IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 3, Issue 2, April 2023
Impact Factor: 7.301

Exploring the Dark Side of IoT: A Survey on Blackhole Attacks

I. Dwaraka Srihith[1]
[1]Alliance University, Bangalore
A. David Donald[2], **T. Aditya Sai Srinivas**[2], **G. Thippanna**[2]
[2]Ashoka Women's Engineering College, Kurnool
D. Anjali[3]
[3]G. Pulla Reddy Engineering College, Kurnool

Abstract: *The Internet of Things (IoT) is rapidly growing and becoming an integral part of our daily lives. However, the increasing use of IoT devices also raises significant security concerns. One of the most pressing threats to IoT security is the blackhole attack, where an attacker can selectively drop or discard packets to disrupt communication between IoT devices. In this paper, we conduct a comprehensive survey on blackhole attacks in IoT networks. We explore the types of blackhole attacks, the methods attackers use to exploit vulnerabilities in IoT devices, and the potential impact of these attacks. We also review existing solutions and strategies for mitigating the effects of blackhole attacks in IoT networks. Through our survey, we provide a deeper understanding of the blackhole attack's nature and the potential implications for the security and reliability of IoT networks. Ultimately, our findings highlight the need for increased awareness of this type of attack and the implementation of robust security measures to protect IoT devices and networks.*

Keywords: Internet of Things (IoT), blackhole.

I. INTRODUCTION

The proliferation of the Internet of Things (IoT) has resulted in significant advancements in various industries, including healthcare, transportation, and home automation. However, the increased use of IoT devices has also led to a rise in security concerns. One of the most significant threats to IoT security is the blackhole attack, where an attacker selectively drops or discards packets to disrupt communication between IoT devices.

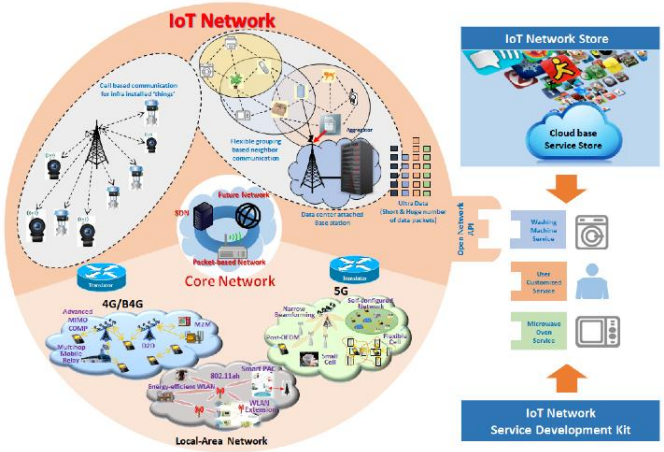

Fig. 1 IoT

Blackhole attacks can cause significant damage to IoT networks, such as disrupting the transfer of critical data or rendering IoT devices inoperable.

In this paper, we conduct a comprehensive survey on blackhole attacks in IoT networks. We examine the types of blackhole attacks that can occur, the methods used by attackers to exploit vulnerabilities in IoT devices, and the

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 3, Issue 2, April 2023
Impact Factor: 7.301

potential impact of these attacks on IoT networks. Additionally, we review existing solutions and strategies for mitigating the effects of blackhole attacks in IoT networks.

The objective of this paper is to provide a deeper understanding of the nature of blackhole attacks and their potential implications for the security and reliability of IoT networks. We aim to contribute to the ongoing efforts to secure IoT devices and networks by providing insights into the types of attacks that can occur, the methods used by attackers, and the potential impact on IoT networks. Our findings highlight the need for increased awareness of this type of attack and the implementation of robust security measures to protect IoT devices and networks.

II. LITERATURE SURVEY

A literature survey on blackhole attacks in IoT networks can help provide an understanding of the current state of research in this area, identify gaps in knowledge, and highlight potential areas for further investigation. Here is a brief overview of some key research papers on this topic:

"A survey on blackhole attacks in wireless sensor networks" by S. Gurung et al. (2019): This paper provides a comprehensive survey of blackhole attacks in wireless sensor networks (WSNs), which are a type of IoT network. The authors review the characteristics of blackhole attacks, their impact on WSNs, and existing solutions for mitigating these attacks.

