A Survey on IoT Security: Security Threads and Analysis of Botnet Attacks Over IoT and Avoidance

M. Vijayakumar and T. S. Shiny Angel

Abstract IoT is an emerging technology that provides humans very handy support in various aspects and applications. This technology faces various threats in various aspects. The proposed work will analyze the various levels of threats and combating the threats. Various levels of threats are identified to the IoT. Over twenty-five, different levels of threats are identified for the IoT in different aspects. As the IoT is an emerging technology, it has to overcome these hurdles. In this paper, a nitty dirty review of the security-related challenges and wellsprings of peril in IoT applications is presented. Within the wake of talking around the security issues, diverse emerging and existing developments focused on finishing, and also, mainly Botnets-based threats feature over IoT is been provided solution as it is most vulnerable comparing other threats. Combating features are recommended.

Keywords Threats · Botnet attacks · Bargaining · Negotiation

1 Introduction

All recent technologies are having some sort of issues that makes the system handle with some sort of fear of safety; similarly ,the IoT-based devices have the same issues. Most of the IoT devices are targeted because of certainly valid reasons as embedded components are easy to exploit, these devices are always in on condition, they follow low-security standards, even all users can be able to configure the device with a simple password that is easily accessible by the attackers, and developing malware can easily crack the password used as security in the IoT device. Monitoring and servicing of IoT are not well established for security. A single attack affects a large

M. Vijayakumar (✉) · T. S. Shiny Angel
SRM Institute of Science and Technology, Kattankulathur, Tamil Nadu, India
e-mail: vm2893@srmist.edu.in

T. S. Shiny Angel
e-mail: shinyant@srmist.edu.in

D. P. Agrawal et al. (eds.), *Cyber Security, Privacy and Networking*, Lecture Notes in Networks and Systems 370, https://doi.org/10.1007/978-981-16-8664-1_13

Fig. 1 Different IoT structures

Table 1 Comparison of security between IT devices and IoT devices

IT security everywhere	IoT security
Devices with a lot of resources are common in IT	IoT devices need to be carefully provisioned with security measures
Far reaching IT is built on contraptions with a part of assets	IoT frameworks are composed of gadgets having confinements in terms of their program and equipment
For wide security and lower capabilities, complex calculation is actualized	As it was lightweight, algorithms are favored
Homogeneous innovation is mindful for tall security	IoT with heterogeneous innovation produces a huge sum of heterogeneous information expanding the assault surface

number of systems at a low cost, so attackers have an elation in attack on IoT devices. Figure 1 shows the past, present, and future architecture of IoT.

In the future, the contraptions (devices) are not fair anticipated to be related with the Web and other neighborhood contraptions (devices) but at the same time are required to talk with diverse contraptions (devices) on the Web authentically. Aside from the contraptions or things being associated, the thought of social IoT (SIoT) in addition creating. Social IoT will empower unmistakable social organizing clients to be related with the contraptions, and clients can share the contraptions over the Net [1].

With this colossal extend of IoT applications comes the issue of security and assurance. Without a trusted and interoperable IoT environment, rising IoT applications cannot arrive at ubiquity and may lose all their idle capacity. Nearby the security issues gone up against for the foremost portion by the Web, cell organizations, and WSNs, IoT also has its uncommon security challenges, for example, protection issues, confirmation issues, board issues, data stockpiling, etc.

