IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 11, Issue 3, March 2023

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.379

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 |

|| Volume 11, Issue 3, March 2023 ||

| DOI: 10.15680/IJIRCCE.2023.1103114 |

Security in the Internet of Things (Iot): A Review, Block Chain Applications

Prof. Ranu Sahu[1], Prof. Saurabh Verma[2], Nidhi Sahu[3], Sourbh Shripal[4]

Department of Computer Science and Engineering, Baderia Global Institute of Engineering & Management, Jabalpur, Madhya Pradesh, India

ABSTRACT: The rise of smart technologies in various domains such as homes, cities, and other interconnected systems has propelled the Internet of Things (IoT) into a realm of immense influence, potential, and expansion. Cisco Inc. has forecasted a staggering 50 billion connected devices by 2020, underscoring the rapid proliferation of IoT. Despite this growth, a significant concern looms over the security of these IoT devices, as many are susceptible to hacking and compromise. Their limited computational, storage, and networking capabilities render them more vulnerable compared to traditional endpoint devices like smartphones, tablets, and computers.This paper examines and categorizes the major security challenges facing IoT devices. It reviews prevalent security issues within the layered architecture of IoT, encompassing networking, communication, and management protocols. The paper also delineates the security prerequisites for IoT and surveys current attacks, threats, and state-of-the-art solutions. Additionally, it presents a comparative analysis of IoT security challenges and existing solutions found in the literature.Furthermore, the paper delves into the potential of blockchain, the foundational technology behind bitcoin, as a pivotal tool for addressing numerous security issues in IoT. It discusses how blockchain can enhance security in IoT ecosystems. The paper concludes by outlining open research problems and ongoing challenges in IoT security, underscoring the need for continued innovation in this domain.

KEYWORDS: Security in the Internet of Things (IoT), Blockchain Technology ,Protocols for IoT, Security in IoT Networks ,Security of IoT Data.

I. INTRODUCTION

The rapid proliferation of smart devices and high-speed networks has propelled the Internet of Things (IoT) into widespread acceptance and adoption as the primary standard for Low-Power Lossy Networks (LLNs) with limited resources. This network framework interconnects embedded devices equipped with sensors via either private or public networks, enabling remote control for desired functionalities. Information exchange among these devices occurs through standardized communication protocols. Ranging from simple wearable accessories to large machinery, these smart connected devices encompass diverse sensor-equipped technologies. Additionally, Wireless Sensor Networks (WSNs) and Machine-to-Machine (M2M) or Cyber-Physical Systems (CPS) have become integral components of the broader IoT landscape. However, security challenges stemming from WSNs, M2M, or CPS persist within the IoT ecosystem, with the IP protocol serving as the primary connectivity standard. The entire deployment architecture requires robust security measures to safeguard against potential attacks that could disrupt IoT services and compromise data privacy, integrity, or confidentiality. Given the interconnected nature and heterogeneous composition of IoT networks, conventional security issues inherited from computer networks are prevalent. Moreover, the resource constraints posed by small sensor-equipped devices further compound security challenges, necessitating tailored security solutions adapted to these constrained architectures.

Given that IoT encompasses interconnected networks and heterogeneous devices, it inherits traditional security challenges associated with computer networks. The constraints imposed by limited resources further compound the security challenges within IoT, as the small sensor-equipped devices possess restricted power and memory capabilities. Consequently, security solutions must be tailored to accommodate these constrained architectures.

In recent years, significant efforts have been made to address security challenges within the Internet of Things (IoT) paradigm, with various approaches targeting specific layers or aiming to provide comprehensive end-to-end security solutions. A recent survey conducted by Alaba et al. [7] introduces a novel taxonomy for categorizing IoT security issues based on application, architecture, communication, and data, diverging from conventional layered architectures. This taxonomy facilitates discussions on threats affecting hardware, network, and application components of IoT.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 |

|| Volume 11, Issue 3, March 2023 ||

| DOI: 10.15680/IJIRCCE.2023.1103114 |

Likewise, Granjal et al. [8] explore and evaluate security concerns pertaining to IoT protocols, while other studies [9–11] delve into comparative analyses of key management systems and cryptographic algorithms. Additionally, research [12–14] focuses on assessing intrusion detection systems, and security challenges related to fog computing are examined in works such as [15,16]. Sicari et al. [17] survey contributions addressing confidentiality, access control, and privacy within IoT, including security considerations for middleware, encompassing trust management, authentication, privacy, data and network security, and intrusion detection. Furthermore, surveys [18] delve into security aspects specific to edge computing paradigms, such as mobile cloud computing, mobile edge computing, and fog computing, covering topics including identity authentication, access control, network security, trust management, fault tolerance, and forensics implementation.

