A COMPREHENSIVE ANALYSIS ON IOT SECURITY

Gouri Shukla[1*], Krishna Nand Mishra[2], Sanjeev Kumar Trivedi[3], Neeraj Kumar Tiwari[4]

Article History: **Received: 15.04.2023** **Revised: 28.04.2023** **Accepted: 05.05.2023**

Abstract
The Internet of Things (IoT) has attracted a lot of interest recently since it has fundamentally altered human life. The IoT enables information exchange in numerous applications, including smart homes, healthcare, transportation, many more. These various application fields can be combined to form the concept of "smart life".Cybercriminals and security professionals are in a race as a result of the IoT quick development. Due of the communication and exchange of potentially sensitive information across billions of linked devices. Consequently, enhancing IoT security and protecting user privacy present significant challenges. In-depth research on IoT security is the goal of this study. After examining many IoT security assaults, a classification of the security conditionsbuilt on the goals of the incidents is suggested. Corresponding to the functionareas in which they are employed, recent security solutions are also described and organized into categories. Open research questions and security issues are argued as a conclusion.

Keywords: IoT, Security, Privacy, Smart life, Cyber-attacks.

[1*]Department of Computer Science, Radha Govind University, Ramgarh, Jharkhand (India), gouri07@gmail.com
[2]Department of Computer Science, Radha Govind University, Ramgarh, Jharkhand (India), knmishra24@gmail.com
[3]Department of Computer Science, Radha Govind University, Ramgarh, Jharkhand (India), sanjeevtrivedi13@gmail.com
[4]Babasaheb Bhimrao Ambedkar University (A Central University), neerajmtech@gmail.com

***Corresponding Author:** Gouri Shukla
*****Department of Computer Science, Radha Govind University, Ramgarh, Jharkhand (India), gouri07@gmail.com

DOI: - 10.48047/ecb/2023.12.Si6.745

1 Introduction

As of 1999, Kevin Ashton presented the idea of the IoT. Everything at any time, anywhere can be connected thanks to the IoT(Gubbi et al., (2013). IoT refers to physical objects that can range in size from extremely small to very large and link with one another via the Internet without requiring human interaction (Yan et al., 2014). IoT devices have actuators, which carry out tasks automatically and intelligently, and sensors, which collect data(Saif et al., 2015). Figure 1 depicts several examples of IoT devices.

With the expansion of wireless sensor networks, which have numerous uses, IoT breakthroughs have lately been made. A wide range of human endeavours, includes environmental surveillance, healthcare, sectors including smart grid, public health, and ITS (Intelligent Transportation System), can gain a great deal from the development and deployment of the IoT. The IoT is a vast collection of gadgets that are wired or wirelessly connected and feature sensors or, you might say, actuators. The IoT refers to a link between two physically distinct items (Dargad and Sutar, 2019). One of the key ideas is that we utilize and hear about new IoT-based technologies every day in our daily lives. According to Zhou (2010), the term "IoT" a number of information sensing techniques tools and technologies, including sensors, RFID, GPS, infrared sensors, laser scanners, and gas inductors. It gathers in real-time any process or item that needs to be tracked, connected, and engaged with. It gathers data on their different demand factors, such as geography, mechanics, chemistry, biology, sound, light, heat, and electricity.

