increases its flexibility in communication models and its ability to reduce latency. One of the benefits of using HTTP semantics on top of CoAPs UDP rather than HTTPs TCP is that a device can easily use the same protocol code to talk to the cloud and other devices on the local network.
- EXI is abbreviation for Efficient XML Interchange. This format is a compact XML representation. The resource constrained devices needs some technique to support XML application hence EXI is defined as it requires less bandwidth and enhances encoding/decoding performance. EXI compression helps in reducing the content of document structure by generating internally small tags based upon the present XML schema, the processing stage and the context. Ensuring that the tags are to optimize data representation. The document is in binary format that has all data tags of document encoded using event code. Event codes are binary tags that maintains their value only in their assigned position within the EXI stream.

2 Security Issues in IoT

In traditional network the expected requirement for secure network are Confidentiality, Integrity, Availability, Non-repudiation and Privacy. In IoT the same requirements are considered but violation of any of these can be life threatening.

In confidentiality the network should not allow unauthorized access to certain information like time critical or sensitive data like medical records and prescription of a patient [12].

Integrity is necessary to ensure reliable communication such that the information sent and received are legitimate. Integrity attack takes place on medical devices like an insulin pump [13] or pacemaker [14].

Availability of data in IoT environment is a major requirement as many analytic and strategic decisions are made based on real time data generated in IoT domain.

Non-repudiation ensures that whether an event has occurred or not in the network thus leading to reliable working of network. In each layer of IoT reference model there are different vulnerabilities which can lead to various attacks. In Table 1 the survey of all attacks in each layer and their solutions given by different researchers

2.1 Attacks in IoT

The current section provides details of various attacks that takes place on edge node along with their respective counter measures. The scope of attack on edge side layer includes edge nodes like RFID tags, readers, smart controller, sensors, communication channel between edge nodes and edge computing or fog node.

- Hardware Trojan: In this attack the attacker can maliciously modify the integrated circuit and helps to obtain access to the software running on ICs [15].
- Denial of Service Attack: In Edge layer devices there are few types of denial of service attacks like sleep deprivation attack, battery draining and outage attack.
    - Battery draining Attack: In this attack the attacker can send many random packets which will force the node to authenticate its validity [16].
    - Sleep deprivation Attack: In this attack the attacker sends many undesired requests which seems valid and the energy constrained device will exhaust itself processing these battery draining requests [17].
    - Outage attacks: Outage can be caused due to battery draining or sleep deprivation attack which stops the device from performing its scheduled tasks [18].

  DoS attack can create unnecessary traffic and misdirect the packets in the communication channel. Many attacks of DoS include injecting fraudulent packets using insertion, manipulation and replication [19].
- Routing attacks like Sybil, Black hole, Worm hole and Hello flood are possible which can spoof, misdirect, drop or alter the packets.
    - In Sybil attack a single compromised entity can present itself with multiple identities which can control large part of its network [20].
    - Black hole attack is the attack in which a malicious node tries attract all traffic to go through it by broadcasting that it has shortest path to reach the destination node [21].
    - Worm hole attack the packets that are transmitted in a network are recorded in a particular location then it is tunneled to another location [22].
- Physical attacks on edge devices: In this attack the attacker tries extract valuable cryptographic information, modify the operating system or tamper the circuit. Hence the main purpose of this attack is to extract information for further analysis like find the fixed shared key [23].
- Tag cloning: It is also called as spoofing, RFID tag cloning can be used to impersonate RFID tags and gain access to restricted areas. There can be high potential damage by too much of automation [24].
- Node Replication attack: In this attack the attacker adds a malicious node along with remaining nodes which can easily misdirect the traffic. The malicious node may revoke authorized nodes by executing node-revocation protocols [25,26].
- Side channel attacks: In this attack the attacker extracts information that is unintentionally leaked like details of service provider or servers from communication channel even when the messages are encrypted.

The summary Table 1 covers major attacks happening in IoT and based on type of attack different countermeasures are identified.