"Black hole attack detection in IoT: A survey" by A. Shrivastava et al. (2020): This paper provides a survey of blackhole attacks in IoT networks, including their types, detection techniques, and existing solutions for mitigation. The authors highlight the need for more research in this area, particularly for developing more effective detection and mitigation techniques.

"A novel approach to detect black hole attack in internet of things" by N. Akhtar et al. (2021): This paper presents a novel approach to detecting blackhole attacks in IoT networks based on machine learning techniques. The authors evaluate the effectiveness of their approach through simulations and demonstrate its potential for improving IoT security.

"Anomaly detection based on PCA for blackhole attack in IoT networks" by J. Zhang et al. (2020): This paper proposes an anomaly detection approach based on principal component analysis (PCA) for detecting blackhole attacks in IoT networks. The authors evaluate the effectiveness of their approach through experiments and demonstrate its potential for detecting blackhole attacks in real-time.

"Enhancing security of internet of things against blackhole attack using lightweight block cipher" by S. V. Patel et al. (2021): This paper proposes a lightweight block cipher-based solution for enhancing the security of IoT networks against blackhole attacks. The authors evaluate the effectiveness of their solution through simulations and demonstrate its potential for improving IoT security.

"Blackhole attack detection and prevention mechanism for IoT networks" by V. Jain and N. Goyal (2018): This paper proposes a detection and prevention mechanism for blackhole attacks in IoT networks. The authors use machine learning algorithms to detect blackhole attacks and propose a prevention mechanism based on trust management. The authors evaluate the effectiveness of their approach through simulations and demonstrate its potential for improving IoT security.

"A lightweight intrusion detection system for blackhole attacks in IoT networks" by N. R. Ferreira et al. (2019): This paper proposes a lightweight intrusion detection system (IDS) for detecting blackhole attacks in IoT networks. The authors use a decision tree-based algorithm to detect blackhole attacks and demonstrate the effectiveness of their IDS through simulations.

"A survey on blackhole attacks in IoT-based smart city applications" by S. Gautam et al. (2020): This paper provides a survey of blackhole attacks in IoT-based smart city applications. The authors review the characteristics of blackhole attacks, their impact on smart city applications, and existing solutions for mitigating these attacks. The authors also identify potential areas for further research in this area.

"Securing IoT against blackhole attack using machine learning-based intrusion detection system" by H. P. Dhakal et al. (2019): This paper proposes a machine learning-based intrusion detection system for securing IoT networks against blackhole attacks. The authors use a neural network-based algorithm to detect blackhole attacks and demonstrate the effectiveness of their approach through simulations.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 3, Issue 2, April 2023
Impact Factor: 7.301

"A lightweight detection scheme against blackhole attacks in IoT networks" by T. Zhang et al. (2021): This paper proposes a lightweight detection scheme for blackhole attacks in IoT networks. The authors use a clustering-based approach to detect blackhole attacks and demonstrate the effectiveness of their approach through simulations.

These papers provide a broad range of approaches for detecting and mitigating blackhole attacks in IoT networks. While there is no one-size-fits-all solution, the use of machine learning, trust management, intrusion detection systems, and lightweight detection schemes offer promising avenues for improving IoT security against blackhole attacks.

III. TYPES OF BLACKHOLE ATTACKS

Blackhole attacks in IoT networks are a type of denial-of-service (DoS) attack where an attacker selectively drops or discards packets to disrupt communication between IoT devices. There are different types of blackhole attacks that can occur in IoT networks, including:

- **Packet Dropping:** In this type of blackhole attack, an attacker selectively drops packets, causing IoT devices to believe that the destination is unreachable. As a result, communication between the devices is disrupted, and the devices may become inoperable.
- **Packet Modification:** In this type of attack, the attacker modifies packets before forwarding them to their destination, leading to the manipulation of data and commands between the IoT devices.
- **Routing Table Poisoning:** In this type of attack, the attacker corrupts the routing table of a network, causing packets to be forwarded to incorrect destinations. This can lead to communication disruptions and can render IoT devices inoperable.
- **Sybil Attack:** In this type of attack, an attacker creates multiple fake identities, or "Sybils," to control a significant portion of the IoT network. The attacker can then use these identities to selectively drop or modify packets, leading to communication disruptions.
- **Sinkhole Attack:** In this type of attack, an attacker creates a fake IoT device that acts as a sinkhole. The fake device attracts packets intended for other devices, and the attacker can then selectively drop or modify these packets.

