ARTICLE IN PRESS

Materials Today: Proceedings xxx (xxxx) xxx

Contents lists available at ScienceDirect

Materials Today: Proceedings

journal homepage: www.elsevier.com/locate/matpr

An investigation of various security and privacy issues in Internet of Things

Richa Singhai *, Rama Sushil

Department of Computer Science and Engineering, Dit University, Dehradun, India

ARTICLE INFO

Article history:
Available online xxxx

Keywords:
Internet of Things
Security
Privacy
Attacks
Threats

ABSTRACT

IoT enables the smart cities worldwide model. Smart houses, smart farming, smart surroundings, smart fitness, smart government, etc., are all kinds of intelligent communities. IoT is also used in the oil refining, gas mining and manufacturing sectors. IoT improving efficiency, optimizing prices, maximizes energy, maintaining predictions, and providing a great deal of convenience for people. Security risks are growing with increasingly heterogeneous systems and data processing. The main reasons for preventing IoT from flourishing are security and privacy issues. This paper contains an investigation of various security and privacy issues in Internet of Things.

Selection and peer-review under responsibility of the scientific committee of the International Conference on Nanoelectronics, Nanophotonics, Nanomaterials, Nanobioscience & Nanotechnology.

1. Introduction

One of the most spectacular pheasants of the last decade is the word "Internet of Things." It took advantage of Kevin Ashton's management in the supply chain for the first time at a presentation in 1999. Ashton argues that we have to seriously rethink the "material" nature of the way we communicate and live in the physical world, due to developments in computers, Internet and the generation of data from intelligent devices. He was then Executive Director at MIT's Auto-ID Centre, where he helped expand RFID implementations on wider realms that formed the basis for the current vision of IoT.

By expanding numerous web-related products and gadgets, they are used in the real world to discuss and render people. The word "Internet of things (IoT),' in Forbes magazine, was quoted by Kevin Ashton, Radio Frequency Identification (RFID) individual [1]. IoT is a structure framed by physical things and widely referred to in formal ways as elements that speak to one another. Objects can be anything we meet daily and are linked to a user application through the internet as shown. But gadgets like paper, style, key, garments can be used daily, etc. Objects are necessarily not electronic gadgets.

[2] The writer referred to the possibility of making papers recognizable, efficiently accessible, localizable and useful for communication methods such as internet, LAN, WAN, RFID, or sensors.

The key purpose of IoT is to collect information from users allowed to use the functionality of wireless networks. An approximate 50 billion intelligent things are to part of IoT by 2020, according to a survey [3]. By 2020 Different organisations and working groups today rely on IoT such as Samsung, Apple, Thread Alliance, and so on. Samsung has released the smart home kits for various modules with the same application [4], according to Dr.news Hong's release. Below Fig. 1 gives a clear understanding of IoT architecture.

For instance, if nobody in your room automatically switches lights and AC off, the lights or the AC or refrigerator will be monitored. The use of the alarm is raised when someone breaks the door or glass of the house. For these movement sensors, the user's movement is regulated.

In 2017 the Technology Consultancy company Gartner, Inc. predicts that 8.4 trillion linked things will be used globally, up 31% from 2016, and that IoT will be prepared to change the way we operate and live; better electricity, water, transport and safety management and to link people together. And it is projected that by 2022 this figure will rise to almost 50 billion. It is a breakup of security and privacy if one factor will slow the broader acceptance of IoT technology.

2. IoT enabling technologies

In the advent of IoT, there are many technologies. The key building blocks of today's IoT life are considered. Identifying, locating,

* Corresponding author.
E-mail address: btirtjs@gmail.com (R. Singhai).

https://doi.org/10.1016/j.matpr.2021.07.259
2214-7853/© 2021 Elsevier Ltd. All rights reserved.
Selection and peer-review under responsibility of the scientific committee of the International Conference on Nanoelectronics, Nanophotonics, Nanomaterials, Nanobioscience & Nanotechnology.