A survey on privacy-preserving mechanisms for IoT is presented in [19], focusing on secure multi-party computations to protect IoT user privacy. The use of credit checking and attribute-based access control is highlighted as effective approaches for privacy preservation in IoT. Zhou et al. [20] discuss various security threats and potential countermeasures for cloud-based IoT, including identity and location privacy, node compromise, layer manipulation, and key management issues. Zhang et al. [21] survey major IoT security challenges, including unique object identification, authentication, authorization, privacy, lightweight cryptographic requirements, malware, and software vulnerabilities. The IOT-a project [22] introduces a reference architecture emphasizing trust, privacy, and security implementation, where the trust model ensures data integrity and confidentiality through authentication for end-to-end communication. The privacy model defines access policies and encryption mechanisms to prevent improper data usage. The security aspect includes service, communication, and application layers. Additionally, the Open Web Application Security Project (OWASP) [23] identifies the top 10 vulnerabilities in IoT, such as insecure interfaces, inadequate security configurations, physical security weaknesses, and insecure software/firmware.

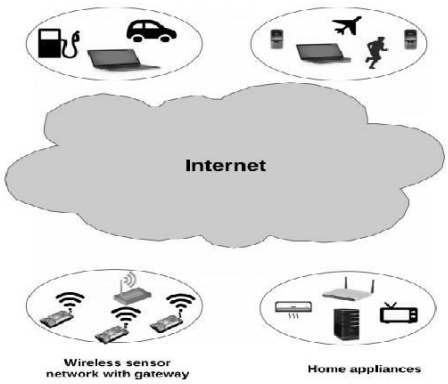

Fig. 1. An overview of IoT elements.

II. IOT ARCHITECTURE AND SECURITY CHALLENGES

In a typical Internet of Things (IoT) setup, diverse devices with embedded sensors are linked via a network, as depicted in Figure 1. These IoT devices are distinctively identifiable and often possess traits such as low power consumption, limited memory, and constrained processing capabilities. Gateways are utilized to connect IoT devices to external networks, enabling remote access to data and services for IoT users.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 |

|| Volume 11, Issue 3, March 2023 ||

| DOI: 10.15680/IJIRCCE.2023.1103114 |

2.1. IoT protocols and standards

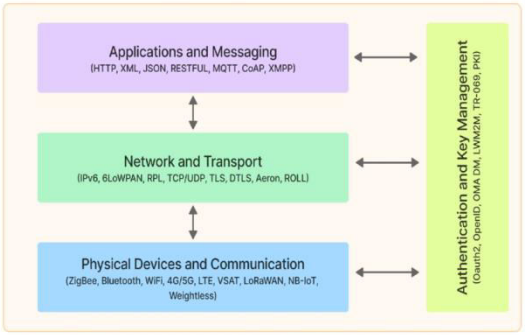

Fig. 2. Common IoT standards and protocols.

Figure 2 illustrates a layered architecture showcasing prevalent IoT protocols for various functions including applications and messaging, routing and forwarding, physical device communication, as well as key management and authentication. This architecture encompasses standards and protocols for low-rate wireless personal area networks (LR-WPANs) [24], along with more recent developments in protocols for low-power wide-area networks (LPWANs).
The IEEE standard 802.15.4 defines two primary layers for LR-WPANs: the Physical Layer and the Medium Access Control (MAC) layer. The Physical Layer specification pertains to wireless communication across diverse frequency bands and data rates, while the MAC layer specifies mechanisms for channel access and synchronization. Due to the limited maximum transmission unit (MTU) in IEEE 802.15.4, an adaptation layer known as IPv6 over low-power wireless personal area network (6LoWPAN) is added above the link layer to enable sensor nodes with IP-based communication capabilities. Each IoT device is uniquely identified by an IPv6 network address. The Routing Protocol for Low-Power and Lossy Networks (RPL) is used in 6LoWPAN environments to support point-to-point, multipoint, and single-point communications. For efficient communication in IoT, User Datagram Protocol (UDP) is favored over Transmission Control Protocol (TCP) due to its simplicity and efficiency, especially with UDP header compression for optimal use of limited payload space. The Internet Control Message Protocol (ICMP) is used for control messages in 6LoWPAN. The Constrained Application Protocol (CoAP) offers a request-response model for low-power lossy networks, providing asynchronous message communication and HTTP mapping to access IoT resources through HTTP. LPWAN enables long-range communication for IoT devices with low power consumption, using protocols like LoRaWAN for communication between gateways and end devices at varying data rates. Additionally, narrow-band IoT (NB-IoT) is a 3GPP protocol designed for indoor coverage in LPWANs using LTE spectrum. The Weightless protocol encompasses three standards to support uni-directional, bi-directional, and low-power modes of communication in LPWANs.