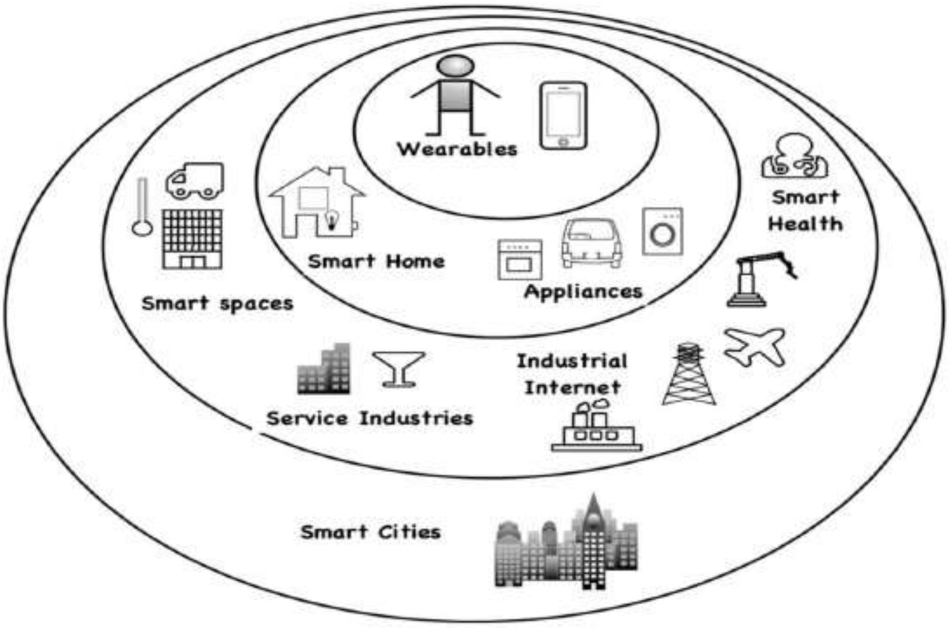

Figure 1 The application of IoT

It's anticipated that billions of gadgets will soon be online (Singh & Singh, 2015). As a result, the volume of data travelling via the Internet will expand (Borgohain et al., 2015). Eavesdropping and data modification are two security dangers to this data. As a result, the user's privacy will be jeopardised (Jing et al., 2014). An attacker, for example, could utilise to interrupt a baby monitor arrangement in order to violate the user's space (Cesare, 2014).

The IoT incorporates several currently used technologies, including cloud computing, constrained application protocol, wireless sensor network(WSN), and RFID. As a result, it inherits each technology's security weaknesses (Andrea et al., 2015). Fig. 2 depicts a few of the technologies that are now in use.

- A WSN is a collection of numerous physically placed independent sensors that are used to monitor and regulate the environment (Gubbi et al., 2013). The WSNs are vulnerable to a variety of assaults, including jamming, node tampering, sinkhole and wormhole attacks, etc. (Borgohain et al., 2015).
- RFID is used to recognize and track IoT things. It enables data sharing across a small distance using radio signals (Gubbi et al., 2013). Like the WSN, RFID technology is prone to spoofing, cloning, and sniffer attacks (Borgohain et al., 2015).

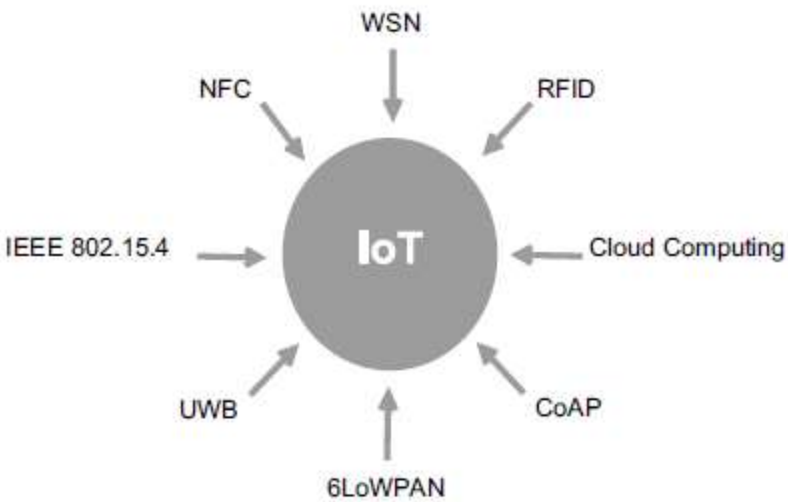

Figure 2 IoT enabling technologies.

- Using the cloud computing is essential to the IoT because it offers endless processing and storage capacity. (Botta *et al*., 2016).
- According to Al-Fuqaha et al. (2015), it provides low-energy connectivity for items in the personal area.

A variety of IoT systems, including payment and authentication, can use An example of a short-range technology is Near Field Communication (NFC). Data interchange and network access are made simple with NFC. However, it is vulnerable to information leakage because an attacker can intercept the wireless signal the device generates (Madlmayr et al., 2008; Curran et al., 2012).

IoT security is a difficult task. However, the majority of IoT devices are made to be compact and have constrained resources (such as battery, computing power, and storage). Conventional security procedures cannot be implemented since doing so would be extremely difficult and complex (Cole & Ranasinghe, 2008; Eisenbarth et al., 2007). The main difficulty is creating a lightweight security system for devices with tight constraints.