Please cite this article as: R. Singhai and R. Sushil, An investigation of various security and privacy issues in Internet of Things, Materials Today: Proceedings, https://doi.org/10.1016/j.matpr.2021.07.259

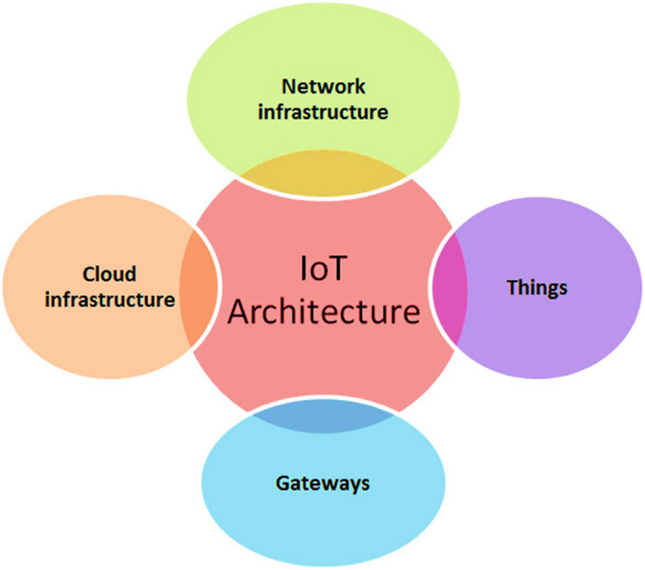

Fig. 1. Basic IoT Architecture.

sensing and IP technology for the projected large number of devices, as well as technologies allowing small devices to connect on internet with other organizations. In this segment, some of the core technologies for IoT are highlighted.

2.1. Radio frequency identification

One of the main enablers of IoT is radio frequency identification (RFID). To connect and communicate with small objects, a specific framework and in real-time monitoring, RFID or, at times, an RFID tag is required. It is a very small microchip with an antenna for target identification and tracking. The RFID reader reads the data that is contained in the RFID tag without having to be online-of-view [5,6].

2.2. Internet protocol version 6 (IPV6)

The estimated number of IoT devices attached is enormous. Present IPV4 addresses are 32-bit, so 4.3 billion IP addresses can be supported. But addresses are mostly used so that the planned trillions of IoT devices cannot be accommodated [7]. IPV6 was created to enhance the amount of IP addresses available with a significantly greater space using 128-bit address formats that can include 3.4 × 1038 addresses to define the objects used to participate in the IoT environment [8]. Therefore, all things in the network can be assigned an IPv6 address. A single IP address should be sent to each device.

2.3. Wireless sensor networks

The sensor nodes, usually "feel" (gather physical data), "think" (process data and make informed decisions) and "talk" (communicate with other individuals through a wireless channel) [9] have advanced substantially in recent years; a fundamental aspect of WSNs lies in the sensor nodes. This sensor knots are incorporated in objects that mean the knowledge surrounding things like weather environments, movement, and so on. This information will also allow proper intervention and sensor knots (electronic or non-electronic, e.g., machines, foodstuffs, automobiles, lamps, chairs, doors) to make their environment known.

For instance, cooler will notify whether food is required, intelligent lights report the light state, intelligent locks report whether or not doors are locked. Stuff are made alive by sensors and conscious of their environments.

2.4. IPv6 low power personal area networks (6LoWPAN)

Incompatibility of packet size between IPv6 and restricted networks, for example, IPv6 requires at least 1028 bytes of packet size, while packet size 803.15.4 requires a maximum of 128 bytes, so the IETF has developed an adaptation layer for IPv6 links to network layers called 6LoWPAN to overcome such a problem. However, 6LoWPAN specified the RFC 6282 RFC 4919 [11] and RFC 4944 [12] protocols and mechanics that allow IoT devices to be incorporated into IPv6 networks.

3. Security and privacy in the IoT

The specifications of IoT protection vary from those of other systems. IoT combines the physical system with cyber world, which constitutes a new challenge [13,14]; it interconnects heterogeneous smart devices with a vast volume of data generated by the numbers of connected devices in billions. In addition, most IoT devices have limited resource space, limited memory and limited resources, thereby reducing the use of conventional protection solutions for such low-capacity devices. Moreover researchers are proposing various protocols in the field of healthcare [27–29] and vehicle communication [33–39] to protect the information exchanged among various devices to devices.