2.2. Security requirements for IoT

For a secure IoT deployment, various mechanisms and parameters need to be reckoned with as described below

2.2.1. Data privacy, confidentiality and integrity

Data privacy, confidentiality, and integrity are critical considerations in IoT networks, particularly as data traverses multiple nodes. Robust encryption mechanisms are essential to maintain data confidentiality. Given the varied integration of services, devices, and networks in IoT, data stored on devices is susceptible to privacy breaches from compromised nodes within the network. Attacks on vulnerable IoT devices can compromise data integrity, allowing attackers to maliciously modify stored data.

2.2.2. Authentication, authorization and accounting

Authentication is crucial for securing communication in IoT, requiring verification between communicating parties. Devices need to be authenticated for privileged access to services. The diversity of authentication mechanisms in IoT is largely due to the heterogeneous underlying architectures and environments supporting IoT devices, making it challenging to define a standard global protocol. Similarly, authorization mechanisms ensure that access to systems or information is granted only to authorized entities. Proper implementation of authorization and authentication establishes a trustworthy environment, ensuring secure communication. Additionally, accounting for resource usage, along with auditing and reporting, provides a reliable mechanism for securing network management.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 |

|| Volume 11, Issue 3, March 2023 ||

| DOI: 10.15680/IJIRCCE.2023.1103114 |

2.2.3. Availability of services

Attacks on IoT devices can disrupt service provision, often through denial-of-service attacks. Sinkhole attacks, jamming adversaries, and replay attacks are among the strategies used to exploit IoT components at various layers, leading to a degradation in the quality of service (QoS) for IoT users.

2.2.4. Energy efficiency

IoT devices are often constrained in terms of resources, with low power and limited storage capacity. Attacks on IoT architectures can lead to increased energy consumption, achieved by flooding the network and depleting IoT resources. redundant or forged service requests.

2.3. Single points of failure

The expanding diversity of networks within IoT infrastructure can create numerous single points of failure, potentially compromising the envisioned services. This situation underscores the need to establish tamper-proof environments for the multitude of IoT devices and to devise alternative mechanisms for implementing fault-tolerant networks.

III. Categorization of security issues

Given the diverse range of devices in the IoT ecosystem, from small embedded chips to large servers, addressing security concerns becomes multi-faceted. Figure 3 presents a taxonomy of IoT security issues, with corresponding references. These security threats are categorized based on the IoT deployment architecture as follows:

- Security issues at the lower level
- Security concerns at an intermediate level
- Security challenges at a higher level

