International Research Journal of Multidisciplinary Scope (IRJMS), 2024; 5(3):894-906

Review Article | ISSN (O): 2582-631X DOI: 10.47857/irjms.2024.v05i03.0885

A Comprehensive Survey on Applications, Security Concerns, Attack Mitigation and Secure Routing in IoT

Azmera Chandu Naik[1], Madhu Kumar Vanteru[2], Bandru Sanjeev[3], Sravan Kumar V[4], Karthik Kumar Vaigandla[1]*

[1]Department of Computer Science and Engineering, CVR College of Engineering, Telangana, India, [2]Department of Electronics and Communication Engineering, Balaji Institute of Technology and Science, Telangana, India, [3]Department of IT, Sreenidhi Institute of Science and Technology, Telangana, India, [4]Department of Computer Science and Engineering, Balaji Institute of Technology and Science, Telangana, India. *Corresponding Author's Email: vkvaigandla@gmail.com

Abstract

The widespread adoption of Internet of Things (IoT) technologies presents considerable challenges in terms of security, vulnerability, and privacy. This paper conducts a comprehensive review of IoT applications, focusing on emerging trends and their wide-ranging impacts. Emphasis is placed on critical security issues, advocating for strong measures to mitigate attacks and improve system resilience. The paper highlights innovative attack mitigation strategies and the role of secure routing in upholding data integrity and network resilience. It examines the applications of deep learning approaches in enhancing IoT security and efficiency. The paper explores the interaction between technological progress and security issues in IoT, culminating with a call for ongoing research and development to advance security protocols and leverage new technologies, addressing the evolving IoT landscape.

Keywords: Applications, Attack mitigation, IoT, Routing, Security.

Introduction

The IoT stands as a pivotal advancement in the technological landscape, integrating a diverse array of devices into a connected network. This innovation extends beyond standard computing devices to incorporate everyday objects, all equipped with sensors and the ability to communicate data. The proliferation of IoT devices is significantly transforming numerous sectors, including healthcare, smart cities, and industrial applications. According to recent studies, the number of connected IoT devices is projected to reach 25.4 billion by 2030, highlighting the expansive growth in this field. This widespread adoption underscores the critical importance of addressing security issues associated with IoT. The integration of IoT devices in various domains introduces numerous vulnerabilities, making it imperative to implement robust security measures to safeguard sensitive data and ensure the integrity and reliability of IoT systems.

The essence of IoT lies in its ability to bridge the physical and digital realms, enabling objects to interact and respond intelligently to various stimuli and conditions (1). The key components of IoT systems include data-gathering sensors, connectivity options such as Wi-Fi and Bluetooth, and data-processing units, all working in concert to facilitate a new level of interaction between devices and their environments. IoT's significance in the contemporary world is profound, marking a revolution in how technology can be applied across various sectors. Its relevance spans numerous fields, from healthcare, where it enables remote patient monitoring and personalized treatments, to agriculture, where it aids in precision farming and resource management (2).

IoT contributes to the fourth Industrial Revolution and Industry 4.0with its devices and systems integral in sensing, gathering, and storing data. This data is processed through a network of connected devices,

(Received 2nd April 2024; Accepted 15th July 2024; Published 30th July 2024)

often involving cloud-based servers, which are vital for high-performance data processing and energy-efficient operations. The processed data from IoT systems is pivotal for making informed decisions across various operational levels, enabling real-time interactions among different sectors. The economic impact of IoT is substantial, projected to increase from $3.9 trillion to $11.1 trillion in the next two years, reflecting its extensive applications in industries such as healthcare, transportation, energy, supply chain management, and manufacturing (3).