The high-level security goals were described as data integrity, availability and confidentiality by National Institute of Standards and technology (NIST). To accomplish these objectives, Mechanisms such as encryption, authentication, access control or key management are used. The safety conditions for IoT properties are, however, the following [23–26], Fig. 2 shows a clear understanding of IoT related privacy and Security concerns.

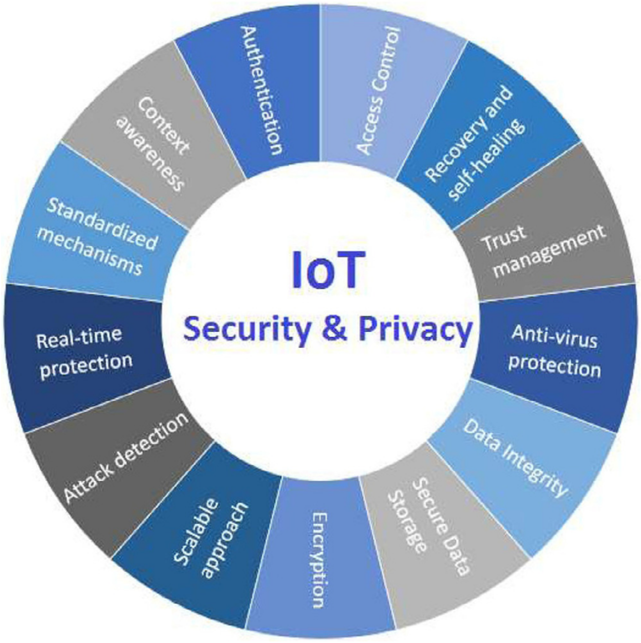

Fig. 2. IoT Security & Privacy Framework.

3.1. Confidentiality

In the context of IoT, data secrecy is of the utmost importance since it guarantees the reliable transfer of data. In the field of Internet transmission, technologies such as TLS [15], IPsec [16] are used, but the overall cost of these methods exceeds IoT systems, which have resource constraints. The main sensitivity to secrecy, however, is communicated, stored, located / tracked, and identified in the IoT context [17].

3.2. Data integrity

Data integrity guarantees the data is not corrupted or changed during transfer by an unauthorized party. IoT Wireless Medium and network style LLNs cause huge data errors and exploit data-modification attackers. Integrity can be accomplished by adding a checksum or (MIC) message integrity code [18] for any packet.

3.3. Availability

Disposability is a computer or the whole system's ability to provide the data and resources provided if necessary. It is difficult to make available the existence of IoT network LLNs and the presence of confined machines in the network. It takes advantage of attackers to execute attacks like DoS against the network. While strong security measures such as classical security mechanisms increase the protection of the network and equipment, it also affects network availability.

Following the high overheads induced by these mechanisms on the restricted devices, contact is delayed, and the time of calculation is also delayed which results in the transfer time, leading to battery depletion used on devices which eventually affect the network availability.

3.4. Authenticity

In IoT, authentication is designed to ensure that the communication parties are identical as objects interact with or include a human being they must be legally allowed and not be authorized to obtain access to the properties of unauthorized individuals.

4. Security and privacy challenges in IoT

In the following section we are presenting these problems because of the special features of IoT, security challenges vary from traditional network security [20–22,30–32].Underneath a block diagram has been demonstrated to provide a deep understanding of IoT security challenges in Fig. 3.

4.1. Heterogeneous devices and communication

The design of IoT's network of physical devices integrated with the cyber world means the variety of devices from the small sensor system to larger devices, such as servers, since devices are built by various vendors of different architectures that support different software and hardware specifications. For instance, IP-based safety solutions like IPsec, SSL and SSH cannot be used on constrainted devices, such as sensors that leave a whole class of devices unsecured that threaten the whole network [19]. This is not the case in the context of conventional protection mechanisms.