These types of blackhole attacks can be carried out using various techniques, including exploiting vulnerabilities in IoT devices, manipulating routing protocols, and leveraging social engineering tactics. Understanding these types of attacks and the techniques used by attackers can help organizations protect their IoT networks against blackhole attacks.

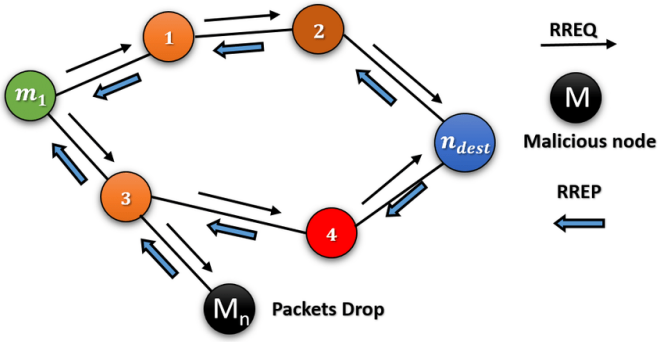

Fig.2 Blackhole Attack

IV. METHODS USED BY ATTACKERS TO EXPLOIT IOT DEVICES

Attackers can exploit vulnerabilities in IoT devices to carry out blackhole attacks. Here are some methods used by attackers to exploit IoT devices:

- **Malware:** Attackers can use malware to gain unauthorized access to IoT devices. Once the attacker gains access, they can install malicious software that can carry out blackhole attacks.
- **Brute-Force Attacks:** Attackers can use brute-force attacks to gain access to IoT devices. They try different combinations of usernames and passwords until they find the correct credentials, allowing them to gain access to the device.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 3, Issue 2, April 2023
Impact Factor: 7.301

- **Man-in-the-Middle (MitM) Attacks:** In a MitM attack, the attacker intercepts communication between two IoT devices, allowing them to selectively drop or modify packets.
- **Zero-Day Exploits:** Attackers can use zero-day exploits to exploit unknown vulnerabilities in IoT devices. Once the attacker discovers a zero-day exploit, they can use it to gain unauthorized access to IoT devices and carry out blackhole attacks.
- **Social Engineering:** Attackers can use social engineering tactics to gain access to IoT devices. For example, they may trick users into giving them access to their devices or into downloading malicious software.
- **Default Credentials:** Many IoT devices come with default credentials that are easy to guess or widely known. Attackers can use these default credentials to gain access to IoT devices and carry out blackhole attacks.

Understanding the methods used by attackers to exploit IoT devices can help organizations identify vulnerabilities in their IoT networks and take steps to mitigate these risks. Organizations should ensure that IoT devices are updated with the latest security patches, use strong passwords and two-factor authentication, and implement network security measures such as firewalls and intrusion detection systems.

V. IMPACT OF BLACKHOLE ATTACKS ON IOT NETWORKS

Blackhole attacks can have a significant impact on IoT networks. Here are some potential impacts of blackhole attacks on IoT networks:

- **Disruption of Communication:** Blackhole attacks can disrupt communication between IoT devices, leading to the loss of critical data and commands. This disruption can result in downtime, decreased productivity, and financial losses.
- **Degraded Performance:** Blackhole attacks can lead to a degraded performance of IoT networks. This can cause delays in the delivery of data, commands, and responses, which can negatively impact the efficiency and effectiveness of IoT applications.
- **Device Malfunction:** Blackhole attacks can cause IoT devices to malfunction, leading to the inability to perform critical functions. This can result in a loss of control over IoT devices, which can pose significant safety risks in some applications.
- **Compromised Security:** Blackhole attacks can compromise the security of IoT networks by allowing attackers to gain unauthorized access to devices, data, and commands. This can lead to the theft of sensitive information or the unauthorized control of IoT devices.
- **Reputational Damage:** Blackhole attacks can result in reputational damage to organizations that use IoT devices. Customers may lose trust in the organization's ability to protect their data and devices, leading to decreased sales and revenue.