Table 1 sums up different factors because of which making sure about IoT climate is substantially more testing than making sure about typical data innovation (IT) gadget (devices) so, in the proposed research work, the various vulnerabilities are

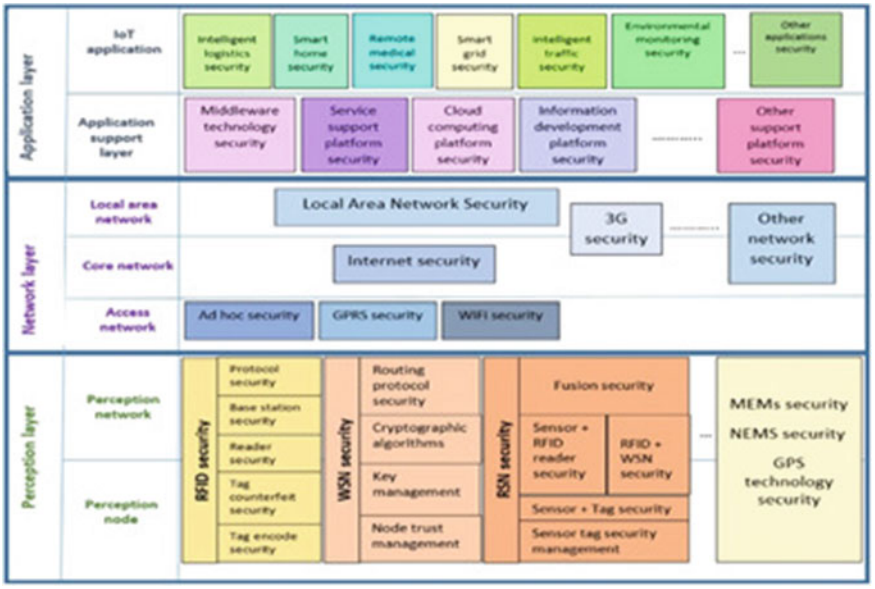

Fig. 2 Typical IoT architecture

discussed. Solution for those threats has been researched out as a research paper [1, 2].

1.1 IoT Security Architecture

Due to the differing qualities of the gadgets and huge number of communication conventions in an IoT framework, conjointly different interfacing and services offered, it is not reasonable to actualize security moderation based on the conventional IT organize arrangements. The current security measures which are connected in an ordinary organize may not be adequate. Assault vectors as recorded by the Open Web Application Security Venture (OWASP) concern the three layers of an IoT framework, which are equipment, communication interface, and interfaces/services. Thus, the usage of IoT security relief ought to envelop the security design at all IoT layers, as displayed in Fig. 2 [3].

There are different existing reviews on IoT security and protection issues. Yuchen et al. [4] have summed up different security issues in IoT applications. Hameed [5] was discussed many algorithms to secure the IoT network. In any case, these algorithms and strategies still need improvement in numerous angles to be utilized in the IoT framework and give confidence in the security and privacy environment. Ngu [6] focused mainly on the security issues related to IoT middleware and provides a detailed survey of related existing protocols and their security issues. Guizani et al.

[7] have reviewed different trust the executive's procedures for IoT alongside their advantages and disadvantages. Security components for IoT security, for example, software-defined networking (SDN) and network function virtualization (NFV), are discussed.

The main contributions of this work are as follows:

1. An arrangement of different IoT applications and unequivocal security and security issues were recognized with those applications.
2. A positive clarification of different threat sources in different layers of IoT.
3. Review on the proposed countermeasures to the security issues in IoT.
4. An examination of the open issues, troubles, and future examination headings for making secure IoT applications.

2 Sources of Security Threats in IoT Applications

As discussed in Section I, any IoT application can be divided into four layers: (1) sensing layer; (2) network layer; (3) middleware layer; and (4) application layer. Each of these layers in an IoT application uses diverse technologies that bring several issues and security threats. Figure 3 shows various technologies, devices, and applications at these four layers. This section discusses various possible security threats in IoT applications for these four layers [8].

2.1 Security Issues at Sensing/Physical Layer

Issue through Humans

There are many applications are being used on various devices by humans which are supported by the IoT device. Reference [9] Humans communicate with different devices in different forms for example in text mode, voice mode, and face-to-face mode. With single connectivity called the internet without the cybersecurity knowledge, people are not aware about the attackers in the digital world. People use most of the Internet-connected devices without the knowledge they are exposed to threats to their data, which would become a threat to their life itself in some cases. Most unsecured components could be a backend information provider of some organization or a corporate network. This should be secured with a certain research methodology that will provide complete protection.