The examination of IoT security threats and vulnerabilities is presented in this research. Then, based on the goals of the attackers, we propose a taxonomy of the IoT security requirements. Additionally, we include numerous current security solutions and group them according to the application domains in which they are used. We conclude by talking about open research questions and IoT security difficulties.

2 Literature Review

Recently, several surveys on IoT security have been published. Not all of the worries were addressed, despite the fact that some of them were. All the IoT security issues have not been covered by any of

these polls. The provision of a safe IoT environment is the aim of this taxonomy. Table 1 compares the results of the surveys mentioned.

Sfar *et al*. (2018) outlined IoT security in a roadmap that considered privacy, trust, identification, and access management. They began by giving a methodical a cognitive strategy, to the IoT (Riahi *et al.*, 2014). The authors believed their vision was more practical and adaptable than the tiered strategy**.** They described the approach's components and relationships, as well as its effectiveness in smart manufacturing. After that, they discussed a taxonomy of current security issues, revealed useful fixes, and provided several research avenues. Finally, they demonstrated essential IoT security standardization actions. Although the study was intriguing, it only examined the security vulnerabilities that could arise from their approach's interactions and did not explore additional concerns with IoT security include integrity, confidentiality, and availability.

Mendez *et al*. (2017) talked about the security objectives of current IoT standards. They set a few security standards for IoT devices and data. They then discussed several technologies and protocols for the application, network, and perception that are supported by IoT levels. Numerous solutions were put out when the technologies' faults, such as those in WSN and RFID, were discovered. They prioritized data privacy, availability, and secrecy in terms of security. They also talked about security concerns and possible fixes. However, they avoided going into specifics concerning the shortcomings of the enabling technology. A study on the difficulties with security and privacy for IoT systems and applications was released by Yang *et al*. in 2017. There are four sections to their work. First, they looked at the two main computational and battery limits of IoT devices. Second, they provided an IoT attack classification based on (Andrea et al., 2015; Ronen & Shamir, 2016). Thirdly, the writers concentrated on IoT system topologies and methods for access verification and control. Then, it was looked into the security vulnerabilities at the network layer, transport layer, perception layer, and application layer. The authors of this article covered IoT security and privacy issues. However, they were only capable of access control and authentication. As a result, numerous important security issues were disregarded, including integrity, confidentiality, and privacy. Additionally, they didn't give adequate information regarding the IoT attacks.

In addition to describing the application, network, and perception levels, Chahid et al. (2017) also identified a few IoT security attacks. The authors then provided a few options put out by various businesses and organizations. They finally discussed potential directions as they put their efforts to rest. The authors researched current security practices in relation to IoT. However, they only provided a cursory definition of the security issues and did not offer any literature-based answers. Furthermore, a thorough discussion of the security measures was omitted.

Additionally, they didn't elaborate much on the potential security issues. Industry, healthcare, and smart homes were among the IoT applications covered by Razzaq *et al.* (2017). The main criteria for IoT security, such as authentication, access control, privacy, and secrecy, were then listed. They then homed in on security concerns, especially those that arise categorised these assaults into four categories depending on their outcomes and provided some viable remedies in a smart house. Additionally, most of the identified attacks were not described.

Table 1. Literature review on security concern

Authors	IoT Vision	Security Concern
Sfar *et al*. (2018)	The ecosystem of people, processes, intelligent objects, and technologies	Security, confidentiality, and authenticity
Mendez *et al*., (2017)	three levels: application, network, and perception	Confdentiality, reliability, accessibility, and privacy
Yang *et al*. (2017)	Perception, network, transport, and application are the four levels.	Authentication and access management
Oracevic *et al*. (2017)	Both tangible objects and digital objects	Confdentiality, authenticity and reliability
Alaba *et al*., (2017)	Perception, network, and application are the three layers	Identification, consent, confidentiality, and trust
Razzaq *et al*. (2017)	Not mentioned	Access control, confidentiality, privacy, and authentication

3. Security Risks with IoT

IoT devices and security breaches are both developing quickly. Analysing IoT vulnerabilities and attacks is a good place to start if you want to integrate security needs into IoT systems effectively. The objectives of various IoT security risks are examined in this section.