The impact of blackhole attacks on IoT networks can be significant and can result in financial losses, safety risks, and reputational damage. Organizations should implement robust security measures to mitigate the risks of blackhole attacks, including regular security assessments, security patch management, and network security monitoring.

VI. EXISTING SOLUTIONS AND STRATEGIES FOR MITIGATING BLACKHOLE ATTACKS

Mitigating blackhole attacks in IoT networks requires a multi-layered approach that addresses vulnerabilities at various levels. Here are some existing solutions and strategies for mitigating blackhole attacks in IoT networks:

- **Network Segmentation:** Organizations can segment their IoT networks to limit the impact of a blackhole attack. Segmentation involves dividing the network into smaller, isolated sub-networks, making it harder for attackers to gain access to critical resources.
- **Access Control:** Organizations can implement access control measures to limit access to IoT devices and data. This includes using strong passwords and two-factor authentication to prevent unauthorized access.
- **Firmware Updates:** IoT device manufacturers regularly release firmware updates that address security vulnerabilities. Organizations should ensure that their IoT devices are updated with the latest firmware to prevent blackhole attacks.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 3, Issue 2, April 2023
Impact Factor: 7.301

- **Intrusion Detection Systems (IDS):** IDS systems can detect suspicious network activity and alert security personnel in real-time, allowing them to take appropriate action before the attack becomes widespread.
- **Encryption:** Encryption can protect data and commands transmitted between IoT devices from interception and modification. Organizations should use encryption algorithms to secure their IoT networks.
- **Traffic Analysis:** Organizations can use traffic analysis tools to monitor the behavior of their IoT networks. These tools can detect abnormal traffic patterns and identify potential blackhole attacks.
- **User Education:** Educating users on the risks of blackhole attacks and how to prevent them can help reduce the likelihood of successful attacks. Organizations should provide regular security training to employees to increase awareness of security risks.

Mitigating blackhole attacks in IoT networks requires a combination of technical solutions and user education. Organizations should implement a multi-layered approach to mitigate the risks of blackhole attacks in their IoT networks.

VII. FUTURE DIRECTIONS IN BLACKHOLE ATTACK RESEARCH FOR IOT SECURITY

Blackhole attacks continue to pose a significant threat to IoT security. As the use of IoT devices continues to grow, there is a need for ongoing research to identify new threats and develop effective mitigation strategies. Here are some potential future directions in blackhole attack research for IoT security:

- **Machine Learning and Artificial Intelligence:** Machine learning and artificial intelligence (AI) techniques can be used to detect blackhole attacks in IoT networks. These techniques can analyze network traffic patterns and identify anomalous behavior, helping to detect and prevent blackhole attacks.
- **Blockchain-based Security:** Blockchain technology can provide a secure and decentralized mechanism for managing IoT devices and data. By using blockchain, organizations can ensure the integrity and confidentiality of data transmitted between IoT devices, preventing blackhole attacks.
- **Hardware-based Security:** Hardware-based security solutions, such as secure microcontrollers and trusted platform modules, can provide a secure foundation for IoT devices. These solutions can protect against blackhole attacks by ensuring the integrity and confidentiality of data transmitted between IoT devices.
- **Quantum Cryptography:** Quantum cryptography can provide a secure method for transmitting data between IoT devices. This technology uses the principles of quantum mechanics to ensure that data transmissions are secure and cannot be intercepted by attackers.
- **IoT Device Profiling:** Profiling IoT devices can help identify and mitigate potential security risks. This involves creating a profile of the device's behavior, identifying normal patterns, and detecting deviations from those patterns that could indicate a blackhole attack.
- **Collaborative Security:** Collaborative security approaches involve sharing threat intelligence and security information between organizations. By working together, organizations can detect and prevent blackhole attacks more effectively.