Challenges pervade the IoT domain, not least of which are security and privacy issues arising from the highly sensitive data at stake. Technical hurdles manifest in the form of communication standards, hardware and software integration, and the cultivation of IoT-related expertise, which are considerable obstacles (4). Factors of a regulatory, legislative, and cultural nature also play a part in shaping the widespread acceptance and effective implementation of IoT technologies. In the implementation of IoT, particular challenges include ensuring reliable connectivity, strong security, and interoperability among devices, systems, and software (5). The burgeoning number of interconnected devices brings to the fore concerns regarding network coverage, availability, security, and energy use. Furthermore, the diversity and quantity of security threats present significant risks, highlighting the necessity for the identification, authentication, and management of endpoint devices to safeguard the integrity of data transmission. The intent of this review is to execute an extensive examination of the IoT, concentrating on four pivotal elements: application domains, security issues, countermeasure strategies, and the integrity of data transmission. Delving into these sectors, the document endeavors to furnish an in-depth comprehension of both the present landscape and the prospective advancements in IoT technologies. Additionally, it addresses the impediments and strategies pivotal to the secure and efficient deployment of these technologies.

Scope

This section presents the scope of the paper, focusing on four pivotal areas: applications, security concerns, attack mitigation strategies, and secure routing.

Applications of IoT

The paper will explore the myriad applications of IoT across various sectors. Each application will be examined to understand how IoT technologies are being used to enhance efficiency, productivity, and user experience. This section aims to showcase the versatility and transformative potential of IoT in different contexts as below.

Home Automation: This section explores how IoT devices facilitate automated control and monitoring of household systems, enhancing convenience, energy efficiency, and security.

Industrial IoT (IIoT): This part examines the integration of advanced technologies in industrial operations, focusing on improving efficiency, reducing costs, and enhancing safety protocols.

Smart Cities: This section delves into the use of IoT solutions in urban environments, improving urban management and planning through smart traffic management, waste management, energy distribution, and public safety.

Healthcare IoT (IoMT): This segment addresses the significant role of IoT in healthcare, enabling continuous patient monitoring, telehealth services, and personalized healthcare approaches.

Security Concerns in IoT

A primary obstacle to the widespread acceptance of IoT pertains to its security. This segment will probe into the array of security challenges linked with IoT, including the intrinsic vulnerabilities of IoT devices and networks, concerns regarding data privacy, and the repercussions of these security threats. Attack Mitigation Strategies in IoT: s a countermeasure to these security predicaments, this segment will examine the array of strategies and technological solutions being crafted and employed to counteract assaults on IoT frameworks. Secure Routing in IoT: The integrity and efficiency of IoT systems are heavily dependent on secure and efficient routing of data. This section will focus on the challenges in IoT routing, including the need for data integrity, confidentiality, and the prevention of data tampering and interception.

This comprehensive review of the IoT is significant for its holistic coverage of IoT applications, security concerns, attack mitigation strategies, and secure routing, offering valuable insights for a diverse audience including policymakers, industry professionals, researchers, and educators. It underscores the criticality of security and privacy in IoT, catalyzes further research and innovation, and informs policy and regulatory frameworks. The review also serves as an essential academic reference, elucidating the complexities and potentials of IoT technologies and their impact across various sectors.

The composition of this document is delineated as follows: Section 2 delineates various extant and nascent applications within the IoT sphere. Section 3 elucidates the security concerns within IoT, encompassing a synopsis of security challenges, susceptibilities, and privacy issues. Section 4 elucidates strategies for the mitigation of attacks, and Section 5 scrutinizes the concept of secure routing in IoT. Section 6 introduces deep learning methodologies pertinent to the issues discussed in this document. The principal discoveries of this investigation are elaborated upon in Section 7, while the paper is concluded in Section 8. Figure 1 depicts the structural layout of this document.