Table 1. Summarized IoT attacks and countermeasures

Layers of IoT	Attacks	Countermeasures
Edge node	Side-channel attacks:	Malicious firmware/software detection [27] Randomized delay [28] Intentionally-generated noise [29] Ba1ancing Hamming weights [30]
	Battery-draining sleep deprivation attack	Policy-based mechanisms and intrusion detection systems (IDSs) [19]
	RFID tag	Personal RFID firewall [31] Anonymous tag [32] Lightweight cryptographic protocol [33]
Communication layer	DoS Sybil Wormhole Black hole	IDS designed for IoT [34]
		Lightweight encryption techniques like CLEFIA [35] and PRESENT [36]
Edge computing layer	Code injection	IDS diglossia [37]
	Virus, worms, spyware	Anti-virus, firewall, IDS [3]

In Traditional network similar kind of security issues were found and solutions were also similar, but since these attacks are in IoT environment it is more resource constrained and has critical impact. Hence improving the existing countermeasures would not be sufficient to resolve security issues in IoT (Table 2).

Table 2. Comparison between traditional network and IoT network security

Traditional network security	IoT network security
Add-on security reactive in nature	Built-in security proactive in nature
Complex algorithms requires more processing and computation time	Lightweight algorithms for resource-constrained devices and less computation time
User control can be monitored continuously	Privacy issue: IoTs often collect automatically user private information hence cannot be disclosed
Small technological heterogeneity	Large technological heterogeneity due communication with different devices and thus also large attack surface
Placed in closed environments	Placed in both open and closed environments depending on IoT application

Initially the approach for resolving the security issues in IoT network was using the counter measures of traditional network. Currently researchers are changing their approach of resolving IoT network related issues rather than implement reactive measures to resolve issues, research is currently towards proactively resolving the network security issues in IoT.

3 Survey on Different Approaches to Secure IoT Framework

In last few years some technologies were found that can be compatible with IoT network which helps to make the network more secure and proactive in nature. Software Defined Network (SDN) helps network operators to program and manage the network. SDN helps IoT network to be managed dynamically in a resource constrained network. It provides opportunities to enhance security in IoT networks, applications can be created on SDN to prevent, detect and react to threats.

The main functionality of SDN is to decouple the data planes and control plane in a network. Decision making in SDN is done by control plane and data forwarding is handled by switches. Compared to traditional network high level algorithms are used for decision making hence require sophisticated router while using SDN simpler networking hardware can be used and network can be managed more easily.

However despite these advantages of SDN there are some security issues with respect storage of to huge collection of data from to IoT environment in cloud. Hence to resolve security issues in cloud they have recently introduced blockchain paradigm whenever SDN and IoT is integrated.

3.1 Secure IoT Framework with SDN Gateways

In paper [38] Salman et al. proposed a mechanism called identity based authentication which can be used to secure IoT with SDN. In SDN a trusted third party certificate authority is implemented to control the security of network. They have proposed a mechanism of identifying each device connected to IoT network by assigning virtual IPv6 based identity to all things via a controller. The controller and gateways generates public key for devices using ECC. Thus SDN controller can identify heterogeneous IoT devices using virtual IPv6 addresses and authenticate gateways and devices. This technique protects IoT network from masquerade, man-in-the-middle and replay attacks.

In paper [39] Nobakht et al. proposed a methodology of host-based intrusion detection and mitigation framework for IoT network using SDN. The technique they created is called IoT-Intrusion Detection and Mitigation (IoTIDM). The modules required for IoTIDM are implemented on an SDN controller. Third party entity provides security as a service for remote security management. The authors uses SDN technology along with machine learning techniques to provide security services. The IoT-IDM framework, is placed on the top of SDN controller.