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 |

|| Volume 11, Issue 3, March 2023 ||

| DOI: 10.15680/IJIRCCE.2023.1103114 |

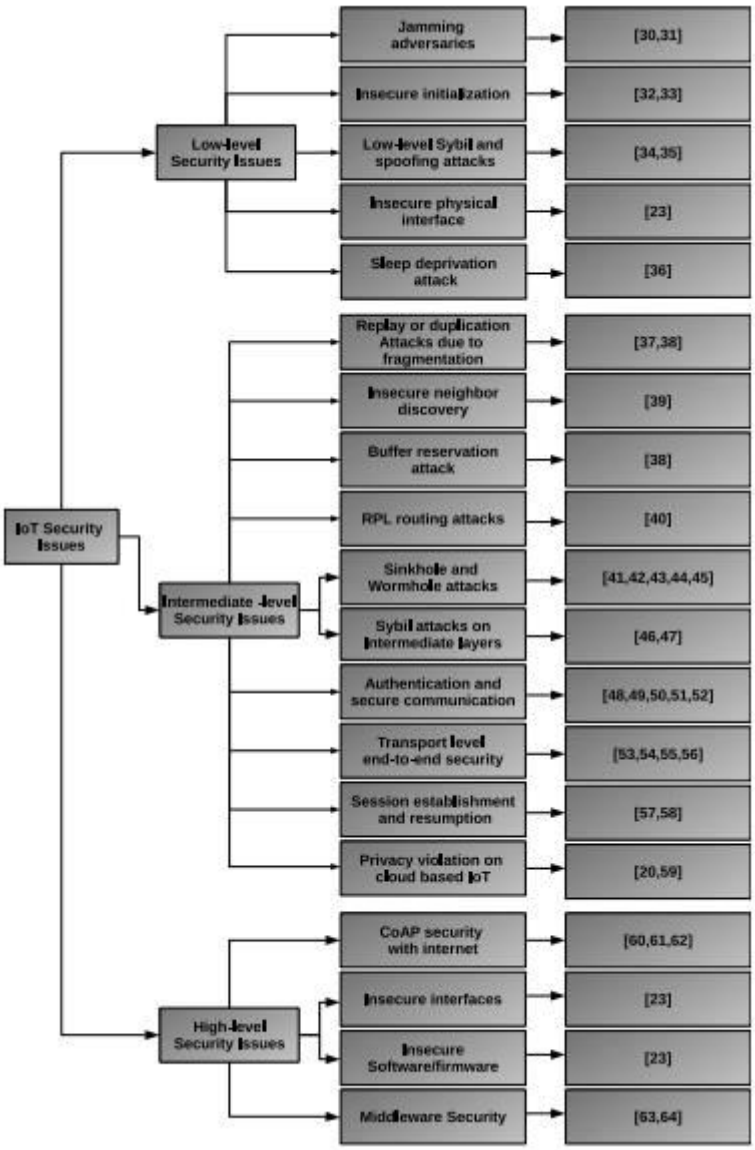

Fig. 3. A taxonomy of security issues and related publications

3.1. Low-level security issues

The initial security level addresses issues at the physical and data link layers, as well as the hardware level. Jamming adversaries, for example, target wireless devices by emitting radio signals without adhering to a specific protocol, causing severe radio interference that disrupts network operations. Insecure initialization practices can also compromise IoT systems, highlighting the need for secure mechanisms for initializing and configuring IoT devices at the physical layer to ensure proper functionality and protect privacy. Additionally, securing physical layer communication is crucial to prevent unauthorized access.

Sybil and spoofing attacks at a low level involve malicious nodes using fake identities to disrupt IoT functionality, with Sybil nodes potentially using forged MAC values to masquerade as different devices, leading to resource depletion and denial of access to legitimate nodes. Insecure physical interfaces present additional threats, as factors like poor physical security and unauthorized software access can be exploited to compromise IoT nodes. Sleep deprivation attacks target energy-constrained IoT devices by keeping sensor nodes awake, depleting their batteries when numerous tasks are scheduled for execution in the 6LoWPAN environment.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 |

|| Volume 11, Issue 3, March 2023 ||

| DOI: 10.15680/IJIRCCE.2023.1103114 |

3.2. Intermediate-level security issues

Intermediate-level security concerns focus on communication, routing, and session management at the network and transport layers of IoT.

Replay or duplication attacks stemming from packet fragmentation are a concern for devices adhering to the IEEE 802.15.4 standard, which mandates small frame sizes. Fragmentation of IPv6 packets at the 6LoWPAN layer can lead to resource depletion, buffer overflows, and device reboots. Insecure neighbor discovery poses another threat, as the identification process for every device must be secure to ensure data reaches the correct destination. Neighbor discovery packets lacking proper verification can result in severe implications and potential denial-of-service attacks. Buffer reservation attacks exploit receiving nodes by sending incomplete packets, leading to denial-of-service as other fragment packets are discarded due to the space occupied by incomplete ones.

RPL routing attacks target the IPv6 Routing Protocol for Low-Power and Lossy Networks, making it vulnerable to resource depletion and eavesdropping through compromised nodes. Sinkhole attacks involve the attacker node responding to routing requests, diverting packets through it for malicious activity. Wormhole attacks create tunnels between nodes, facilitating immediate packet delivery and posing risks of eavesdropping, privacy violation, and denial-of-service. Sybil attacks on intermediate layers can also degrade network performance and compromise data privacy, as Sybil nodes communicate with fake identities to spam, disseminate malware, or launch phishing attacks.

Authentication and secure communication are imperative in IoT, necessitating robust key management systems to authenticate devices and users. Transport level end-to-end security aims to ensure secure message communication without privacy violations, requiring efficient cryptographic mechanisms given constrained resources. Session establishment and resumption are vulnerable to session hijacking, where forged messages lead to denial-of-service or message alteration.

Cloud-based IoT faces privacy violations, with attacks targeting identity and location privacy. Malicious cloud service providers may access confidential information transmitted within the IoT deployment, compromising data confidentiality and integrity.

3.3. High-level security issues

High-level security issues in IoT pertain to applications running on IoT devices. For example, the Constrained Application Protocol (CoAP), which is a web transfer protocol for constrained devices, utilizes Datagram Transport Layer Security (DTLS) bindings to ensure end-to-end security. CoAP messages, following a specific format defined in RFC-7252, require encryption for secure communication. CoAP's multicast support necessitates robust key management and authentication mechanisms to prevent unauthorized access.