Deficiency Technology Update

Most people lack in investing to have IoT-based infrastructures that will pave way for the attackers to make an easy entry for attacking the devices. The lack of proper update of installed devices also makes a chance of attack, and it makes device open for all to take up the data. Making proper updates will avert the breach of the data that will be major security assert for the concern [10].

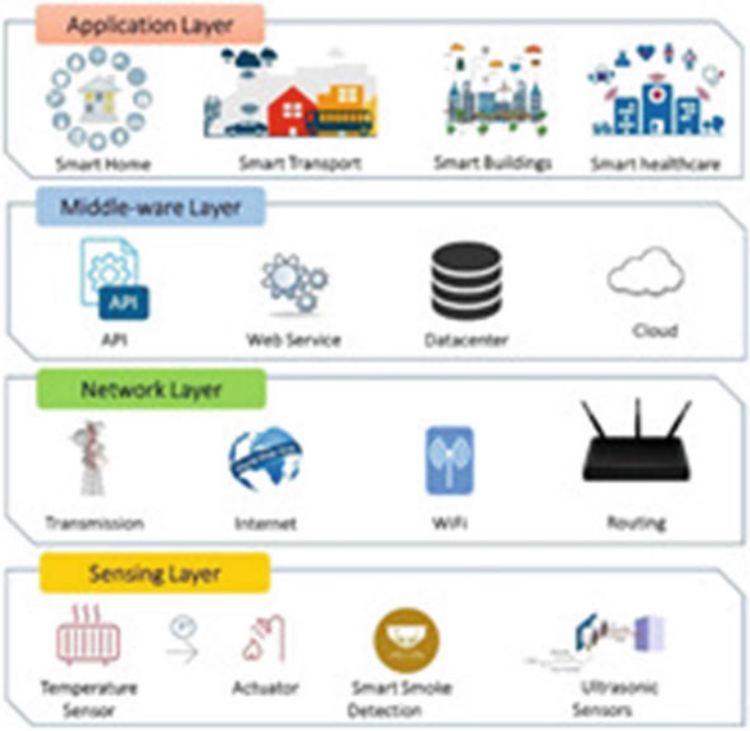

Fig. 3 Layers in IoT System

Poor Physical Security

Software-based security is being discussed by most of the researchers, but there are chances of hardware-based security too, and the intruders and hackers planning access the device with the hardware devices too. The hardware protection should be enabled in a way that tampering of the device can be possible by the hackers, in that USB ports are one of the devices which could be able to tamper [11]. A seal can be proposed to the USB ports that would have an anti-tampering shield that would protect the device from the hacker. The shield will be embedded with the main circuit of the device, which would collapse the entire system if the device is meant to tamper, by that the hackers will not attempt to disassemble the device.

RFID Skimming

The hackers use this mode of attack to gain information about a transaction made through all transaction cards. The card detectors are compromised with RFID Skimming techniques supported by near field communication (NFC) device [12]. The device which is placed by the hackers will make a copy of the transaction data and will transfer it to the hacker's system. It will mean to sense plain data from the device and transfer it to the hacker's server.

2.2 Security Issues at Data Link Layer

Appliance Phishing
Phishing of machines will be an identified concern in the forthcoming period of years. Attackers will try to enter illegally and try to access IoT components and will send fake signals to networks that will cause owners large damage. The operating system will be in attack; for instance, if there is a plant controlled by an IoT device, the fake signals will be giving different signals that make the machinery large damaged. The varying and wrong signals will make the system a large troublesomely [13]. This increases chances of appliance phishing issue. This could be rectified through strong encryption-based chippering security.