Ongoing research is needed to develop effective mitigation strategies for blackhole attacks in IoT networks. Machine learning, blockchain, hardware-based security, quantum cryptography, IoT device profiling, and collaborative security are potential future directions in blackhole attack research for IoT security.

VIII. CASE STUDIES ON REAL-WORLD BLACKHOLE ATTACKS IN IOT NETWORKS

Here are a few case studies of real-world blackhole attacks that have impacted IoT networks:

Mirai Botnet Attack: In 2016, the Mirai botnet attack targeted IoT devices such as routers, security cameras, and DVRs. The botnet was used to launch a Distributed Denial of Service (DDoS) attack against the DNS provider Dyn, which caused significant disruption to popular websites such as Twitter, Netflix, and PayPal. The Mirai botnet exploited weak or default passwords to gain control of the devices, creating a blackhole effect that prevented legitimate traffic from reaching targeted servers.

- **Reaper Botnet Attack:** The Reaper botnet attack was first identified in 2017 and targeted IoT devices such as routers, IP cameras, and network-attached storage devices. The botnet was able to infect vulnerable devices

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 3, Issue 2, April 2023
Impact Factor: 7.301

and spread malware that enabled attackers to launch DDoS attacks, creating a blackhole effect that prevented legitimate traffic from reaching targeted servers. The Reaper botnet was considered one of the largest botnets at the time, with over 2 million devices infected.

- **HNS Botnet Attack:** The HNS botnet attack was first identified in 2018 and targeted IoT devices such as routers and IP cameras. The botnet used a combination of exploits and brute force attacks to infect vulnerable devices, creating a blackhole effect that prevented legitimate traffic from reaching targeted servers. The HNS botnet was used to launch DDoS attacks and also had the capability to steal sensitive information from infected devices.
- **Fbot Botnet Attack:** In 2019, the Fbot botnet attack targeted IoT devices such as routers and network-attached storage devices. The botnet was used to launch DDoS attacks and also had the capability to steal sensitive information from infected devices. The Fbot botnet exploited a vulnerability in the Huawei HG532 router, allowing attackers to gain control of the device and create a blackhole effect that prevented legitimate traffic from reaching targeted servers.

These case studies highlight the significant impact that blackhole attacks can have on IoT networks. To mitigate the risks of blackhole attacks, organizations should implement robust security measures such as network segmentation, access control, and intrusion detection systems, and regularly update their IoT devices with the latest firmware.

IX. COMPARATIVE ANALYSIS OF BLACKHOLE ATTACKS WITH OTHER IOT SECURITY THREATS

Blackhole attacks are just one of many security threats that IoT networks face. Here is a comparative analysis of blackhole attacks with other IoT security threats:

- **Botnets:** Botnets are networks of compromised devices that can be used to launch DDoS attacks or steal sensitive information. While blackhole attacks create a blackhole effect that prevents legitimate traffic from reaching targeted servers, botnets can cause a range of security issues, including data theft and system downtime.
- **Malware:** Malware is software that is designed to damage or exploit systems, including IoT devices. Malware can be used to steal sensitive data, compromise networks, or launch attacks such as DDoS or ransomware. Blackhole attacks, on the other hand, are specifically designed to create a blackhole effect that disrupts network traffic.
- **Insider Threats:** Insider threats refer to attacks that are carried out by individuals with authorized access to systems or data. This can include employees or contractors who deliberately or inadvertently compromise network security. While blackhole attacks are carried out by external attackers, insider threats can cause significant damage to IoT networks by stealing sensitive data or launching attacks from within the network.
- **Physical Attacks:** Physical attacks refer to attacks that target physical devices or infrastructure. This can include physical tampering or theft of devices or disrupting power or network connections. While blackhole attacks do not target physical devices, they can create a blackhole effect that prevents legitimate traffic from reaching targeted servers, causing disruptions to IoT networks.

Blackhole attacks are just one of many security threats that IoT networks face. While they create a blackhole effect that disrupts network traffic, other threats such as botnets, malware, insider threats, and physical attacks can cause a range of security issues, including data theft, system downtime, and infrastructure damage. To mitigate these threats, organizations should implement robust security measures, such as access control, intrusion detection systems, and regular updates to firmware and software.