Interfaces used to access IoT services through web, mobile, and cloud are susceptible to various attacks, potentially compromising data privacy. Insecure software/firmware in IoT devices can create vulnerabilities, requiring careful testing of code written in languages like JSON, XML, SQLi, and XSS. Secure methods for software/firmware updates are also essential. Furthermore, security in IoT middleware, which facilitates communication among heterogeneous IoT entities, is crucial for service provision. Incorporating secure communication interfaces and environments using middleware is imperative for ensuring IoT security.

IV. BACKGROUND

A blockchain is a decentralized, distributed, shared, and immutable database ledger that records the registry of assets and transactions across a peer-to-peer network. It consists of chained blocks of data that have been timestamped and validated by miners. The blockchain uses elliptic curve cryptography (ECC) and SHA-256 hashing to provide strong cryptographic proof for data authentication and integrity. Each block contains a list of all transactions and a hash to the previous block, ensuring a full history of all transactions and providing cross-border global distributed trust. Unlike Trusted Third Parties (TTP) or centralized authorities that can be disrupted, compromised, or hacked, blockchain transactions are verified by a majority consensus of miner nodes, ensuring immutability once validated and preventing data from being erased or altered. Blockchain networks can be permissioned (private) or permission-less (public), with permissioned blockchains offering more privacy and better access control.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 |

|| Volume 11, Issue 3, March 2023 ||

| DOI: 10.15680/IJIRCCE.2023.1103114 |

The design structure of a blockchain consists mainly of the block header and the block body containing a list of transactions. The block header includes fields such as a version number to track software or protocol upgrades, a timestamp, block size, and the number of transactions. The Merkle root field represents the hash value of the current block, using Merkle tree hashing for efficient data verification in distributed systems and P2P networks. The nonce field is used for the proof-of-work algorithm, serving as a trial counter value that produces the hash with leading zeros. The difficulty target specifies the number of leading zeros, adjusting periodically to maintain a blocktime of approximately 10 minutes for Bitcoin and 17.5 seconds for Ethereum. This adjustment accounts for the increasing computation power of hardware over time, ensuring a consistent blocktime to reach a consensus among miners.

Bitcoin is among the first and most popular applications that utilize blockchain technology. It serves as the underlying platform for many of today's popular cryptocurrencies. Ethereum, on the other hand, introduced smart contracts, expanding the potential applications of blockchain technology. Launched in July 2015, Ethereum allows users to store records and execute smart contracts. Smart contracts are computerized transaction protocols that automatically execute the terms of a contract. These contracts are written in Solidity, a JavaScript-like language, and are uploaded and executed on the blockchain. Ethereum provides Ethereum Virtual Machines (EVM), which are miner nodes capable of executing and enforcing these contracts in a cryptographically tamper-proof manner.
Unlike bitcoin, which primarily facilitates digital currency transactions, Ethereum supports its own digital currency called Ether. Users can transfer coins to each other using normal transactions recorded on the ledger. However, for Ethereum to support smart contract execution, a blockchain state is used. Smart contracts have their own account, address, executable code, and balance of Ether coins. Ethereum's smart contracts can store validation hashes of remotely stored information, enabling a wide range of applications from cryptocurrency trading to autonomous machine-to-machine transactions, supply chain and asset tracking, automated access control, digital identity, voting, certification, and governance of records. Commercial deployments of blockchain technology are increasing rapidly, with examples like SafeShare offering insurance solutions using blockchain and IBM utilizing its blockchain framework based on Hyperledger Fabric for applications in banks, supply chain systems, and cargo shipping companies.

V. BLOCKCHAIN AND IOT RELATED WORK

Research on the intersection of blockchain and IoT is currently limited, with most work focusing on how blockchain can enhance IoT. A study categorized 18 blockchain use cases, with four specifically for IoT, including maintaining an immutable event log, managing data access control, trading IoT data, and managing keys for IoT devices. Challenges in IoT identity, such as ownership, authentication, and privacy, are also highlighted as areas where blockchain could be beneficial. Another proposal introduces a blockchain framework for industrial IoT (IIoT), enabling IIoT devices to interact with the cloud and blockchain. Each IIoT device is equipped with a single-board computer (SBC) for communication with both the cloud and the Ethereum blockchain, allowing data storage, analysis, transaction management, and smart contract execution. A review discusses how blockchain smart contracts can support autonomous workflows and service sharing among IoT devices, citing examples in billing, e-trading, shipping, and supply chain management. They also propose scenarios for automated energy trading among smart meters and asset tracking in container shipments using smart contracts and IoT.