4.2. Integrating physical devices

The attacker will be able to communicate more than before, if an attacker breaks the home protection, he is able to manipulate the illumination system, lock the door controls TV sets, etc. the attacker may think of an intelligent home where he controls everything remotely. Engagement of physical equipment raises the probability of violations of protection in the latest survey, a mobile computer such as Smart TVs and baby monitors, manipulating physical machines by attackers, has seen 25% of the total botnet. The results are recorded. An intruder, for instance, might compromise the lights of an intelligent home or endanger the lives of the population and cause enormous financial losses for the whole city.

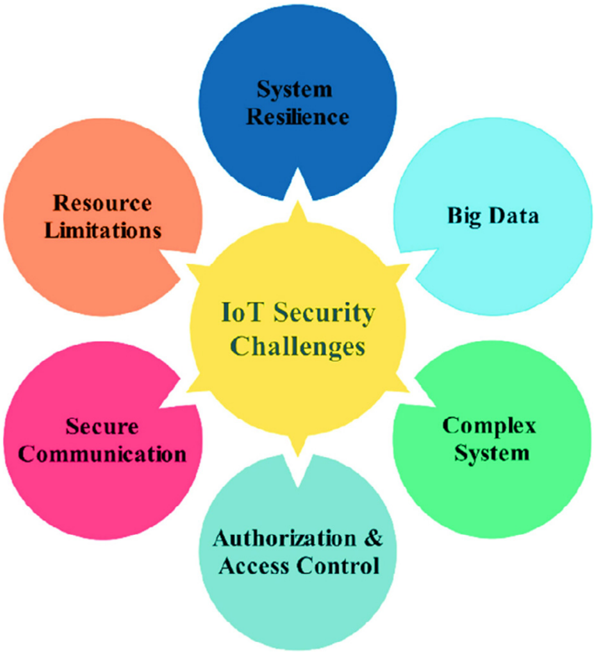

Fig. 3. Primary IoT security Challenges.

4.3. Constrained devices

Manufacturers of IoT devices have a tendency to reduce the cost of production and development, resulting in IoT devices having limited resources, small memory space, limited energy and low bandwidth; these stringent characteristics considerably reduce the security solutions and make conventional security techniques unapplicable.

But some IoT devices have only minimal batterical energy available for execution of planned functionality and heavy security instructions for cryptographic algorithms which can drain the battery from the devices in outdoor or hostile environments.

4.4. Large scale

There are currently more computers wired to the Internet than human beings on the globe. This figure is expected to rise substantially by 50 billion by 2020.Furthermore, the management of the large number of intelligent devices would inevitably raise the security risks.

4.5. Privacy

The idea of IoT's Ubiquitous Computing makes IoT physical devices communicate seamlessly with Internet infrastructure via various wireless connectivity technologies. IoT allows anywhere to be interacted, generating a large volume of data generated by IoT devices and using a wide range of applications to challenge pri-