Much components, More Coercions
As many devices are connected with IoT, they much have chances of attack by both active attackers and passive attackers. A device meant for support is the data centers at the backend. The product which is in use can store the personal information about the user and has the chance to propagate to the remote server, so there are chances of a copy of the secret personal information of the user to known to the third person. So, secret gateway should be derived at the IoT device itself to hold the data transfer or data store of the user over the device or the server [14].

2.3 Security Issues at Network Layer

Hazardous Communication
Most of the IoT components will not encode the communications while transferring to the networked systems. It is considered the largest safety task for IoT out there. IoT using concerns want to make certain conversations among gadgets and cloud server-based amenities in a steady and encrypted form. Great exercises to conform steady communique are to practice delivery ciphered then to custom criteria similar TLS. Quarantining gadgets via the usage of diverse networks likewise facilitate produce stability in addition to a secluded conversation that maintains the communicated statistics stable as well as trusted [15].

Resident-Based Attack
Internet of Things (IoT) protection had become a freighting fear; subsequently, it links the opening among the digital and somatic sphere. By way of previously stated, unprotected Internet of Things (IoT) components may ooze user's connectivity (Internet Protocol) domicile that may not identify users living locality. Illegal control takers have chances to have a business by using collected data toward dissident Web services, place in which unlawful outfits. As well as, while the user in a make of Internet of Things (IoT) coupled wise household protection arrangements, after that this setup will have chances of negotiated too. For this reason, IoT device protection is stressed often. The user would like to protect his associated components via the Internet of

Things (IoT) protection as well as therefore by the support of tunnel-like networks as VPNs [16].

Individual Data Disclosures
Skilled computer-generated delinquents can be a reason for huge mutilation even though inspection data provides some of the network protocols (Internet Protocol) connectivity via unprotected IoT components. The connection modes often will not locate the utilizer's area as well as the user's original location they live. So, the virtual private network (VPN) is recommended by techies and experts. Setting up a tunnel network like VPN over the user router may encode the entire movement via ISP [17]. Virtual private network or tunnel networks have the user connecting privy Internet address as well as protect the user overall user resident connecting setup.

Privacy Concerns
Huge datum is being collected through most of the IoT devices that might include with most sensitive and secret information without any proper security aspect for the information. Users should review the security agreement made by the apps and the nature of the information being collected. If the information is more personal or sensitive, then the user to be cautious using that such apps [18]. *Or a security application should be developed to encapsulate the sensitive and most private information while uploading apps. This encapsulation must be a security lock that could open by only the user. If it requires for the app service provider*

2.4 Security Issues at Application Layer

IoT components drafted to Botnets
Alike other gadgets presence attacked in form of hackers who takes control of the device and email servers are changed into bulk junk mails or messages; clever device gadgets may also be customized in the form of vulnerable device code for carrying out distributed denial of service (DDoS) attacks. Earlier, attackers used infant displays-oriented output device watches to hold available huge gauge DDoS attacks. Producers want to recognize dangers linked with IoT-associated components and yield to vital actions to protect respective components. This attack is a danger, and it is to be countered with the aspect of security pattern, in an unbreakable server setup [19].

IoT device negotiation through junk Emails
The science and technology developments that occur date to date have made room for an overabundance of shrewd components into the usage of humans, but never stopped to shrewd utilizations, self-governing house control systems, etc. The components utilize the same computing energy by way of other IoT-linked components that have been utilized for many jobs. As per a new update, it has been identified that the devices that are been in negotiable condition can produce a huge amount of spam mails to perplex the user. For this issue, the server should be properly secured to counter this issue [20].

Resident-Based Attack
Internet of Things (IoT) protection had become a freighting fear; subsequently it links the opening among the digital and somatic sphere. By way of previously stated, unprotected Internet of Things (IoT) components may ooze user's connectivity (Internet Protocol) domicile that may not identify users living locality. Illegal control takers have chances to have a business by using collected data toward dissident Web services, place in which unlawful outfits rig function [21]. As well as, while the user in the make of Internet of Things (IoT) coupled wise household protection arrangements, after that this setup will have chances of negotiated too [22].