The framework consists of five key modules: Device Manager, Sensor Element, Feature Extractor, Detection and Mitigation. These modules help in decreasing the volume of traffic and identifying source of attack. This is done using machine learning algorithm to build predictive model for detecting malicious traffic. Once the source of attack is identified traffic rules are loaded on switches to mitigate the attack as Openflow gives the flexibility to isolate the infected host. The drawback of this framework is, it can only provide protection for a specific host and cannot provide protection or monitor the whole network.

In paper [40], Chakrabarty et al. proposed Black SDN for IoT a SDN-based secure networking mechanism. Black SDN tries to mitigate traffic and gather data regarding attacks, they also encrypt payload along with header, source and destination IP address. However, encrypting header causes issues while routing, hence to resolve it a simple broadcast routing protocol is proposed that is utilized by SDN controller. The SDN controller acts as a trusted third party and controls the flow of black packets. The SDN controller manages the flow of black packets through active nodes. Since IoT environment has nodes with less battery life its possible nodes have their sleep or duty cycle. Hence SDN controller helps in dynamically rerouting packets if nodes are in sleep cycle.

In paper [41] Bull et al. proposed a SDN gateway which can provide flow based security to mitigate DDoS attack. The idea is IoT gateways are used as SDN gateway and it monitors the traffic to find any anomaly behavior. In proper SDN environment its switches are dumb and used only for forwarding but in his work author tries to add additional capabilities to the switches and provides mitigation of DDoS attack on TCP and ICMP packets.

3.2 Secure IoT Framework with SDN cluster formation

Flauzac et al. [42] they proposed a secure SDN based solution in which node has two Openflow enabled node and each node is connected to a controller in a domain. SDN controller will be playing the role of security guard at edge of each domain. The SDN controller is each domain is responsible for the nodes in its domain and is aware of policies of its domain only, hence each domain will communicate with other domain through domain's border controller. The same work is extended in paper [43] in which each domain is defined as cluster with cluster head that is SDN controller and they also proposed a routing protocol for distributed clusters

Bhunia et al. [44] they proposed a secured SDN based IoT framework called SoftThings which monitors the network and finds the abnormal behavior thus trying to resolve network security issues at the earliest. Their aim is to prevent attacks at network level rather than at device level. SoftThings consists of different components like IoT devices, SDN enabled switches, Cluster SDN controller and Master SDN Controller.

The master SDN Controller is updated frequently by Cluster SDN controller when there is change in pattern of traffic and hence detects anomalies. The Cluster SDN Controller consists of Learning module, Classification module and

Flow management module. The learning module is provided with known behavior of DDoS attacking pattern and passes its knowledge to classification module. Machine learning algorithm is used by SDN controller and Support Vector Machine is used for classification of traffic. The techniques used are promising and able to detect attack with high precision and recall.

3.3 Secure IoT Framework with SDN and Blockchain

Tselios et al. [46] suggest that despite all advantages of integrating SDN with IoT network there is large scope for attack compared to traditional network. Especially when SDN is integrated with IoT related networking elements, more security concerns arise, due to the increased vulnerability in deployments of inter-cloud communication. The main concern while working in a heterogeneous IoT environment is need of a trustworthy third party to authenticate and authorize the communication. Relying on a centralized third party authority has its own security issues due to which concept of blockchain arises.

A blockchain distributed data structure that is replicated and shared among the members of a network and is tamper-proof. The concept of blockchain based security layer is implemented in their proposed architecture. Cloud deployment consists of interconnected nodes and sensors through blockchain which improves inter-cloud communication. Blockchain is used as a distributed data structure that can create a digital transaction ledger and also maintain history of all transaction records. It also allows transfer of encrypted data between interconnected nodes in IoT environment regardless of the network size or its geographical barrier. This mechanism is still under research by industry and academia [47–50].

In paper [52] Sharma et al. proposed a model for distributed cloud architecture based on blockchain technology, that can provide more secure, least cost and dynamic access to the most exhaustive computing infrastructures in an IoT network. The proposal is based on recent technologies: blockchain and fog computing. They have created a distributed cloud infrastructure, the proposed model achieves high-performance computing in cost effective manner.