IoT devices are vulnerable to a range of assaults. Additionally, we point out that the major objectives of various attacks are as follows:

·Having access to confidential or sensitive data.

• Manage the conversation.

4.1 Data Security

There are other security threats, though, including data modification and eavesdropping. In the IoT environment, we must safeguard the data's integrity, confidentiality, and privacy.

Data confidentiality is a method of preventing unauthorised IoT devices from accessing private data. According to (Miorandi et al., 2012), data confidentiality is a crucial issue that demands a lot of attention. Due to the constrained resources of IoT devices, the IoT system cannot directly use standard encryption algorithms (Alam et al., 2011). (Babar et al., 2011) recommended using simple cryptographic techniques to provide data security and confidentiality. According to Weber (2015), applying privacy-based designs can increase levels of secrecy. Privacy, according to Misra et al. (2017), includes the choice to conceal personal information and to select its intended usage. The collection, transmission, and storage of data must take data privacy into account.

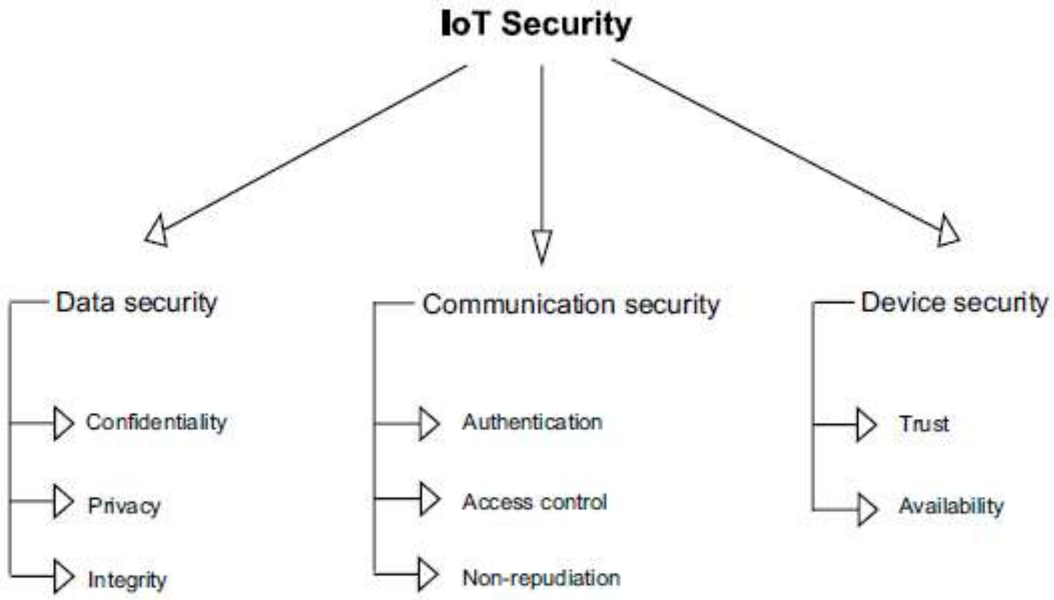

Figure 3 IoT Security Taxonomy

Many viable options for dealing with data privacy have been proposed. Among these methods are stream and block cyphers, anonymization, and pseudo-random number generators(Sfar et al., 2018).

• Solutions based on anonymization, such as T-closeness (Li et al., 2006), L-diversity, and K-anonymity (Sweeney, 2002).

4.2 Communication Security

Authentication prevents communication declines and ensures that only authorised individuals may access IoT devices.

A newly connected device should authenticate itself with the network before delivering data. Authentication can be verified using, lightweight cryptographic approaches (Abyaneh, 2012).

• According to Attribute-Based Access Control (ABAC), in order to access a resource or certain data, a user must provide the relevant attributes (Sfar et al., 2018).

4.3 Device Security

Making ensuring that interacting nodes can trust and believe in one another is a vital task in providing security in a critical environment. IoT device accessibility is also required. As previously indicated, trust is crucial for IoT users (Coetzee et al., 2018). The process of choosing which unknown entities to communicate with is known as trust management. It is crucial to communicate with reputable IoT devices in order to safeguard IoT systems and stop rogue nodes from acting in an undesirable way. Deterministic and non-deterministic trust are the two primary categories of trust management systems, according to (Sfar et al.,

2018). Systems based on suggestions, reputation, predictions, and social networks fall under nondeterministic trust, whereas policy-based and certificate-based processes go under deterministic trust.