Negotiating Medicinal Procedures
Medicinal equipment coupled with the IoT have somewhat large chances of attack by hackers, who can take control over these devices and make eavesdrop on the important and secure medical and personal data of some important persons in society and even common man medical reports are to be secured in this money minded world, those records can be sold for some purposes.

For medical data protection, a chip can be inbuilt in the device to analyze the patients. The memory chip presents analysis, and device stores the present status of the the patient's conditions to make double encryptions. These chips are compatible in nature. These memory chips are given to the patient to maintain secrecy with him or herself to maintain secrecy, while he meets with his physician, a onetime password is generated and delivered to both doctor and patient personal mobile number to make the access of the memory device and get the information about the particular patient and provide the treatment [23].

Man-in-the-Middle Attacks
Eavesdropping mode of attack is made in this attack, hackers try to intercept the communication between the communicating persons through IoT device which would be insecure in nature or a dangerous network, masquerade attack is made over the users, and the attack makes a major bad impact over the user's major and most important information [24]. A security-based provision is proposed for this issue, a new technique is enhanced by combining the block chaining the IoT data and transferring the block chained the enciphered data through a tunneled network [25]. This would be a better approach which would be a strong network of secure IoT communication.

3 Common Attacks on IoT Devices

Shortage of development
Most of the devices based on IoT techniques do not adapt any protection aspect in their devices from hackers and data-based threats. A recent analysis warns of this aspect, around 30 million devices all over the world are used without any proper data security in their devices, and this will lead to any network-oriented attack over the devices. Most of the devices lack security updating. Even though they have a security aspect, they never update after a particular level. The concerns provide security to a

certain level only. This level is also not enough to combat the threats and attacks of hackers [26]. This makes users exposed to the hackers without any defending device. This should be made overcome by external security support, which might defend the system even though there is a stop in the security update for the concerned device.

Distant Contact

Reports discharged through Web data of Central Intelligence Agency conveys the about the USA. CIA have been controlling the devices illegally into IoT gadgets as well as changing the direction of the image capturing device/mouthpieces by deprived of the information on the proprietors. Indeed, the likelihood that assailants will occupy the gadgets in use by any user as well as store the proprietors deprived of their insights alarming and made utilized through no one additionally by the Administration themself. Its reports highlighted monstrous vulnerabilities in the most recent programming [25], for example, Android and iOS, which implies hoodlums can likewise exploit these vulnerabilities and complete preposterous wrongdoings.

Information Larceny

Hackers are usually after information which includes, however, no longer restricted to, patron names, purchaser location information, bank card numerical, monetary particulars, then additional. Alike while an organization has compact Internet of Things (IoT) protection, still some special assault courses by hackers may take advantage. In that case, such kind of tool is hooked up toward a concern's network establishments, the person who takes control over other devices is able to get benefit get right of entry toward the computer connected establishments as well as cull entire valued information [27]. Then, this information will be shared to illicit users for a huge sum by the foretold beneficiaries through the procedure as briefed earlier.

Computational Intelligence coupled IoT

Computational intelligence is an emerging technology that could IoT in countering the threats over it. The data storage-based threats can be somewhat averted through artificial intelligence technology. If the IoT device possesses this AI support. The technology will be providing support to control the IoT device based on the task. Automation can be defined as a code as IoT codes. In some cases, the IoT codes can also be interrupted by the hackers or attackers to change the activities of IoT devices by just changing the code and make the device work harmfully to the user itself [28]. So, there is both safety and security issue while using the artificial intelligence supported IoT device. An alternate technique should be sorted out to avert this issue to have safe usage of the IoT devices.