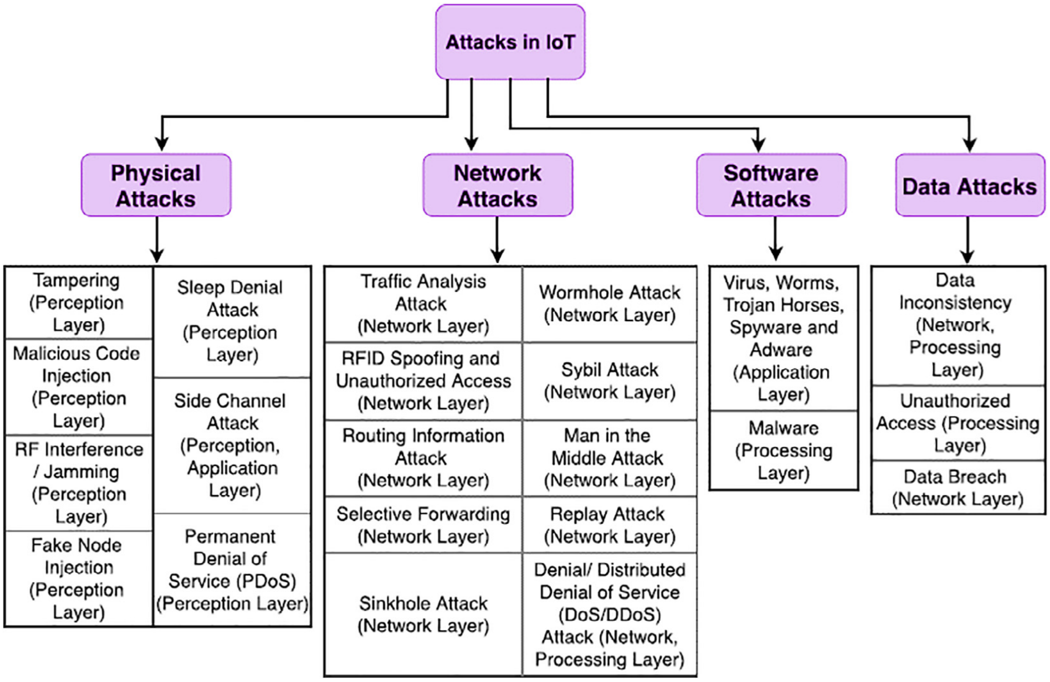
Attacks in IoT
Physical Attacks
Network Attacks
Software Attacks
Data Attacks
Tampering (Perception Layer)
Malicious Code Injection (Perception Layer)
RF Interference / Jamming (Perception Layer)
Fake Node Injection (Perception Layer)
Sleep Denial Attack (Perception Layer)
Side Channel Attack (Perception, Application Layer)
Permanent Denial of Service (PDoS) (Perception Layer)
Traffic Analysis Attack (Network Layer)
RFID Spoofing and Unauthorized Access (Network Layer)
Routing Information Attack (Network Layer)
Selective Forwarding (Network Layer)
Sinkhole Attack (Network Layer)
Wormhole Attack (Network Layer)
Sybil Attack (Network Layer)
Man in the Middle Attack (Network Layer)
Replay Attack (Network Layer)
Denial/ Distributed Denial of Service (DoS/DDoS) Attack (Network, Processing Layer)
Virus, Worms, Trojan Horses, Spyware and Adware (Application Layer)
Malware (Processing Layer)
Data Inconsistency (Network, Processing Layer)
Unauthorized Access (Processing Layer)
Data Breach (Network Layer)

Fig. 4. Different Attacks in IoT.

vacy in IoT. Millions of heterogeneous networks in diverse and dispersed areas would certainly increase the risk of privacy.

Important and private information, which exploit attackers to use such information to infringe privacy, is exchanged for applications such as the Smart home or remote smart health care. In addition, information on locating certain critical nodes in the network, such as the source node and sink node position, which can be used by eavesdroppers to develop other attacks that threaten certain nodes or events. Some significant attack has been shown in Fig. 4.

5. Conclusion

In various real-world implementations, IoT saves life and costs. By continuous data collection and evaluation, IoT allows one to forecast the future. There are also some questions and problems in IoT. IPV6 would be essential for IoT interface addressing in the near future. IoT application needs to be able to handle Large Data and vast amounts of data, with the IoT community growing even more.

Major IoT challenges, including anonymity and identity, will also be addressed. In the near future, the analysis will help researchers create an extremely stable IoT health care infrastructure by reducing different issues and obstacles.

These identified security challenges can be recognized in prospective work with recent vulnerabilities. An appropriate protection policy can then be established to eliminate vulnerabilities. This may be further extended to construct a full security model for the IoT environment.

CRediT authorship contribution statement

Richa Singhai: Conceptualization, Data curation, Formal analysis, Funding acquisition, Investigation, Methodology, Project administration. **Rama Sushil:** Resources, Software, Supervision, Validation, Visualization, Writing - original draft, Writing - review & editing.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