5 IoT Security Solutions

We list a few recent recommendations for securing the IoT across several application areas in this section.

a framework for data security and authentication for Internet of Things gadgets. It uses both symmetric and asymmetric key encryption, and Regev's (2009) Learning With Errors (LWE) method is used to build the key pair.

Li et al. (2017) emphasised joint validation in Smart City functions, which calls for sensors and servers to work together to seek permission before switching data. The suggested method performs well with low-resource devices utilised in Smart City applications. There are several other approaches available to boost IoT security across a variety of application industries. However, it's significantly more challenging to offer lightweight security.

Security Challenges

In IOT applications or systems, security agencies should be applied to ensure the integrity of that data while packets are transferred through various devices and connections in order to reach the target recipient over the internet. Moreover, the majority of IOT devices are high-power devices, making it impossible to apply the previously proposed cryptographic approach in the IOT context. The integration of any application into network infrastructures is now solely concerned with obtaining functionality rather than taking into account its security, which is the most crucial component of any system or application throughout the planning stage. Also, this creates a backdoor for the adversaries and attackers. Hence, it makes it feasible for such applications and systems to be hacked. As previously said, cyber security professionals have issued warnings that IOT is one of the most vulnerable technologies and is anticipated to see significantly more focused assaults compared to the present and developing infrastructures. For instance, data theft, system damage or bodily injury, denial-of-service attacks, and certain ransomware for smart watches, smart automobiles, and smart homes. For each IOT system or application, there are four key security problems.

(1) Trillion points of vulnerability:
Everymachine that connects to the IoT represents a potential risk, and when these risks materialize, they immediately raise the question of how confidently an organization can rely on the collected data and its integrity. When it comes to such danger, this is a subject that is frequently on everyone's mind.

(2) Trust and Data integrity
This is done to verify that the data hasn't been altered between the time it leaves the senders' computers and the time it reaches the intended recipient, or, to put it another way, till it reaches its destination. In order to confirm the data's integrity and to validate its verification certificate, it also participates in the data verification process.

(3) Data protection:
It is the law that must be intended in order to safeguard the data or to govern the personal and organisational data that has been gathered by the application or by the sensors and has been saved as part of filing system.

(4). Data privacy:
The protection of data from exposure in the context of IOT systems or applications is data privacy. For instance, every logical or physical item may be assigned a network address that is completely unique. Such objects or entities would also be granted the capacity to communicate through a network.

6 Discussion and Conclusion

The amount of data is growing along with the increase of IoT devices. For the IoT to develop into a secure infrastructure, it must address several security flaws that plague this expansion. Additionally, intelligent object design should progress towards increased autonomy in identifying hazards and responding to them. To allow devices to identify trustworthy nodes in a vibrant, diversified, and comprehensive ecosystem, adaptive beliefpatterns are needed. In these networks, efficient significant management should be contemplated. We looked at attacks and IoT security weaknesses. After that, depending on the goals of the attacks, we developed a taxonomy of IoT security requirements. This nomenclature can help researchers and developers create fresh security measures for the IoT. Additionally, we reviewed some of the most recent security solutions that have been put forth for specific IoT application categories. Finally, we contend that several security issues are raised by the increase of IoT. The major challenge is coming up with capable and flexible protection measures for machines with restricted resources.

References

1. Alaba, F. A., Othman, M., Hashem, I. A. T., & Alotaibi, F. (2017). Internet of Things security: A survey. *Journal of Network and Computer Applications*, *88*, 10-28.
2. Andrea, I., Chrysostomou, C., & Hadjichristofi, G. (2015, July). Internet of Things: Security vulnerabilities and challenges. In *2015 IEEE symposium on computers and communication (ISCC)* (pp. 180-187). IEEE.
3. Alam, S., Chowdhury, M. M., & Noll, J. (2011). Interoperability of security-enabled internet of things. *Wireless Personal Communications*, *61*, 567-586.
4. Atzori, L., Iera, A., & Morabito, G. (2010). The internet of things: A survey. *Computer networks*, *54*(15), 2787-2805.
5. Abyaneh, M. R. S. (2012). Security analysis of lightweight schemes for RFID systems.
6. Bogdanov, A., Knežević, M., Leander, G., Toz, D., Varıcı, K., & Verbauwhede, I. (2011). SPONGENT: A lightweight hash function. In *Cryptographic Hardware and Embedded Systems–CHES 2011: 13th International Workshop, Nara, Japan, September 28–October 1, 2011. Proceedings 13* (pp. 312-325). Springer Berlin Heidelberg.
7. Babar, S., Stango, A., Prasad, N., Sen, J., & Prasad, R. (2011, February). Proposed embedded security framework for internet of things (iot). In *2011 2nd International*