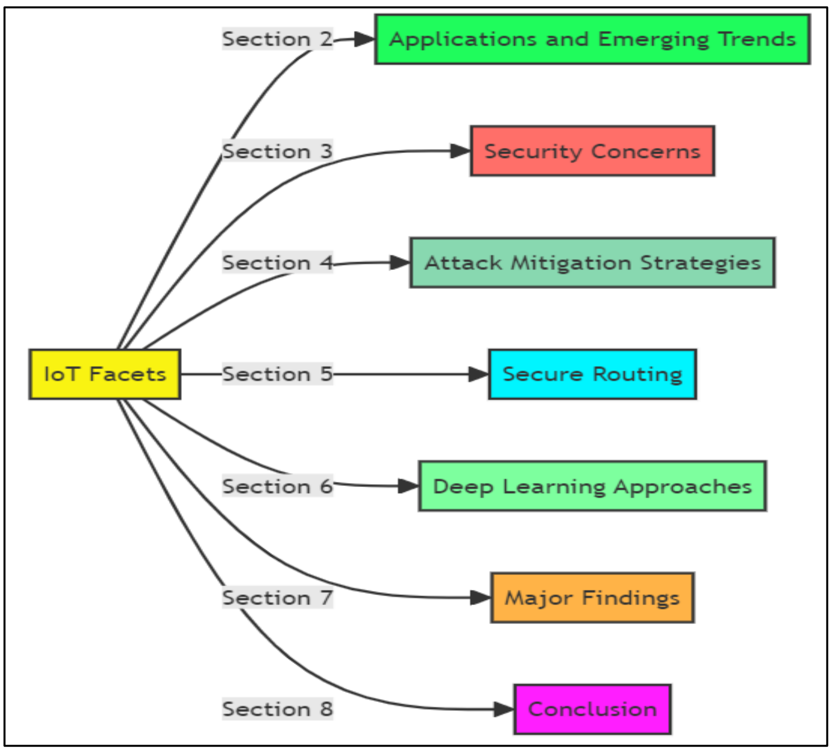

Figure 1: Organization of Review

Applications of IoT

This section provides a comprehensive overview of IoT applications in various sectors and also discusses emerging applications, highlighting the expansive and evolving nature of IoT across various sectors.

Home Automation

Home automation, as a pivotal application of IoT, transforms conventional residences into smart homes. In this arena, IoT devices facilitate automated control and monitoring of household systems such as lighting, heating, and security (6). These devices allow users to manage home functions remotely, enhancing convenience, improving energy efficiency, and bolstering security. Advanced smart home solutions integrate a variety of IoT elements, like sensors for environmental monitoring and connectivity solutions for seamless device interaction, creating responsive and integrated living environments. Modern smart home systems encompass intelligent energy meters, health tracking, and even smart surveillance, ensuring not just ease of living but also energy conservation and heightened security (7). IoT in home automation extends to sophisticated functionalities like user tracking for personalized device control, employing edge computing for efficient data processing and minimizing energy costs. This holistic approach to home automation underscores the transformative impact of IoT on daily life (8).

Industrial IoT (IIoT)

IIoT represents a paradigm shift in manufacturing and production, integrating advanced technologies such as sensors, connected machinery, and data analytics to revolutionize industrial operations, improves infrastructure, and ensures a higher quality of life for residents (9). This integration leads to markedly improved efficiency, reduced operational costs, and enhanced safety protocolsfacilitates prognostic maintenance, permitting enterprises to foresee equipment malfunctions prior to their occurrence, thus curtailing both downtime and maintenance expenses.Real-time monitoring of assets becomes a cornerstone in IIoT, facilitating immediate responses to operational changes and maintaining continuous production flows (10). Moreover, IIoT is instrumental in refining production workflows, guaranteeing resource utilization is maximized, and elevating the caliber of products. Through the exploitation of big data analytics and machine learning, IIoT infrastructures are capable of scrutinizing extensive data setsto uncover insights, drive innovation, and create more responsive and intelligent industrial environments. This transformation not only elevates the capabilities of individual factories but also reshapes entire supply chains, leading to more resilient and adaptive industrial ecosystems.