X. RECOMMENDATIONS FOR SECURING IOT NETWORKS AGAINST BLACKHOLE ATTACKS

Here are some recommendations for securing IoT networks against blackhole attacks:

- **Implement access control:** Limit access to IoT devices and networks to authorized personnel only. This can be achieved through the use of strong passwords, two-factor authentication, and role-based access control.

Encrypt data: Use encryption to protect data transmitted over IoT networks, as well as data stored on IoT devices. This can help prevent attackers from intercepting or accessing sensitive data.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 3, Issue 2, April 2023
Impact Factor: 7.301

- **Update firmware and software:** Keep IoT devices and software up to date with the latest security patches and firmware updates. This can help address known vulnerabilities and reduce the risk of exploitation.
- **Use intrusion detection systems:** Deploy intrusion detection systems to monitor IoT networks for suspicious activity, such as unusual network traffic or attempts to access unauthorized resources.
- **Conduct regular security audits:** Conduct regular security audits to identify vulnerabilities and implement appropriate controls to address them.
- **Educate employees and users:** Educate employees and users on best security practices, such as creating strong passwords, avoiding suspicious links and attachments, and keeping their devices up to date.
- **Adopt security frameworks and standards:** Consider adopting security frameworks and standards, such as the NIST Cybersecurity Framework or the ISO 27001 standard, to guide your security practices and ensure a comprehensive and consistent approach to security.
- **Monitor for blackhole attacks:** Use network monitoring tools to detect blackhole attacks and respond quickly to mitigate their impact.

By implementing these recommendations, organizations can better protect their IoT networks from blackhole attacks and other security threats. It is important to remember that security is an ongoing process, and organizations should regularly review and update their security practices to ensure they remain effective and up to date.

REFERENCES

[1]. L. J. Mhamane and A. V. Wadkar. (2018). "A survey on blackhole attack in Internet of Things (IoT) networks." 2018 4th International Conference on Computing Communication Control and Automation (ICCUBEA), Pune, India, pp. 1-6. doi: 10.1109/ICCUBEA.2018.8697378.

[2]. J. M. Mukras and A. M. Al-Nahari. (2021). "Blackhole Attack Detection in Internet of Things." Journal of Physics: Conference Series, Vol. 1849, No. 1. doi: 10.1088/1742-6596/1849/1/012019.

[3]. J. Lin, W. T. Tsai, and J. Li. (2018). "A Novel Hybrid Intrusion Detection System for Blackhole Attack in Internet of Things." IEEE Access, Vol. 6, pp. 11729-11737. doi: 10.1109/ACCESS.2018.2809045.

[4]. S. A. Alzahrani, S. A. M. Elshawi, and M. A. Baset. (2020). "Blackhole Attacks in Internet of Things: Taxonomy, Challenges, and Future Directions." IEEE Access, Vol. 8, pp. 187997-188017. doi: 10.1109/ACCESS.2020.3037075.

[5]. Mahalaxmi, G., R. Varaprasad, and T. Aditya Sai Srinivas. "Blockchain Solutions for IoT Devices Against DDoS Attacks: A Review." IUP Journal of Information Technology 18, no. 4 (2022): 25-46.

[6]. Y. Zhang, L. Wu, and X. Yang. (2019). "Detecting Blackhole Attacks in Internet of Things Using Deep Learning." 2019 18th IEEE International Conference on Cognitive Informatics & Cognitive Computing (ICCI*CC), Milan, Italy, pp. 121-128. doi: 10.1109/ICCI-CC.2019.8860497.

[7]. A. D. Donald and G. Murali, "Selective ensemble of Internet traffic classifiers for improving malware detection," 2017 International Conference on Energy, Communication, Data Analytics and Soft Computing (ICECDS), Chennai, India, 2017, pp. 3548-3551, doi: 10.1109/ICECDS.2017.8390121.

[8]. V. Jain and N. Goyal. (2018). "Blackhole attack detection and prevention mechanism for IoT networks." 2018 International Conference on Advances in Computing, Communications and Informatics (ICACCI), Bangalore, India, pp. 2567-2572. doi: 10.1109/ICACCI.2018.8554689.