Conference on Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronic Systems Technology (Wireless VITAE) (pp. 1-5). IEEE.
8. Botta, A., De Donato, W., Persico, V., & Pescapé, A. (2016). Integration of cloud computing and internet of things: a survey. *Future generation computer systems*, *56*, 684-700.
9. Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. (2015). Internet of things: A survey on enabling technologies, protocols, and applications. *IEEE communications surveys & tutorials*, *17*(4), 2347-2376.
10. Bormann, C., Castellani, A. P., & Shelby, Z. (2012). Coap: An application protocol for billions of tiny internet nodes. IEEE Internet Computing, 16(2), 62.
11. Borgohain, T., Kumar, U., & Sanyal, S. (2015). Survey of security and privacy issues of internet of things. *arXiv preprint arXiv:1501.02211*.
12. Bouij-Pasquier, I., Ouahman, A. A., Abou El Kalam, A., & de Montfort, M. O. (2015, November). SmartOrBAC security and privacy in the Internet of Things. In *2015 IEEE/ACS 12th International Conference of Computer Systems and Applications (AICCSA)* (pp. 1-8). IEEE
13. Curran, K., Millar, A., & Mc Garvey, C. (2012). Near field communication. *International Journal of Electrical and Computer Engineering*, *2*(3), 371.
14. Cole, P. H., & Ranasinghe, D. C. (2008). Networked RFID systems and lightweight cryptography. *London, UK: Springer. doi*, *10*, 978-3.
15. Chahid, Y., Benabdellah, M., & Azizi, A. (2017, November). Internet of things protocols comparison, architecture, vulnerabilities and security: State of the art. In *Proceedings of the 2nd International Conference on Computing and Wireless Communication Systems* (pp. 1-6).
16. Cesare, S. (2014). Breaking the security of physical devices. *Presentation at Blackhat*, *14*.
17. Coetzee, L., Oosthuizen, D., & Mkhize, B. (2018, May). An analysis of CoAP as transport in an Internet of Things environment. In *2018 IST-Africa Week Conference (IST-Africa)* (pp. Page-1). IEEE.
18. Dennis, J. B., & Van Horn, E. C. (1966). Programming semantics for multiprogrammed computations. *Communications of the ACM*, *9*(3), 143-155.
19. Eisenbarth, T., Kumar, S., Paar, C., Poschmann, A., & Uhsadel, L. (2007). A survey of lightweight-cryptography implementations. *IEEE Design & Test of Computers*, *24*(6), 522-533.
20. Fan, J., Batina, L., & Verbauwhede, I. (2009). HECC goes embedded: an area-efficient implementation of HECC. In *Selected Areas in Cryptography: 15th International Workshop, SAC 2008, Sackville, New Brunswick, Canada, August 14-15, Revised Selected Papers 15* (pp. 387-400). Springer Berlin Heidelberg.
21. Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. *Future generation computer systems*, *29*(7), 1645-1660.
22. Gusmeroli, S., Piccione, S., & Rotondi, D. (2013). A capability-based security approach to manage access control in the internet of things. *Mathematical and Computer Modelling*, *58*(5-6), 1189-1205.
23. Hossain, M. M., Fotouhi, M., & Hasan, R. (2015, June). Towards an analysis of security issues, challenges, and open problems in the internet of things. In *2015 ieee world congress on services* (pp. 21-28). IEEE.
24. Hell, M., Johansson, T., & Meier, W. (2007). Grain: a stream cipher for constrained environments. *International journal of wireless and mobile computing*, *2*(1), 86-93.
25. Jing, Q., Vasilakos, A. V., Wan, J., Lu, J., & Qiu, D. (2014). Security of the Internet of Things: perspectives and challenges. *Wireless Networks*, *20*, 2481-2501.
26. Koblitz, N., Menezes, A., & Vanstone, S. (2000). The state of elliptic curve cryptography. *Designs, codes and cryptography*, *19*, 173-193.
27. Kasinathan, P., Pastrone, C., Spirito, M. A., & Vinkovits, M. (2013, October). Denial-of-Service detection in 6LoWPAN based Internet of Things. In *2013 IEEE 9th international conference on wireless and mobile computing, networking and communications (WiMob)* (pp. 600-607). IEEE.
28. Li, N., Li, T., & Venkatasubramanian, S. (2006, April). t-closeness: Privacy beyond k-anonymity and l-diversity. In *2007 IEEE 23rd international conference on data engineering* (pp. 106-115). IEEE.
29. Li, F., Hong, J., & Omala, A. A. (2017). Efficient certificateless access control for