Smart Cities and Infrastructure

IoT is pivotal to the evolution of urban environments, considerably advancing urban management and planning. Within intelligent urban landscapes, IoT solutions are deployed for the management of traffic through sensors and real-time data analytics to streamline traffic, alleviate congestion, and bolster road safety. Waste management undergoes a transformation with IoT-powered smart bins and waste collection systems, which signal municipal services upon reaching capacity, thereby enhancing the efficiency of waste collection routes and schedules. In the domain of energy distribution, IoT holds a vital role in the regulation and equalization of energy loads, aiding in the establishment of intelligent grids capable of adapting to fluctuating energy demands, incorporating sustainable energy sources, and curtailing overall energy usage. This progression fosters the creation of more sustainable and environmentally congenial cities.Public safety is another crucial area where IoT contributes significantly. Smart surveillance systems, emergency response mechanisms, and disaster management strategies are improved with the integration of IoT devices and systems. For instance, sensors can detect environmental changes or structural weaknesses in buildings, triggering early warning systems for natural disasters or structural failures. Additionally, IoT facilitates better water management in urban areas, monitoring water quality and consumption, and detecting leaks or losses in the system. This is essential for conserving water resources and ensuring safe water supply.

IoT's impact on smart cities extends to various aspects of urban life, making cities more efficient, sustainable, and livable. It enhances resource management, cities more adaptive and resilient to the challenges of urbanization and climate change (11).

Healthcare IoT

The Internet of Medical Things (IoMT) considerably boosts healthcare provision by enabling continuous patient surveillance, telehealth services, and tailored healthcare approaches. Wearable health gadgets and interconnected medical equipment are fundamental to this progression, delivering instantaneous health data that are essential for the enhancement of patient results and the amplification of healthcare service efficacy. These advancements enable continuous remote monitoring of patients, providing critical data on various health parameters, which is essential for chronic disease management and preventive healthcare. Additionally, IoMT is instrumental in telemedicine, offering remote consultations and diagnosis, thereby making healthcare more accessible, especially in remote or underserved areas (12).

The contribution of IoMT reaches into the realm of predictive analytics within healthcare, utilizing data to preempt potential health concerns and facilitating early intervention. The synergy of IoMT with advanced technologies like big data, blockchain, and edge computing bolsters the security and heightens the efficiency of healthcare provision (13). Nevertheless, these advancements are accompanied by challenges, which include safeguarding the privacy and security of delicate health data and surmounting technical hurdles associated with scalability, immediacy in operations, resource limitations, and energy expenditure. Tackling these issues is imperative for the sustained progression and proficient deployment of IoMT frameworks.

Emerging IoT Applications

Sophisticated IoT applications are significantly impacting various sectors, demonstrating the breadth and versatility of this technology. In AgriTech, precision agriculture is being revolutionized through IoT, enabling more sustainable farming practices by optimizing resource use, such as water and fertilizers, thus enhancing productivity and environmental stewardship (14). The transportation and logistics sector is witnessing a transformation with IoT-driven traffic pattern discovery and optimization, leading to more efficient urban mobility and reduced environmental impact (15). Environmental monitoring has taken a leap forward with IoT systems, particularly in smart cities, where real-time air pollution monitoring and control are becoming more sophisticated and responsive, contributing to healthier urban environments (16). The energy sector is not left behind, as smart grids powered by IoT are reshaping energy distribution and consumption, making it more efficient and sustainable, thereby addressing some of the critical challenges in energy management (17). In the retail domain, IoT is creating advanced, integrated multichannel retail settings, enhancing consumer engagement through personalized experiences and efficient inventory management, marking a significant shift in how retail businesses operate and interact with customers (18). These advancements collectively highlight the transformative potential of IoT across diverse sectors, paving the way for more efficient, sustainable, and consumer-friendly practices.

IoT stands as a transformative force in the technological landscape, driving significant advancements across multiple sectors. From enhancing home automation to revolutionizing industrial processes, healthcare, smart city infrastructure, agriculture, and transportation logistics, IoT has demonstrated its versatility and impact. It not only streamlines operations and enhances efficiency but also significantly improves the quality of life by offering smarter, more sustainable solutions.

Table 1 gives a broad classification of literature covered in this paper to get a quick glimpse of the issues reviewed.