VI. CONCLUSION

Today's IoT devices lack security measures and are vulnerable due to limited resources, immature standards, and a lack of secure hardware and software practices. Establishing a robust global security mechanism for IoT is challenging due to the diverse nature of IoT resources. This paper surveys and reviews key security issues in IoT, categorizing them into high-level, intermediate-level, and low-level layers. It also provides a summary of proposed security mechanisms at different levels and analyzes attacks in IoT along with their potential solutions. The paper explores how blockchain technology can help mitigate some of the major security challenges in IoT. Finally, it identifies future research directions and challenges for the research community to develop reliable, efficient, and scalable IoT security solutions.

REFERENCES

[1] L. Atzori, A. Iera, G. Morabito, The internet of things: A survey, Comput. Netw.54 (15) (2010) 2787–2805.
[2] D. Giusto, A. Iera, G. Morabito, L. Atzori, The Internet of Things: 20th Tyrrhenian Workshop on Digital Communications, Springer Publishing Company, Incorporated, 2014.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 |

|| Volume 11, Issue 3, March 2023 ||

| DOI: 10.15680/IJIRCCE.2023.1103114 |

[3] B. Heater, Lenovo shows off a pair of intel-powered smart shoes, 2016. URL https://techcrunch.com/2016/06/09/lenovo-smart-shoes/
[4] M. Rouse, I. Wigmore, Internet of things, 2016. URL http://internetofthingsagenda.techtarget.com/definition/Internet-of-Things-IoT.
[5] A.A. Khan, M.H. Rehmani, A. Rachedi, Cognitive-radio-based internet of things: Applications, architectures, spectrum related functionalities, and future research directions, IEEE Wirel. Commun. 24 (3) (2017) 17–25. http://dx.doi.org/10.1109/MWC.2017.1600404
[6] F. Akhtar, M.H. Rehmani, M. Reisslein, White space: Definitional perspectives
and their role in exploiting spectrum opportunities, Telecommun. Policy 40 (4) (2016) 319–331. http://dx.doi.org/10.1016/j.telpol.2016.01.003
[7] F.A. Alaba, M. Othman, I.A.T. Hashem, F. Alotaibi, Internet of things security: A survey, J. Netw. Comput. Appl. 88 (Suppl. C) (2017) 10–28. http://dx.doi.org/10.1016/j.jnca.2017.04.002
[8] J. Granjal, E. Monteiro, J.S. Silva, Security for the internet of things: A Survey of existing protocols and open research issues, IEEE Commun. Surv. Tutor. 17 (3) (2015) 1294–1312. http://dx.doi.org/10.1109/COMST.2015.2388550
[9] R. Roman, C. Alcaraz, J. Lopez, N. Sklavos, Key management systems for sensor networks in the context of the internet of things, Comput. Electr. Eng. 37 (2) (2011) 147–159. Modern Trends in Applied Security: Architectures, Implementations and Applications.
[10] J. Granjal, R. Silva, E. Monteiro, J.S. Silva, F. Boavida, Why is IPSec a viable option for wireless sensor networks, in: 2008 5th IEEE International Conference on Mobile Ad Hoc and Sensor Systems, 2008, pp. 802–807. http://dx.doi.org/10.1109/MAHSS.2008.4660130
[11] S. Cirani, G. Ferrari, L. Veltri, Enforcing security mechanisms in the IP-based internet of things: An algorithmic overview, Algorithms 6 (2) (2013) 197–226. http://dx.doi.org/10.3390/a6020197