They have provided a secure distributed fog node architecture that uses blockchain techniques such that it can bring computing resources to the edge of Iot network which enhances security. They used the protocol of 2 hop blockchain [53] for combining Proof-of-Work and Proof-of-Stake Securely to ensure security of blockchain. The have considered Matchmaking algorithm to link a resource requester and resource provider. Scheduling algorithm CLOUDRB [54] is used. It is a technique for managing and scheduling the high-performance computing application in the cloud. The proposed architecture was designed to support high scalability, security, high availability, real-time data delivery, low latency and resiliency (Table 3).

Table 3. Survey of SDN-IoT integration for n/w security

Sr.no	Reference paper	Methodology	Resolves	Security parameter
1	"Identity-based authentication scheme for the Internet of Things" [38]	ECC key management by SDN controller to authenticate gateway and things associated	Masquerade man-in-the-middle replay attacks	Confidentiality, Integrity
2	"A host-based intrusion detection and mitigation framework for smart home IoT using OpenFlow," [39]	IoT-IDM uses technologies SDN and machine learning. An API is created which extracts features, detect and mitigate attacks	Masquerade, DoS	Privacy Availability Accountability
3	"Black SDN for the internet of things" [40]	Secure each layer of communication by encrypting metadata and payload	Eavesdropping packet injection	Integrity, Confidentiality
4	"Flow based security for IoT devices using an SDN gateway," [41]	IoT gateway as SDN switch and integrated controller to analyse traffic	DoS	Availability, Security
5	"SDN based architecture for IoT and improvement of the security" [42]	Cluster management with SDN cluster head and gateway for communication between clusters	Routing flexibility	Availability
6	"Dynamic attack detection and mitigation in IoT using SDN" [44]	Cluster SDN controller and master SDN controller with machine learning	DoS, DDoS	Integrity, Availability, Security
7	Enhanced SDN security using firewall in a distributed scenario [45]	OpenFlow switch is intermediate firewall and	Flexible routing load balancing	Availability, Auditability
8	Enhancing SDN security for IoT-related deployments through blockchain [51]	Communication between IoT cloud through secure gateway using SDN and blockchain	DDoS forged switch flow rule	Integrity Availability Accountability Auditability Trustworthiness
9	"A software defined fog node based distributed blockchain cloud architecture for IoT" [52,55]	secure distributed fog node architecture that uses SDN and blockchain techniques	Low network performance overhead, Energy efficient communication	Accountability Auditability Trustworthiness

4 Critical Analysis

SDN converts the static network paradigm to adaptable and programmable networks. SDN can program the network routing thus avoiding network bottlenecks. As SDN controller has a global view of the network and can modify traffic when needed. Major research is happening in the field of implementing more security features in SDN. SDN is helpful in dynamic rerouting of network flow and scalability but currently it is lagging from security point of view. When SDN does traffic re-routing it has access only to header fields of the packet, there is no provision to do a deep packet inspection to check whether the packet flow is malicious or harmful to SDN Controller or Data plane. If the SDN controller is compromised then indirectly the attacker has access to the whole view of network thus leading to easy attack on network.

The advantages of SDN and IoT integration is recognized in many domains like smart grid settings, smart homes or smart transportation. SDN-IoT integration is also provides security in IoT, because security mechanisms can be implemented easily by implementing SDN-API [39–50]. In papers [51–55] authors have discussed improving security in inter cloud communication and IoT environment devices by using the concept of blockchain.

5 Conclusion

The literature survey motivates researchers to shift their thought process of having similar solutions to secure IoT network as for security issues in traditional network. The mitigation of security issues in IoT environment should be proactive in nature to sustain the versatile demand of IoT. It is necessary to appropriately enforce Trust Management and Security in the IoT network starting from the changing the framework for securing IoT. The survey for resolving IoT network security issues using SDN along with Blockchain, Firewall and Machine learning gives rise to more potential area for research.