Table 1: Classification of Reviewed Literature

Area of Interest	Key Papers	Key Aspects
Applications	(6), (8), (15)	IoT-enabled home automation systems enhancing energy efficiency and security; Industrial IoT (IIoT) applications improving operational efficiency and predictive maintenance; Smart city applications for urban management and sustainability.
Security Problems	(19-21)	Analysis of common IoT device vulnerabilities; Challenges in ensuring data privacy in IoT networks; Issues with current encryption methods and the need for lightweight cryptographic solutions for resource-constrained devices.
Attack Mitigation	(22-24)	Utilization of Simple Network Management Protocol (SNMP) for detecting IoT-based attacks; Application of blockchain technology to prevent Distributed Denial of Service (DDoS) attacks; Machine learning models for real-time intrusion detection.

Secure Routing	(25-27)	Trust-based routing protocols to enhance network reliability; Integration of Software-Defined Networking (SDN) for flexible and secure routing; Optimization of routing protocols for efficient data transmission in low-power and lossy networks.
Privacy Preservation	(28-29)	Implementation of privacy-preserving authentication protocols using blockchain; Development of context-aware privacy-preserving methods for smart cities; Fine-grained access control mechanisms to protect sensitive IoT data.
Emerging Technologies	(30-31)	Use of deep learning for predictive maintenance and anomaly detection in IoT networks; Application of advanced AI techniques for improving the security and efficiency of IoT systems; Blockchain and edge computing for secure data processing and management.

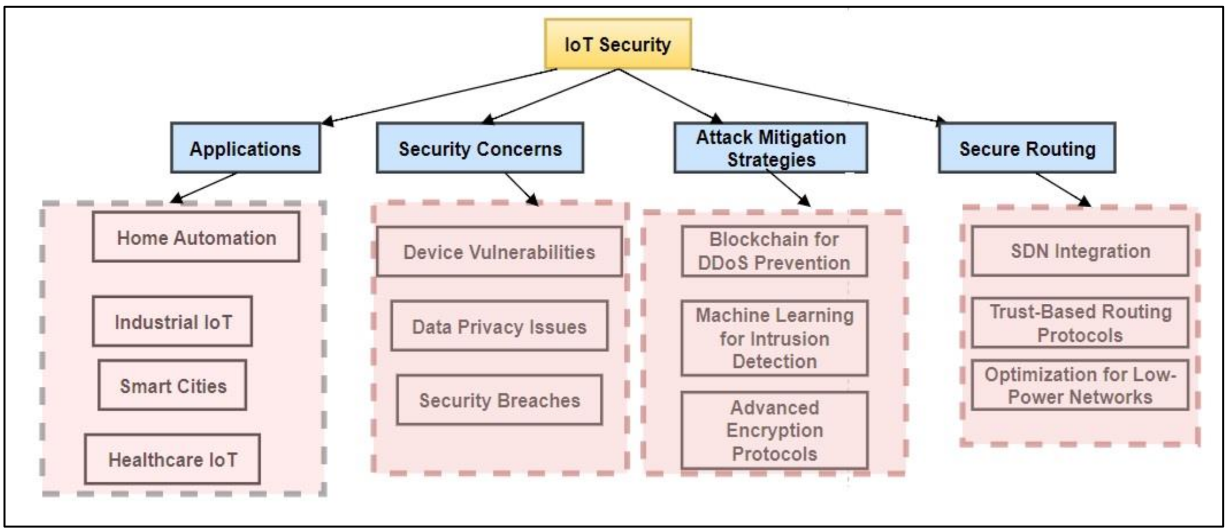

Figure 2: IoT Security Elements

Overview of IoT security challenges

The widespread adoption of IoT has brought with it significant security challenges. The rapid expansion of Internet-connected devices has led to concerns regarding the security and privacy of IoT systems, becoming a major consideration for organizations, consumers, and governments alike. The decentralized topology of IoT and the resource constraints of many of its devices make traditional security and privacy approaches inapplicable, necessitating the development of new models and strategies. This section presents an overview of the security challenges in IoT networks. Figure 2 illustrates diverse elements of IoT security frameworks.