[12] I. Butun, S.D. Morgera, R. Sankar, A survey of intrusion detection systems in wireless sensor networks, IEEE Commun. Surv. Tutor. 16 (1) (2014) 266–282. http://dx.doi.org/10.1109/SURV.2013.050113.00191
[13] A. Abduvaliyev, A.-S.K. Pathan, J. Zhou, R. Roman, W.-C. Wong, On the vital
areas of intrusion detection systems in wireless sensor networks, IEEE Commun. Surv. Tutor. 15 (3) (2013) 1223–1237. http://dx.doi.org/10.1109/SURV.2012.121912.00006.
[14] R. Mitchell, I.-R. Chen, Review: a survey of intrusion detection in wireless network applications, Comput. Commun. 42 (2014) 1–23. http://dx.doi.org/10.1016/j.comcom.2014.01.012
[15] S. Yi, Z. Qin, Q. Li, Security and privacy issues of fog computing: A survey, in: Wireless Algorithms, Systems, and Applications the 10th International Conference on, 2015, pp. 1–10.
[16] Y. Wang, T. Uehara, R. Sasaki, Fog computing: Issues and challenges in security and forensics, in: 2015 IEEE 39th Annual Computer Software and Applications Conference, vol. 3, 2015, pp. 53–59. http://dx.doi.org/10.1109/COMPSAC.2015.173
[17] S. Sicari, A. Rizzardi, L. Grieco, A. Coen-Porisini, Security, privacy and trust in internet of things: The road ahead, Comput. Netw. 76 (Suppl. C) (2015) 146–164. http://dx.doi.org/10.1016/j.comnet.2014.11.008
[18] R. Roman, J. Lopez, M. Mambo, Mobile edge computing, Fog et al.: A survey and analysis of security threats and challenges, Future Gener. Comput. Syst.(2016). http://dx.doi.org/10.1016/j.future.2016.11.009
[19] V. Oleshchuk, Internet of things and privacy preserving technologies, in: 2009
1st International Conference on Wireless Communication, Vehicular Technology, Information Theory and Aerospace Electronic Systems Technology, 2009, pp. 336–340. http://dx.doi.org/10.1109/WIRELESSVITAE.20095172470
[20] J. Zhou, Z. Cao, X. Dong, A.V. Vasilakos, Security and privacy for cloud-based IoT: Challenges, IEEE Commun. Mag. 55 (1) (2017) 26–33. http://dx.doi.org/10.1109/MCOM.2017.1600363CM
[21] Z.K. Zhang, M.C.Y. Cho, C.W. Wang, C.W. Hsu, C.K. Chen, S. Shieh, IoT security:
Ongoing challenges and research opportunities, in: 2014 IEEE 7th International Conference on Service-Oriented Computing and Applications, 2014,pp. 230–234. http://dx.doi.org/10.1109/SOCA.2014.58
[22] IoT-A, Internet of Things–Architecture IoT-A Deliverable D1.5 –Final architectural reference model for the IoT v3.0, 2013. URL http://iotforum.org/wpcontent/uploads/2014/09/D1.5-0130715-VERYFINAL.pdf
[23] OWASP, Top IoT Vulnerabilities, 2016. URL https://www.owasp.org/index.php/Top_IoT_Vulnerabilities
[24] IEEE, IeEEE Standard for Local and metropolitan networks–Part 15.4: LowRate Wireless Personal Area Networks (LR-WPANs), 2012. URL https://standards.ieee.org/findstds/standard/802.15.4-2011.html
[25] T. Winter, P. Thubert, A. Brandt, J.W. Hui, R. Kelsey, Rfc 6550 - rpl: ipv6 routing protocol for low-power and lossy networks, 2012. URL https://tools.ietf.org/html/rfc6550
[26] J. Postel, User datagram protocol, 1980. URL https://tools.ietf.org/html/rfc768
[27] J.W. Hui, P. Thubert, Compression format for IPv6 datagrams over IEEE802.15.4-based networks, 2011. URL https://tools.ietf.org/html/rfc6282