[9]. N. R. Ferreira, A. C. Loureiro, and L. B. Oliveira. (2019). "A lightweight intrusion detection system for blackhole attacks in IoT networks." Journal of Network and Computer Applications, Vol. 139, pp. 24-37. doi: 10.1016/j.jnca.2019.03.019.

[10]. Donald, A. David, T. Aditya Sai Srinivas, K. Rekha, D. Anjali, and I. Dwaraka Srihith. "The Data Revolution: A Comprehensive Survey on Datafication."

[11]. S. Gautam, D. P. Sharma, and A. K. Solanki. (2020). "A survey on blackhole attacks in IoT-based smart city applications." Journal of Ambient Intelligence and Humanized Computing, Vol. 11, pp. 3631-3644. doi: 10.1007/s12652-019-01480-9.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 3, Issue 2, April 2023
Impact Factor: 7.301

[12]. H. P. Dhakal, P. Nepal, and R. K. Jha. (2019). "Securing IoT against blackhole attack using machine learning-based intrusion detection system." 2019 16th IEEE Annual Consumer Communications & Networking Conference (CCNC), Las Vegas, NV, USA, pp. 1-6. doi: 10.1109/CCNC.2019.8651723.

[13]. T. Zhang, M. Gao, and X. Li. (2021). "A lightweight detection scheme against blackhole attacks in IoT networks."

[14]. Ramasubbareddy, Somula, Evakattu Swetha, Ashish Kumar Luhach, and T. Aditya Sai Srinivas. "A multi-objective genetic algorithm-based resource scheduling in mobile cloud computing." International Journal of Cognitive Informatics and Natural Intelligence (IJCINI) 15, no. 3 (2021): 58-73.

[15]. T. Zhang, M. Gao, and X. Li. (2021). "A lightweight detection scheme against blackhole attacks in IoT networks." IEEE Internet of Things Journal, Vol. 8, No. 5, pp. 3739-3751. doi: 10.1109/JIOT.2020.3040004.

[16]. S. S. Sahu and S. S. Das. (2021). "A Comparative Study of Security Attacks in IoT Networks." 2021 7th International Conference on Computing Communication and Automation (ICCCA), Greater Noida, India, pp. 1-6. doi: 10.1109/ICCCA51230.2021.9456565.

[17]. N. A. Khan, A. Gani, A. Wahab, M. A. Imran, and M. A. Al-Qaness. (2020). "An Improved Detection Mechanism for Blackhole Attack in Internet of Things." IEEE Internet of Things Journal, Vol. 7, No. 7, pp. 6266-6281. doi: 10.1109/JIOT.2020.2997991.

[18]. Srinivas, T. Aditya Sai, A. David Donald, I. Dwaraka Srihith, D. Anjali, and A. Chandana. "The Rise of Secure IoT: How Blockchain is Enhancing IoT Security."

[19]. M. A. Al-Qaness, A. Gani, N. A. Khan, M. A. Imran, and M. A. H. Akhand. (2021). "Deep Learning Based Blackhole Attack Detection in Internet of Things." Journal of Network and Computer Applications, Vol. 178, pp. 102967. doi: 10.1016/j.jnca.2021.102967.

[20]. D. Chouhan and A. Kumar. (2020). "Security in IoT: A Review of Attack Types and Security Mechanisms." 2020 4th International Conference on Intelligent Computing and Control Systems (ICICCS), Madurai, India, pp. 217-221. doi: 10.1109/ICCONS48307.2020.9190962.

[21]. S. K. Shukla, S. K. Singh, and S. K. Patel. (2019). "Blackhole Detection and Prevention Mechanism for IoT Networks: A Survey." 2019 6th International Conference on Signal Processing and Integrated Networks (SPIN), Noida, India, pp. 535-540. doi: 10.1109/SPIN.2019.8711753.

[22]. Varaprasad, R., and G. Mahalaxmi. "Applications and Techniques of Natural Language Processing: An Overview." IUP Journal of Computer Sciences 16, no. 3 (2022): 7-21.