Common Vulnerabilities in IoT Devices and Networks

This section offers a synopsis of the security challenges inherent in IoT networks.The pervasive implementation of IoT has been accompanied by substantial security challenges. The swift proliferation of devices connected to the Internet has precipitated apprehensions about the security and confidentiality of IoT infrastructures, becoming a pivotal concern for entities, individual users, and legislative bodies. The decentralized architecture of IoT and the constraints on resources inherent to many of its devices render obsolete the conventional methods of security and privacy, thus requiring the formulation of innovative models and approaches.

Security breaches in IoT can lead to unauthorized access to sensitive patient data in healthcare, compromising patient privacy and potentially causing life-threatening risks due to tampered medical devices. In smart cities, these intrusions can disrupt essential services such as traffic management, waste collection, and energy distribution, compromising public safety and leading to accidents. In industrial IoT, such incidents can cause significant financial losses, production downtime, equipment damage, and compromised product quality, with attacks on critical infrastructure posing widespread economic and safety implications.

The security of IoT networks is challenged by a variety of vulnerabilities. Analysis of the Common Vulnerabilities and Exposures (CVE) database reveals specific weaknesses in IoT devices, including home appliances and industrial devices, highlighting the need for automated recognition systems for IoT vulnerabilities (32). Hybrid networks that combine traditional industrial control systems with IT and IoT networks face unique security challenges, necessitating an improved vulnerability framework like Common Vulnerability Scoring System IoT-Industrial Control Systems called the CVSS-ICS (33). The proliferation of IoT leads to security threats across various data transfer technologies, such as ZigBee and Bluetooth, requiring user awareness and manufacturer responsibility to mitigate risks. Furthermore, Low Power Wide Area Network (LPWAN) technologies in which find applications in IoT are prone to security vulnerabilities, which necessitates a comprehensive review and analysis of cybersecurity strategies tailored to the Io ecosystem (34). Identification and validation approaches for IoT devices are imperative to guard against the distortion and manipulation of information, underscoring the necessity of preemptive security measures (35). Furthermore, the implementation of intrusion detection systems such as Snort within IoT settings is critical for the swift identification and thwarting of prevalent cyber threats, thereby safeguarding the integrity of both wired and wireless IoT networks (19). These studies collectively underscore the need for multifaceted and advanced security approaches to address the diverse vulnerabilities in IoT devices and networks.

Privacy Concerns in IoT Data Handling and Processing

The IoT ecosystem faces significant challenges in terms of security and privacy. One major concern is the lack of encryption in the majority of network traffic from IoT devices, leaving confidential and personal data vulnerable to malware attacks and security threats (20-21). This issue is compounded by ineffective security measures and improper device updates, further endangering user privacy (28). To combat these vulnerabilities, several solutions have been proposed. For instance, a cost-effective, privacy-assuring authentication protocol designed for IoT healthcare applications highlights the shift towards user-centric security approaches (36). Additionally, blockchain technology is being leveraged to create efficient, privacy-preserving authentication protocols, enhancing IoT security and offering protection against cyber-attacks (29). Furthermore, in IIoT, efforts are focused on developing an efficient and fine-grained signature scheme that is resistant to key exposure, addressing the critical security challenges and ensuring the safety and reliability of IIoT systems (37). To fortify IoT security in future, it's crucial to have visibility into data flow and adopt distributed cybersecurity controls and models tailored for IoT environments. Collectively, these strategies endeavor to fortify IoT systems against prospective hazards while preserving the integrity and privacy of the data involved.

Attack Mitigation Strategies in IoT

This section presents an overview of the recent research relevant to attack mitigation strategies in IoT networks in the following subsections.