4 Evolution of Botnet

Generally, there are large numbers of Botnets are developed in the cyber environments for affecting various net-based devices. A short analysis is made about these Botnets. Botnets are generally classified into two Botnets; they are traditional Botnets and IoT-based Botnets.

4.1 Traditional Botnets

This Botnet is not segregated as the specific task of attack, it is meant for the attack of overall computational devices like computers and servers, and they attack the device with malware and zombies, compromise the device to act like malware and zombies. Botnet owners can control devices, they make the device to have denial of services to the users, and other attacks like spam mail and information theft are other attacks by the traditional Botnets.

4.2 IoT-Based Botnets

IoT-based Botnets are the system that forms a cluster that negotiated Internet of Things (IoT) components in the form of all electronic system devices which are already compromised by the Botnets infected by the malware. Malware will permit the assailants to make dominate the device making the task as a conventional Botnet. This IoT Botnet will replicate its patch with the connecting devices to which it connects and makes the device bot-affected device.

4.3 Different Botnet Attacks

For understanding Botnet attack outcomes, some of the attacks are elaborated, and they are as follows

Linux. Aidra
This attack is identified in the year 2012 through the cybersecurity scientists at ATMA.ES. It is the first identified and registered attack where a large number of telnet-connected devices are affected due to this attack.

Bashlite
This attack came to light in the year 2014 a source code is published with multiple variants in the type of Bashlite in the different names gayfgt, qbot, lizkebab, and torlus. Over 1 lakh devices had been affected due to this attack.

Mirai
This attack was made in the year 2016, and this attack made a record-breaking attack over the devices in the form of a DDoS attack on the devices like Krebs, OVH, and Dyn. The main aim of this Botnet is all electronic devices that support IoT, and featuring ten predefined attacks, the Botnet made down many server infrastructures and cloud service providers. Assaults are GRE floods and water torture attacks.

Linux/IRCTelnet
This attack was made in the year 2016 through the malware Must Die, The Internet of Things (IoT) Botnet is aiming at all electronic devices like (routers, DVRs, and

IP cameras). UDP and TCP flooding of data signal along with the IPV4 and IPV6 protocols support is the outcome of this attack.

4.4 IoT Botnet Monitoring System (IBMS)

This system is proposed to monitor the attempt of Botnet-based attacks over IoT devices to provide alerts in means of the nonce to the server in which other IoT devices are connected. This alert will be based on the time interval basis that will make the IoT suspend the communication among the devices connected with. Detection of attack is identified through the behavior of each network that is connected with the main server for the particular application.

The devices which attempt to attack or attempt to fire the Botnet initially will have the behavior change, the sequence signal from the device varies, the time interval of normal time signal and attack planned signal varies, and this one aspect is considered as the behavior based on the probability. Based on it, a training set is made to identify the affected Botnet node or malleolus node which attempts the node [29].

In other modes, an artificial intelligence approach can be handled to identify the devices which are meant for the attack of Botnets and going to become a Botnet [30, 31].

4.5 Bargaining and Negotiation Methodology for Botnet Identification

Bargaining is a communication technique between two people generally to accept one person's ideology by others. Similarly, in a multi-agent concept, two agents had given a task to solve it, and they communicate with each other. One agent generally makes another agent accept its action and the other agent to do the task given by the agent. The same concept can be applied to identify the Botnet-affected node or device and isolate the device from communicating.

Three types of signals are made to arise among the two devices, the commands are as follows,

Signal α*—To accept the task*
Signal β*—The device is busy wait for n seconds*
Signal γ*—Negating the signal cannot accept the signal or task.*
For signal transferring, three different wavelength signals can deploy for each different nonce modulated signal that can only be sensed by the specific sensors that are to be derived [11–13] (Fig. 4).
*Step 1: The device starts to establish the communication with the connected device (D1*α ⇒ *D2)*

Fig. 4 Bargaining and negotiation among the agent in general

Step 2: Waits for t seconds for the response or to accept the task D1α (t)D2)