References

1. Frustaci, M., Pace, P., Aloi, G.: Securing the IoT world: issues and perspectives. In: IEEE Conference on Standards for Communications and Networking (CSCN) (2017)
2. Chahid, Y., Benabdellah, M., Azizi, A.: Traffic-aware firewall optimization strategies (2010)
3. Deogirikar, J., Vidhate, A.: Security attacks inIoT: a survey. In: International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC 2017)
4. Lin, J., Yuy, W., Zhangz, N., Yang, X., Zhangx, H., Zhao, W.: A survey on internet of things: architecture, enabling technologies, security and privacy, and applications. In: 2016 IEEE
5. Mendez, D., Papapanagiotou, I., Yang, B.: Internet of Things: survey on security and privacy. In: IEEE J. July 2017
6. Varga, P., Plosz, S., Soos, G.: Security threats and issues in automation IoT. IEEE (2017)
7. Kumar, S.A., Vealey, T., Srivastava, H.: Security in Internet of Things: challenges, solutions and future directions. In: 49th Hawaii International Conference on System Sciences (2016)
8. Kuusijarvi, J., Savola, R., Savolainen, P., Evesti, A.: Mitigating loT security threats with a trusted network element. In: The 11th International Conference for Internet Technology and Secured Transactions (ICITST-2016)
9. Dorsemaine, B., Gaulier, J-P., Wary, J-P., Kheir, N.: A new approach to investigate IoT threats based on a four layer model. In: 13th International Conference on New Technologies for Distributed Systems (NOTERE 2016)

10. The Internet of Things reference model. 4CISCO (2014). http://cdn.iotwf.com/resources/71/IoTReferenceModelWhitePaperJune42014.pdf
11. Emmerson, B.: Unleashing the Internet of Things. http://www.iotevolutionworld.com/m2m/articles/208798-unleashing-internet-things.htm
12. Zhang, M., Raghunathan, A., Jha, N.K.: Trustworthiness of medical devices and body area networks. Proc. IEEE **102**(8), 1174–1188 (2014)
13. Li, C., Raghunathan, A., Jha, N.K.: Hijacking an insulin pump: security attacks and defenses for a diabetes therapy system. In: Proceedings of the IEEE 13th International Conference on e-Health Networking Applications and Services, pp. 150–156 (2011)
14. Halperin, D., et al.: Pacemakers and implantable cardiac defibrillators: software radio attacks and zeropower defenses. In: Proceedings of the IEEE Symposium Security and Privacy, pp. 129–142 (2008)
15. Bhunia, S., Hsiao, M.S., Banga, M., Narasimhan, S.: Hardware trojan attacks: threat analysis and countermeasures. Proc. IEEE **102**(8), 1229–1247 (2014)
16. Brandt, A., Buron, J.: Home automation routing requirements in low-power and lossy networks. https://tools.ietf.org/html/rfc5826
17. Martin, T., Hsiao, M., Ha, D., Krishnaswami, J.: Denial-of-service attacks on battery-powered mobile computers. In: Proceedings of the IEEE 2nd Conference on Pervasive Computing and Communications, pp. 309–318 (2004)
18. Matrosov, A., Rodionov, E., Harley, D., Malcho, J.: Stuxnet under the microscope, ESET LLC, Technical report (2011)
19. Walters, J.P., Liang, Z., Shi, W., Chaudhary, V.: Wireless sensor network security: a survey. Secur. Distrib. Grid Mobile Pervasive Comput. **1**, 367 (2007)
20. Douceur, J.R.: The sybil attack. In: Druschel, P., Kaashoek, F., Rowstron, A. (eds.) IPTPS 2002. LNCS, vol. 2429, pp. 251–260. Springer, Heidelberg (2002). https://doi.org/10.1007/3-540-45748-8_24
21. Karakehayov, Z.: Using reward to detect team black-hole attacks in wireless sensor networks. In: Proceedings of the Workshop on Real-World Wireless Sensor Networks, pp. 20–21 (2005)
22. Garcia-Morchon, O., Kumar, S., Struik, R., Keoh, S., Hummen, R.: Security considerations in the IP-based Internet of Things. https://tools.ietf.org/html/draft-garcia-core-security-04
23. Hernandez, G., Arias, O., Buentello, D., Jin, Y.: Smart nest thermostat: a smart spy in your home. In: Proceedings of the Black Hat USA (2014)
24. Lehtonen, M., Ostojic, D., Ilic, A., Michahelles, F.: Securing RFID systems by detecting tag cloning. In: Tokuda, H., Beigl, M., Friday, A., Brush, A.J.B., Tobe, Y. (eds.) Pervasive 2009. LNCS, vol. 5538, pp. 291–308. Springer, Heidelberg (2009). https://doi.org/10.1007/978-3-642-01516-8_20
25. Parno, B., Perrig, A., Gligor, V.: Distributed detection of node replication attacks in sensor networks. In: Proceedings of the IEEE Symposium on Security and Privacy, pp. 49–63 (2005)
26. Chan, H., Perrig, A., Song, D.: Random key predistribution schemes for sensor networks. In: Proceedings of the IEEE Symposium on Security and Privacy, pp. 197–213 (2003)
27. Msgna, M., Markantonakis, K., Mayes, K.: The B-Side of side channel leakage: control flow security in embedded systems. In: Zia, T., Zomaya, A., Varadharajan, V., Mao, M. (eds.) SecureComm 2013. LNICST, vol. 127, pp. 288–304. Springer, Cham (2013). https://doi.org/10.1007/978-3-319-04283-1_18