industrial Internet of Things. Future Generation Computer Systems, 76, 285.
30. Li, R., Song, T., Capurso, N., Yu, J., Couture, J., & Cheng, X. (2017). IoT applications on secure smart shopping system. *IEEE Internet of Things Journal*, *4*(6), 1945-1954.
31. Li, N., Liu, D., & Nepal, S. (2017). Lightweight mutual authentication for IoT and its applications. *IEEE Transactions on Sustainable Computing*, *2*(4), 359-370.
32. Liu, J., Xiao, Y., & Chen, C. P. (2012). Internet of things' authentication and access control. *International Journal of Security and Networks*, *7*(4), 228-241.
33. Madlmayr, G., Langer, J., Kantner, C., & Scharinger, J. (2008, March). NFC devices: Security and privacy. In *2008 Third International Conference on Availability, Reliability and Security* (pp. 642-647). IEEE.
34. Mendez, D. M., Papapanagiotou, I., & Yang, B. (2017). Internet of things: Survey on security and privacy. *arXiv preprint arXiv:1707.01879*.
35. Mo, Y., & Sinopoli, B. (2009, September). Secure control against replay attacks. In *2009 47th annual Allerton conference on communication, control, and computing (Allerton)* (pp. 911-918). IEEE.
36. Miorandi, D., Sicari, S., De Pellegrini, F., & Chlamtac, I. (2012). Internet of things: Vision, applications and research challenges. *Ad hoc networks*, *10*(7), 1497-1516.
37. Misra, S., Krishna, P. V., Agarwal, H., Saxena, A., & Obaidat, M. S. (2011, October). A learning automata based solution for preventing distributed denial of service in internet of things. In *2011 international conference on internet of things and 4th international conference on cyber, physical and social computing* (pp. 114-122). IEEE.
38. Misra, S., Maheswaran, M., & Hashmi, S. (2017). *Security challenges and approaches in internet of things*. Cham: Springer International Publishing.
39. Mace, F., Standaert, F. X., & Quisquater, J. J. (2007, July). ASIC implementations of the block cipher sea for constrained applications. In *Proceedings of the Third International Conference on RFID Security-RFIDSec* (Vol. 2007, pp. 103-114).
40. Mahalle, P. N., Anggorojati, B., Prasad, N. R., & Prasad, R. (2013). Identity authentication and capability based access control (iacac) for the internet of things. *Journal of Cyber Security and Mobility*, *1*(4), 309-348.
41. Oracevic, A., Dilek, S., & Ozdemir, S. (2017, May). Security in internet of things: A survey. In *2017 international symposium on networks, computers and communications (ISNCC)* (pp. 1-6). IEEE.
42. Oriwoh, E., al-Khateeb, H., & Conrad, M. (2016). Responsibility and Non-repudiation in resource-constrained Internet of Things scenarios. International Conference on Computing and Technology Innovation (CTI 2015).
43. Pathan, A. S. K., Lee, H. W., & Hong, C. S. (2006, February). Security in wireless sensor networks: issues and challenges. In *2006 8th International Conference Advanced Communication Technology* (Vol. 2, pp. 6-pp). IEEE.
44. Peris-Lopez, P., Hernandez-Castro, J. C., Estevez-Tapiador, J. M., & Ribagorda, A. (2009). LAMED—a PRNG for EPC class-1 generation-2 RFID specification. *Computer Standards & Interfaces*, *31*(1), 88-97.
45. Perrig, A., Stankovic, J., & Wagner, D. (2004). Security in wireless sensor networks. Communications of the ACM, 47(6), 53
46. Razzaq, M. A., Gill, S. H., Qureshi, M. A., & Ullah, S. (2017). Security issues in the Internet of Things (IoT): A comprehensive study. International Journal of Advanced Computer Science and Applications, 8(6), 383
47. Riahi, A., Natalizio, E., Challal, Y., Mitton, N., & Iera, A. (2014, February). A systemic and cognitive approach for IoT security. In *2014 International conference on computing, networking and communications (ICNC)* (pp. 183-188). IEEE.
48. Ronen, E., & Shamir, A. (2016, March). Extended functionality attacks on IoT devices: The case of smart lights. In *2016 IEEE European Symposium on Security and Privacy (EuroS&P)* (pp. 3-12). IEEE.
49. Rghioui, A., Khannous, A., & Bouhorma, M. (2014). Denial-of-Service attacks on 6LoWPAN-RPL networks: Threats and an intrusion detection system proposition. *Journal of Advanced Computer Science & Technology*, *3*(2), 143.
50. Regev, O. (2009). On lattices, learning with errors, random linear codes, and cryptography. *Journal of the ACM (JACM)*, *56*(6), 1-40.
51. Saif, I., Peasley, S., & Perinkolam, A. (2015). Safeguarding the Internet of Things: being secure, vigilant, and resilient in the connected age. Deloitte Rev 17.