[1] C.R. Schoenberger, The internet of things, Forbes Magazine, Mar. (2002).
[2] European Commission, Internet of Things in 2020: A roadmap for the future, 2008.
[3] R. Morabito, V. Cozzolino, A.Y. Ding, N. Beijar, J. Ott, Consolidate IoT edge computing with lightweight virtualization, IEEE Network 32 (1) (2018) 102–111.
[4] Dr. Hong, Internet of Things is now, In sync with real life, 2016.
[5] A. Juels, RFID security and privacy: a research survey, IEEE J. Selected Areas Commun. 24 (2) (2006) 381–394.
[6] Song, Boyeon, Chris J. Mitchell. Scalable RFID pseudonym protocol. Network and System Security, 2009. NSS'09. Third International Conference on. IEEE, 2009.
[7] S. Agrawal, D. Vieira, A survey on Internet of Things, Abakós 1 (2) (2013) 78–95.
[8] Van Kranenburg, Rob, et al. The internet of things. Proc. of the First Berlin Symposium on Internet and Society, 2011.
[9] Jianguo Ma, Internet-of-Things: Technology evolution and challenges. Microwave Symposium (IMS), 2014 IEEE MTT-S International, IEEE, 2014.
[11] https://tools.ietf.org/html/rfc4919.
[12] https://tools.ietf.org/html/rfc4944.
[13] Feng, Hailong, Wenxiu Fu. Study of recent development about privacy and security of the internet of things. Web Information Systems and Mining (WISM), 2010 International Conference on. Vol. 2. IEEE, 2010.
[14] Suo, Hui, et al., Security in the internet of things: a review. Computer Science and Electronics Engineering (ICCSEE), 2012 international conference on. Vol. 3. IEEE, 2012.
[15] Dierks, Tim, Eric Rescorla. The transport layer security (TLS) protocol version 1.2. No. RFC 5246, 2008.
[16] Atkinson, Randall, Stephen Kent. Security architecture for the internet protocol. (1998).
[17] Christoph P. Mayer, Security and privacy challenges in the internet of things, Electronic Communications of the EASST17, 2009.
[18] T.K. Das, A. Banik, S. Chattopadhyay, A. Das, Sub-harmonics Based String Fault Assessment in Solar PV Arrays. In: Chattopadhyay S., Roy T., Sengupta S., Berger-Vachon C. (eds) Modelling and Simulation in Science, Technology and Engineering Mathematics. MS-17 2017. Advances in Intelligent Systems and Computing, vol 749. Springer, Cham., 2019. https://doi.org/10.1007/978-3-319-74808-5_25.

[19] T.K. Das, A. Banik, S. Chattopadhyay, A. Das, FFT based Classification of Solar Photo Voltaic Microgrid System, 2019 Second International Conference on Advanced Computational and Communication Paradigms (ICACCP), Gangtok, India, 2019, pp. 1–5, https://doi.org/10.1109/ICACCP.2019.8882995.

[20] A. Banik, A. Sengupta, Scope, Challenges, Opportunities and Future Goal Assessment of Floating Solar Park, 2021 Innovations in Energy Management and Renewable Resources (52042), Kolkata, India, 2021, pp. 1-5, https://doi.org/10.1109/IEMRE52042.2021.9386735.

[21] A. Banik, A. Shrivastava, R. Manohar Potdar et al., Design, Modelling, and Analysis of Novel Solar PV System using MATLAB, Materials Today: Proceedings, https://doi.org/10.1016/j.matpr.2021.06.226.

[22] Satyadevan, Shiju, Boney S. Kalarickal, and M. K. Jinesh. "Security, trust and implementation limitations of prominent IoT platforms." Proceedings of the 3rd International Conference on Frontiers of Intelligent Computing: Theory and Applications (FICTA) 2014. Springer, Cham, 2015.

[23] Kewei Sha, Wei Wei, T. Andrew Yang, Zhiwei Wang, Weisong Shi, On security challenges and open issues in Internet of Things, Future Gener. Comp. Syst. 83 (2018) 326–337.

[24] A. Čolaković, M. Hadžialić, Internet of Things (IoT): A review of enabling technologies, challenges, and open research issues, Comp. Networks 144 (2018) 17–39, https://doi.org/10.1016/j.comnet.2018.07.017.

[25] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, M. Ayyash, Internet of Things: a survey on enabling technologies, protocols, and applications, IEEE Commun. Surveys Tutorials 17 (4) (2015) 2347–2376, https://doi.org/10.1109/comst.2015.2444095.

[26] A. Khanna, S. Kaur, Internet of Things (IoT), applications and challenges: a comprehensive review, Wireless Personal Commun. 114 (2) (2020) 1687–1762, https://doi.org/10.1007/s11277-020-07446-4.