28. Carluccio, D., Lemke, K., Paar, C.: Electromagnetic side channel analysis of a contactless smart card: First results. http://www.iaik.tu-graz.ac.at/research/krypto/events/index.php
29. Zhang, M., Jha, N.K.: FinFET-based power management for improved DPA resistance with low overhead. ACM J. Emerg. Technol. Comput. Syst. **7**(3), 10 (2011)
30. Sundaresan, V., Rammohan, S., Vemuri, R.: Defense against side-channel power analysis attacks on microelectronic systems. In: Proceedings of the IEEE National Conference on Aerospace and Electronics, pp. 144–150 (2008)
31. Rieback, M.R., Crispo, B., Tanenbaum, A.S.: RFID guardian: a battery-powered mobile device for RFID privacy management. In: Boyd, C., González Nieto, J.M. (eds.) ACISP 2005. LNCS, vol. 3574, pp. 184–194. Springer, Heidelberg (2005). https://doi.org/10.1007/11506157_16
32. Kinoshita, S., Hoshino, F., Komuro, T., Fujimura, A., Ohkubo, M.: Low-cost RFID privacy protection scheme. IPS J. **45**(8), 2007–2021 (2004)
33. Peris-Lopez, P., Hernandez-Castro, J.C., Estevez-Tapiador, J.M., Ribagorda, A.: M2AP: a minimalist mutual-authentication protocol for low-cost RFID tags. In: Ma, J., Jin, H., Yang, L.T., Tsai, J.J.-P. (eds.) UIC 2006. LNCS, vol. 4159, pp. 912–923. Springer, Heidelberg (2006). https://doi.org/10.1007/11833529_93
34. Raza, S., Wallgren, L., Voigt, T.: SVELTE: real-time intrusion detection in the Internet of Things. Ad-hoc Netw. **11**(8), 2661–2674 (2013)
35. Shirai, T., Shibutani, K., Akishita, T., Moriai, S., Iwata, T.: The 128-bit blockcipher CLEFIA (Extended Abstract). In: Biryukov, A. (ed.) FSE 2007. LNCS, vol. 4593, pp. 181–195. Springer, Heidelberg (2007). https://doi.org/10.1007/978-3-540-74619-5_12
36. Bogdanov, A., et al.: PRESENT: An Ultra-lightweight Block Cipher. Springer, Heidelberg (2007). https://doi.org/10.1007/978-3-540-74735-2_31
37. Son, S., McKinley, K.S., Shmatikov, V.: Diglossia: detecting code injection attacks with precision and efficiency. In: Proceedings of the ACM SIGSAC Conference Computer Communications Security, pp. 1181–1192 (2013)
38. Salman, O.: Identity-based authentication scheme for the Internet of Things. In: Proceedings of the IEEE 21st Symposium on Computers and Communication (ISCC), Italy, pp. 1109–1111 (2016)
39. Nobakht, M., Sivaraman, V., Boreli, R.: A host-based intrusion detection and mitigation framework for smart home IoT using OpenFlow. In: Proceedings of the IEEE 11th International Conference on Availability, Reliability and Security (ARES), pp. 147–156 (2016)
40. Chakrabarty, S., Engels, D.W., Thathapudi, S.: Black SDN for the Internet of Things. In: Proceedings of the IEEE 12th International Conference on Mobile Ad Hoc and Sensor Systems (MASS), Dallas, USA, pp. 190–198 (2015)
41. Bull, P.: Flow based security for IoT devices using an SDN gateway. In: Proceedings of the IEEE 4th International Conference on Future Internet of Things and Cloud (FiCloud), Austria, pp. 157–163 (2016)
42. Flauzac, O.: SDN based architecture for IoT and improvement of the security. In: Proceedings of the IEEE 29th International Conference on Advanced Information Networking and Applications Workshops (WAINA), South Korea, pp. 688–693 (2015)
43. Gonzalez, C.: A novel distributed SDN-secured architecture for the IoT. In: Proceedings of the IEEE International Conference on Distributed Computing in Sensor systems (DCOSS), Washington, USA, pp. 244–249 (2016)