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 |

|| Volume 11, Issue 3, March 2023 ||

| DOI: 10.15680/IJIRCCE.2023.1103114 |

[28] A. Conta, S. Deering, M. Gupta, Internet control message protocol (ICMPv6) for the internet protocol version 6 (IPv6) specification, 2000
[29] Z. Shelby, K. Hartke, C. Bormann, The constrained application protocol (CoAP),2014. URL https://tools.ietf.org/html/rfc7252
[30] W. Xu, W. Trappe, Y. Zhang, T. Wood, The feasibility of launching and detecting jamming attacks in wireless networks, in: Proceedings of the 6th ACM International Symposium on Mobile Ad Hoc Networking and Computing,MobiHoc '05, ACM, New York, NY, USA, 2005, pp. 46–57. http://dx.doi.org/10.1145/1062689.1062697
[31] G. Noubir, G. Lin, Low-power DoS attacks in data wireless LANs and countermeasures, SIGMOBILE Mob. Comput. Commun. Rev. 7 (3) (2003) 29–30.
[32] S.H. Chae, W. Choi, J.H. Lee, T.Q.S. Quek, Enhanced secrecy in stochastic wireless networks: Artificial noise with secrecy protected zone, Trans. Info. for.Sec. 9 (10) (2014) 1617–1628. http://dx.doi.org/10.1109/TIFS.2014.2341453
[33] Y.-W.P. Hong, P.-C. Lan, C.-C.J. Kuo, Enhancing physical-layer secrecy in multiantenna wireless systems: An overview of signal processing approaches, IEEE Signal Process. Mag. 30 (5) (2013) 29–40.[34] L. Xiao, L.J. Greenstein, N.B. Mandayam, W. Trappe, Channel-Based detection of sybil attacks in wireless networks, IEEE Transa. Inf. Forensics Secur. 4 (3)(2009) 492–503.
[34] Y. Chen, W. Trappe, R.P. Martin, Detecting and localizing wireless spoofing attacks, in: 2007 4th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks, 2017, pp. 193–202.
[35] T. Bhattasali, R. Chaki, A survey of recent intrusion detection systems for wireless sensor network, in: D.C. Wyld, M. Wozniak, N. Chaki, N. Meghanathan, D.Nagamalai (Eds.), Advances in Network Security and Applications: 4th International Conference, CNSA 2011, Chennai, India, July 15–17, 2011, Springer Berlin Heidelberg, Berlin, Heidelberg, 2011, pp. 268–280.
[36] H. Kim, Protection against packet fragmentation attacks at 6LoWPAN adaptation layer, in: 2008 International Conference on Convergence and Hybrid Information Technology, 2008, pp. 796–801. http://dx.doi.org/10.1109/ICHIT.2008.261.
[37] R. Hummen, J. Hiller, H. Wirtz, M. Henze, H. Shafagh, K. Wehrle, 6LoWPAN Fragmentation attacks and mitigation mechanisms, in: Proceedings of the
Sixth ACM Conference on Security and Privacy in Wireless and Mobile Networks, WiSec '13, ACM, New York, NY, USA, 2013, pp. 55–66. http://dx.doi.org/10.1145/2462096.2462107.
[38] R. Riaz, K.-H. Kim, H.F. Ahmed, Security analysis survey and framework design for IP connected LoWPANs, in: 2009 International Symposium on Autonomous Decentralized Systems, 2009, pp. 1–6. http://dx.doi.org/10.1109/ISADS.2009.5207373.
[39] A. Dvir, T. Holczer, L. Buttyan, VeRA - version number and rank authentication in RPL, in: 2011 IEEE Eighth International Conference on Mobile Ad-Hoc and Sensor Systems, 2011, pp. 709–714. http://dx.doi.org/10.1109/MASS.2011.76
[40] K. Weekly, K. Pister, Evaluating sinkhole defense techniques in RPL networks,in: Proceedings of the 2012 20th IEEE International Conference on Network Protocols (ICNP), ICNP '12, IEEE Computer Society, Washington, DC, USA,2012, pp. 1–6. http://dx.doi.org/10.1109/ICNP.2012.6459948.
[41] F. Ahmed, Y.-B. Ko, Mitigation of black hole attacks in Routing Protocol for Low Power and Lossy Networks, Secur. Commun. Netw. 9 (18) (2016) 5143– 5154 SCN-16-0443.R1.
[42] A.A. Pirzada, C. McDonald, Circumventing sinkholes and wormholes in wireless sensor networks, in: International Workshop on Wireless Ad-Hoc Networks, 2005.
[43] W. Wang, J. Kong, B. Bhargava, M. Gerla, Visualisation of wormholes in underwater sensor networks: A distributed approach, Int. J. Secur. Netw. 3 (1)(2008) 10–23.
[44] M. Wazid, A.K. Das, S. Kumari, M.K. Khan, Design of sinkhole node detection mechanism for hierarchical wireless sensor networks, Sec. Commun. Netw. 9 (17) (2016) 4596–4614. http://dx.doi.org/10.1002/sec.1652.
[45] K. Zhang, X. Liang, R. Lu, X. Shen, Sybil attacks and their defenses in the internet of things, IEEE Internet Things J. 1 (5) (2014) 372–383. http://dx.doi.org/10.1109/JIOT.2014.2344013.
[46] G. Wang, M. Mohanlal, C. Wilson, X. Wang, M. Metzger, H. Zheng, B.Y.Zhao, Social turing tests: Crowdsourcing sybil detection, in: Symposium on Network and Distributed System Security, NDSS, 2013.
[47] J. Granjal, E. Monteiro, J.S. Silva, Network-layer security for the Internet of Things using TinyOS and BLIP, Int. J. Commun. Syst. 27 (10) (2014) 1938– 1963. http://dx.doi.org/10.1002/dac.2444.
[48] S. Raza, S. Duquennoy, T. Chung, D. Yazar, T. Voigt, U. Roedig, Securing communication in 6LoWPAN with compressed IPsec, in: 2011 International Conference on Distributed Computing in Sensor Systems and Workshops (DCOSS), 2011, pp. 1–8. http://dx.doi.org/10.1109/DCOSS.2011.5982177.
[49] J. Granjal, E. Monteiro, J.S. Silva, Enabling network-layer security on IPv6 wireless sensor networks, in: 2010 IEEE Global Telecommunications Conference GLOBECOM 2010, 2010, pp. 1–6. http://dx.doi.org/10.1109/GLOCOM.2010.5684293.

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor: 8.379

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details