[27] Trupil Limbasiya, Mukesh Soni, Sajal Kumar Mishra, Advanced formal authentication protocol using smart cards for network applicants, Comp. Electr. Eng., 66, 2018, 50–63,ISSN 0045-7906.

[28] M. Soni, D. Kumar, Wavelet Based Digital Watermarking Scheme for Medical Images, 2020 12th International Conference on Computational Intelligence and Communication Networks (CICN), Bhimtal, India, 2020, pp. 403-407, doi: 10.1109/CICN49253.2020.9242626.

[29] Mukesh Soni, Dileep Kumar Singh, Privacy Preserving Authentication and Key management protocol for health information System, Data Protection and Privacy in Healthcare: Research and Innovations, pp. 37, CRC Publication, 2021.

[30] Mukesh Soni, Dileep Kumar Singh, Blockchain-based security & privacy for biomedical and healthcare information exchange systems, Materials Today: Proceedings, 2021, ISSN 2214-7853,https://doi.org/10.1016/j.matpr.2021.02.094.

[31] M. Soni, D.K. Singh, LAKA: lightweight authentication and key agreement protocol for internet of things based wireless body area network, Wireless Pers Commun. (2021), https://doi.org/10.1007/s11277-021-08565-2.

[32] Mukesh Soni, Yash Barot, S. Gomathi, A review on privacy-preserving data preprocessing, J. Cybersecurity Inf. Manage., 4 (2), 16–30.

[33] M. Soni, T. Patel, A. Jain, Security Analysis on Remote User Authentication Methods. In: Pandian A., Senjyu T., Islam S., Wang H. (eds) Proceeding of the International Conference on Computer Networks, Big Data and IoT (ICCBI – 2018). ICCBI 2018. Lecture Notes on Data Engineering and Communications Technologies, vol 31, 2020, Springer, Cham. https://doi.org/10.1007/978-3-030-24643-3_60.

[34] M. Soni and A. Jain, "Secure Communication and Implementation Technique for Sybil Attack in Vehicular Ad-Hoc Networks," 2018 Second International Conference on Computing Methodologies and Communication (ICCMC), Erode, 2018, pp. 539-543, doi: 10.1109/ICCMC.2018.8487887.

[35] M. Soni, A. Jain, Secure Communication and Implementation Technique for Sybil Attack in Vehicular Ad-Hoc Networks, 2018 Second International Conference on Computing Methodologies and Communication (ICCMC), Erode, 2018, pp. 539–543, doi: 10.1109/ICCMC.2018.8487887.

[36] M. Soni, B.S. Rajput, T. Patel, N. Parmar, Lightweight Vehicle-to-Infrastructure Message Verification Method for VANET. In: Kotecha K., Piuri V., Shah H., Patel R. (eds) Data Science and Intelligent Applications. Lecture Notes on Data Engineering and Communications Technologies, vol 52. Springer, Singapore, 2021. https://doi.org/10.1007/978-981-15-4474-3_50.

[37] U. Chaudhary, A. Patel, A. Patel, M. Soni, Survey Paper on Automatic Vehicle Accident Detection and Rescue System. In: Kotecha K., Piuri V., Shah H., Patel R. (eds) Data Science and Intelligent Applications. Lecture Notes on Data Engineering and Communications Technologies, vol 52. Springer, Singapore. https://doi.org/10.1007/978-981-15-4474-3_35.

[38] M. Soni, B.S. Rajput, Security and Performance Evaluations of QUIC Protocol. In: Kotecha K., Piuri V., Shah H., Patel R. (eds) Data Science and Intelligent Applications. Lecture Notes on Data Engineering and Communications Technologies, 2021, vol 52. Springer, Singapore. https://doi.org/10.1007/978-981-15-4474-3_51.

[39] M. Soni, A. Jain, T. Patel, Human Movement Identification Using Wi-Fi Signals, 2018 3rd International Conference on Inventive Computation Technologies (ICICT), Coimbatore, India, 2018, pp. 422-427, doi: 10.1109/ICICT43934.2018.9034451.

Further reading

[10] https://datatracker.ietf.org/wg/6lowpan/documents.