52. Sfar, A. R., Natalizio, E., Challal, Y., & Chtourou, Z. (2018). A roadmap for security challenges in the Internet of Things. *Digital Communications and Networks*, *4*(2), 118-137.
53. Singh, S., & Singh, N. (2015, October). Internet of Things (IoT): Security challenges, business opportunities & reference architecture for E-commerce. In *2015 International conference on green computing and internet of things (ICGCIoT)* (pp. 1577-1581). Ieee.
54. Singh, J., Pasquier, T., Bacon, J., Ko, H., & Eyers, D. (2015). Twenty security considerations for cloud-supported Internet of Things. *IEEE Internet of things Journal*, *3*(3), 269-284.
55. Sweeney, L. (2002). k-anonymity: A model for protecting privacy. *International journal of uncertainty, fuzziness and knowledge-based systems*, *10*(05), 557-570.
56. Sheng, Z., Yang, S., Yu, Y., Vasilakos, A. V., McCann, J. A., & Leung, K. K. (2013). A survey on the ietf protocol suite for the internet of things: Standards, challenges, and opportunities. *IEEE wireless communications*, *20*(6), 91-98.
57. Suo, H., Wan, J., Zou, C., & Liu, J. (2012, March). Security in the internet of things: a review. In *2012 international conference on computer science and electronics engineering* (Vol. 3, pp. 648-651). IEEE.
58. Song, T., Li, R., Mei, B., Yu, J., Xing, X., & Cheng, X. (2017). A privacy preserving communication protocol for IoT applications in smart homes. *IEEE Internet of Things Journal*, *4*(6), 1844-1852.
59. Ullah, S., Ali, M., Hussain, A., & Kwak, K. S. (2009). Applications of UWB technology. *arXiv preprint arXiv:0911.1681*.
60. Vermesan, O., & Friess, P. (Eds.). (2013). *Internet of things: converging technologies for smart environments and integrated ecosystems*. River publishers.
61. Weber, R. H. (2015). Internet of things: Privacy issues revisited. *Computer Law & Security Review*, *31*(5), 618-627.
62. Yan, Z., Zhang, P., & Vasilakos, A. V. (2014). A survey on trust management for Internet of Things. Journal of Network and Computer Applications, 42, 120
63. Yang, Y., Wu, L., Yin, G., Li, L., & Zhao, H. (2017). A survey on security and privacy issues in Internet-of-Things. *IEEE Internet of things Journal*, *4*(5), 1250-1258.
64. Yang, Y., Zheng, X., & Tang, C. (2017). Lightweight distributed secure data management system for health internet of things. *Journal of Network and Computer Applications*, *89*, 26-37.
65. Zhao, K., & Ge, L. (2013). In 2013 9th International conference on computational intelligence and security (CIS) (pp. 663–667). IEEE