Cyber Security in IoT

The collective research encapsulated in the following works addresses the multifaceted nature of cybersecurity within the IoT sphere. Gayathri *et al*., (38) concentrate on the identification and mitigation of IoT-based attacks utilizing Simple Network Management Protocol (SNMP) and Moving Target Defense (MTD) strategies, underscoring the necessity for dynamic and adaptable security systems in IoT environments. Knights and Gacovski (39) explore methods for detecting and mitigating vulnerabilities in IoT systems, highlighting the significance of proactive security measures in the protection of IoT devices. Ibrahim *et al.,* (22) investigate the application of Ethereum blockchain technology in averting Distributed Denial of Service (DDoS) attacks on IoT devices, illustrating the blockchain's potential to bolster IoT security. Tariq *et al.,* (40) present a comprehensive overview of cybersecurity within IoT, suggesting future research avenues to address the changing landscape of cyber threats. Garg *et al.,* (23) examine the use of gradient boosting for identifying IoT attacks, evidencing the effectiveness of machine learning in detecting and responding to security incidents. Rueda-Rueda and Porcaro (24) offer a study on structured security strategies for IoT, stressing the importance of systematic approaches in safeguarding IoT ecosystems. These studies collectively provide an integrated perspective on the existing challenges and novel solutions in the domain of IoT cybersecurity.

IoT Security Standards and Frameworks

IoT security standards and frameworks are designed to comprehensively protect IoT ecosystems. They cover various security domains such as endpoint, communications, system protection, and lifecycle management (41). These frameworks set forth essential security features and optimal protocols for the secure deployment and administration of IoT devices. They further incorporate assessment criteria and maturity models for the continual evaluation and enhancement of security postures. Key organizations like the IoT Security Foundation and the Global System for Mobile communication (GSM) Association contribute by providing guidelines and fostering knowledge sharing in IoT security. Numerous well-established IoT security norms (42) and structures are pivotal in upholding the security of IoT ecosystems, which encompass:

National Institute of Standards and Technology (NIST) Cybersecurity Framework: It is a comprehensive framework that guides organizations in managing and diminishing cybersecurity risks. Its wide acceptance and implementation across various industries make it a benchmark in the field.

ISO/IEC 27000 series: This series represents a versatile framework applicable to organizations of varying sizes. ISO 27001 and 27002, the primary standards in this series, provide guidelines for establishing an Information Security Management System (ISMS), ensuring systematic and consistent security practices.

Industrial Internet Consortium (IIC) Framework: Specifically catering to IIoT systems, this framework addresses critical security domains like endpoint protection, communication security, system protection, and lifecycle management. It is tailored to meet the unique requirements of industrial IoT environments.

Open Web Application Security Project (OWASP) IoT Security Verification Standard: This standard provides a structured set of requirements and methods for testing IoT systems' security. It encompasses various security aspects, including device identity management, data protection, secure communication, firmware updates, and vulnerability management, ensuring a comprehensive approach to IoT security.

These standards collectively offer a robust framework for securing IoT devices and systems, emphasizing on security characteristics, best practices, assessment criteria, and maturity models to protect the entire IoT ecosystem effectively.

Secure IoT Routing

Routing in IoT networks is essential for guiding data from its origin to the appropriate destination within a network of interconnected devices. This procedure is essential for facilitating efficient and dependable communication across diverse IoT systems. Routing protocols in IoT are customized to meet the particular requirements of IoT devices, which typically possess limited resources such as energy and computational capacity. These protocols are designed to serve a spectrum of IoT applications, ranging from residential automation to industrial configurations, and they remain a focal point of ongoing research. This research aims to optimize data transfer while balancing factors like energy efficiency, security, and scalability (43).

The safeguarding of these routing protocols poses distinctive difficulties, principally because of the heterogeneous character of IoT networks and the considerable volume of data being processed.Key among these challenges is establishing protocols that securely navigate data transmission routes, considering the varied and resource-limited nature of IoT devices (44). Preserving the integrity and privacy of data as it traverses through network devices is paramount, ensuring that data is not only accurately directed but also shielded from modification or unauthorized access. Moreover, protecting IoT systems from data leaks is crucial, which calls for strong encryption protocols. Finally, secure routing solutions must be scalable to match the growing IoT networks, safeguarding data integrity even under high traffic loads.