Step 3: Produces a Nonce α signal for the alert and negotiating signal to accept the task. (The negotiating signal nonce is made a maximum of three times to ensure the device is ready to take the task in a very short interval of time) D1αt (n1), D1αt (n2), D1αt (n3).D2)

Step 4: Within the 3 nonce signal connected device will respond with the same D2α1 nonce signal for accepting the task.D2)

Step 5: If the signal D2α 1 is received, then the device starts to give the command, for an application that is going to be processed.D2)

Step 6: If the device is in the other task, it alerts with nonce D2β instead of D2α 1 D2)

Step 7: The device stops sending nonce to that device and checks with other devices.D2)

Step 8: If the particular device is affected by the Botnet of some issue nonce γ is arising from the devices.D2)

Step 9: After receiving the signal Dγ the device disconnects with the issued device and stops communicating.D2)

This mode of approach is meant to identify the devices that are not negotiating, and generally, most of the devices tend to negotiate to respond positively, if it or not attacked by the Botnet. This will be a better approach to identify the nature of the device. Whether it is in the position of executing the task or it is affected by any of the issues similar to any attacks [14–16].

5 Conclusion and Future Enhancement

In this paper, various IoT-based issues are identified; a suitable rectification is being provided for the issues. Solutions for Botnet attacks are been derived with a methodology that will identify and segregate the attacked device from other devices, which will stop the further breakdowns of the systems. In future enhancements, modulated signals are derived, with the modulated device sensing sensors, which will support identify the components which are been attacked, and this will be able to protect other components from further attack.

References

1. Frustaci M, Pace P, Aloi G, Fortino G (2018) Evaluating critical security issues of the IoT world: present and future challenges. IEEE Internet Things J 5(4):2483–2495
2. Hassija V, Chamola V, Saxena V, Jain D, Goyal P, Sikdar B, A survey on IoT security: application areas, security threats, and solution architectures. IEEE Access. https://doi.org/10.1109/ACCESS.2019.2924045
3. Sengupta J, Ruj S, Bit SD (2019) Comprehensive survey on attacks, security issues and blockchain solutions for IoT and IIoT. J Netw Comput Appl 149:102481
4. Yang Y, Wu L, Yin G, Li L, Zhao H (2017) A survey on security and privacy issues in internet-of-things. IEEE Internet Things J 4(5):1250–1258
5. Hameed A, Allometry A (2019) Security issues in IoT: a survey. In: 2019 International conference on innovation and intelligence for informatics, computing, and technologies (3ICT)
6. Ngu AH, Gutierrez M, Metsis V, Nepal S, Sheng QZ, IoT middleware: a survey on issues and enabling technologies. IEEE Internet of
7. Din IU, Guizani M, Kim B-S, Hassan S, Khan MK (2019) Trust management techniques for the internet of things: a survey. IEEE Access 7:29763–29787
8. Babar S, Stango A, Prasad N, Sen J, Prasad R (2017) Proposed embedded security framework for Internet of Things (IoT). Center for TeleInFrastruktur, Aalborg University, Aalborg, Denmark 2Tata Consultancy Services, Kolkata, India {sdb, as,np}@es.aau.dk, jaydip.sen@tcs.com, prasad@es.aau.dk. Things J 4(1):1–20
9. A framework of intrusion detection system based on Bayesian network in IoT Jie Wang College of Information and Communication Engineering Harbin Engineering University Harbin. Int J Performabil Eng, Oct 2018. https://doi.org/10.23940/ijpe.18.10.p4.22802288.
10. Security threats/attacks via botnets and botnet detection & prevention techniques in computer networks: a review. Emerald Simkhada Elisha Shrestha Sujan Pandit, Upasana Sherchand Akalanka Mailewa Dissanayaka and IT St. Cloud State University
11. A model to incorporate automated negotiation in IoT Mohammad Irfan Bala, Mohammad Ahsan Chishti Department of Computer Science and Engineering National Institute of Technology, Srinagar, India mirfan508@gmail.com,ahsan@nitsri.ne
12. Faratin P, Sierra C, Jennings NR (1998) Negotiation decision functions for autonomous agents. Robot Autonomous Syst 24(3):159–182
13. Jennings NR, Faratin P, Lomuscio AR, Parsons S, Wooldridge MJ, Sierra C (2001) Automated negotiation: prospects, methods and challenges. Group Decis Negotiat 10(2):199–215
14. Perera C, Zaslavsky A, Christen P, Georgakopoulos D (2014) Sensing as a service model for smart cities supported by the internet of things. Trans Emerg Telecommun Technol 25(1):81–93
15. Kang K, Pang Z, Da Xu L, Ma L, Wang C (2014) An interactive trust model for application market of the internet of things. IEEE Trans Ind Inform 10(2):1516–1526