44. Bhunia, S.S., Gurusamy, M.: Dynamic attack detection and mitigation in IoT using SDN. In: 27th International Telecommunication Networks and Applications Conference (ITNAC). IEEE (2017)
45. Satasiya, D., Raviya, R., Kumar, H.: Enhanced SDN security using firewall in a distributed scenario. In: 2016 International Conference on Advanced Communication Control and Computing Technologies (ICACCCT). ISBN No. 978-1-4673-9545-8
46. Tselios, C., Politis, I., Kotsopoulos, S.: Enhancing SDN security for IoT-related deployments through Blockchain. In: IEEE NFV-SDN 2017 - Third International Workshop on Security in NFV-SDN,978-1-5386-3285-7/17. IEEE (2017)
47. IBM Corp.: Blockchain benefits for electronics - White Paper. https://public.dhe.ibm.com/common/ssi/ecm/gb/en/gbe03809usen/GBE03809USEN.PDF
48. Microsoft Corp.: Blockchain as a Service. https://azure.microsoft.com/en-us/solutions/blockchain/
49. The Linux Foundation: Hyperledger project. https://www.hyperledger.org/
50. Ericsson, Data-centric security. http://cloudpages.ericsson.com/data-centric-security-ebook
51. Citrix Systems Inc., Netscaler: Secure Event Delivery Controller
52. Sharma, P.K., Chen, M-Y., Park, J.H.: A software defined fog node based distributed blockchain cloud architecture for IoT. IEEE Access. https://doi.org/10.1109/ACCESS.2017.2757955
53. Duong, T., Fan, L., Zhou, H.S.: 2-hop blockchain: combining proof-of-work and proof-of-stake securely. In: IACR 2016, pp. 1–40 (2016)
54. Somasundaram, T.S., Kannan, G.: CLOUDRB: a framework for scheduling and managing high-performance computing (HPC) applications in science cloud. Future Gener. Comput. Syst. **34**, 47–65 (2014)
55. Sharma, P.K., Singh, S., Jeong, Y.-S., Park, J.H.: DistBlockNet: a distributed blockchains-based secure SDN architecture for IoT networks. IEEE Commun. Mag. **55**(9), 78–85 (2017)