16. Dementyev A, Hodges S, Taylor S, Smith J (2013) Power consumption analysis of Bluetooth low energy, Zigbee and ant sensor nodes in a cyclic sleep scenario. In: Wireless Symposium (IWS), (2013) IEEE International. IEEE 2013, pp 1–4
17. Bellifemine F, Caire G, Greenwood D (2007) Developing multi-agent systems with JADE, ser. Wiley series in agent technology. Wiley. Available: http://books.google.hr/books?id=ZLBQAAAAMAAJ
18. Zheng X, Martin P, Brohman K, Da Xu L (2014) Cloud service negotiation in the internet of things environment: a mixed approach. IEEE Trans Ind Inform 10(2):1506–1515
19. Raz Lin, Sarit Kraus (2010) Designing automated agents capable of efficiently negotiating with people—overcoming the challenge. Commun ACM 53(1):78–88
20. Choi SPM, Liu J, Chan S-P (2001) A genetic agent-based negotiation system. Comput Netw 37(2):195–204
21. Mukun C (2010) Multi-agent automated negotiation as a service. In: 7th international conference on service systems and service management (ICSSSM), 2010, pp 1–6
22. Bevan C, Fraser DS (2015) Shaking hands and cooperation in tele-present human-robot negotiation. In: Proceedings of the tenth annual ACM/IEEE international conference on human-robot interaction, Mar 2015, Portland, Oregon, USA. https://doi.org/10.1145/2696454.2696490
23. Oliver JR (1996) A machine-learning approach to automated negotiation and prospects for electronic commerce. J Manage Inf Syst 13(3):83–112
24. D'Angelo G, Palmieri F (2021) GGA: a modified genetic algorithm with gradient-based local search for solving constrained optimization problems, Inf Sci 547:136–162. ISSN 0020-0255. https://doi.org/10.1016/j.ins.2020.08.040
25. D'Angelo G, Castiglione A, Palmieri F (2021) A cluster-based multidimensional approach for detecting attacks on connected vehicles. IEEE Internet of Things J 8(16):12518–12527. https://doi.org/10.1109/JIOT.2020.3032935
26. D'Angelo G, Palmieri F (2021) Network traffic classification using deep convolutional recurrent autoencoder neural networks for spatial-temporal features extraction. J Netw Comput Appl 173:102890. ISSN 1084-8045
27. 25 Most Common IoT Security Threats in an Increasingly Connected
28. 20 Surprising IoT Statistics You Don't Already Know
29. 134 Cybersecurity Statistics and Trends for 2021. https://www.varonis.com/blog/cybersecurity-statistics/
30. Cyberattacks on IOT devices surge 300% In 2019, 'Measured In Billions', Report Claims. https://www.forbes.com/sites/zakdoffman/2019/09/14/dangerous-cyberattacks-on-iot-devices-up-300-in-2019-now-rampant-report-claims/#61f7892a5892
31. Symantec Security Center. https://www.symantec.com/security-center/threat-report