IoT Routing Protocols

IoT routing mechanisms are specifically designed to align with the unique needs of IoT devices, which are often constrained by limited energy and computational power (45). They are applicable to a broad spectrum of IoT applications, extending from residential automation to industrial arrangements, and are the subject of ongoing academic investigation. This research aims to optimize data transfer while balancing factors like energy efficiency, security, and scalability.

Securing these routing protocols presents unique challenges, ascribed to the diverse nature of IoT networks and the substantial data to be processed. Key among these challenges is establishing protocols that securely navigate data transmission routes, considering the varied and resource-limited nature of IoT devices (25). Maintaining the integrity and confidentiality of data during its journey across network devices is critical, ensuring data is both correctly routed and protected from alteration or unauthorized access. Furthermore, safeguarding IoT infrastructures against data breaches is imperative, necessitating robust encryption protocols. In conclusion, secure routing solutions must exhibit scalability to keep pace with the expanding IoT networks, ensuring data integrity is maintained even amidst substantial traffic volumes. Recent advancements in IoT routing protocols are addressing significant challenges such as secure routing, managing topological changes, and overcoming resource limitations. Innovations include the development of secure routing algorithms that utilize the structure of IoT packets, enhancing network performance and intrusion detection. These algorithms often incorporate Software-Defined Networking (SDN) and machine learning techniques, offering more robust and adaptive routing solutions (26). The handling of frequent topological changes and limited resources in IoT devices has also seen significant focus. New methods and protocols are being developed to ensure efficient and reliable data routing in dynamic IoT environments. The Routing Protocol for Low-Power and Lossy Networks (RPL) (46), a cornerstone in IoT network layer protocols, is under continuous review to adapt to evolving trends and meet emerging requirements. Additionally, research in congestion management for IoT-based wireless sensor networks is focusing on enhancing routing efficiency, which is crucial for the overall performance of IoT systems.

Collectively, these advancements are geared towards optimizing routing in IoT systems with an emphasis on security, adaptability, and efficient resource utilization. Current IoT routing protocols face several key limitations. Frequent topological changes in dynamic IoT networks complicate efficient and reliable data routing. These devices, constrained by limited processing power, memory, and energy, struggle to support complex routing algorithms, impacting network performance. Scalability is another challenge, as the growing number of devices strains existing protocols, leading to inefficiencies. Security concerns, including unauthorized access and data breaches, pose significant risks to IoT routing. Furthermore, interoperability issues arise from the use of disparate routing protocols and standards across devices, impeding seamless communication. These challenges underscore the urgent need for enhanced IoT routing protocols to better cater to the unique demands of IoT networks.

Trust based Routing Approaches

In the past few years, the adoption of trust-based methods has risen to prominence as a significant means for improving security within IoT environments (27). These approaches leverage trust metrics to assess and establish the reliability of nodes within an IoT network, effectively mitigating risks like Rank and Blackhole attacks. Trust models, typically dynamic in nature, continuously update trust levels based on nodes' behaviors, thereby ensuring a secure and robust routing mechanism. Such models are increasingly relevant in RPL-based IoT networks, where node mobility and network dynamics pose additional security challenges. The integration of trust-based methods into IoT security paradigms represents a significant stride in protecting these networks from various cyber threats and vulnerabilities (47).

Implementing trust-based approaches for secure routing in IoT networks faces several challenges. Establishing trust among nodes in a dynamic environment is complex, particularly when nodes have limited resources and are susceptible to failures (48). Managing trust, which involves computation, storage, and updating of trust information, imposes significant overhead on IoT devices. Dynamic network conditions, characterized by node mobility and fluctuating traffic patterns, complicate accurate trust assessments. Additionally, these approaches raise security and privacy concerns due to the handling of sensitive trust-related data, making systems vulnerable to attacks (49, 50). Scalability is another critical issue, as the growth in IoT device numbers demands efficient trust management. Addressing these challenges is vital for the effective implementation of trust-based secure routing, with ongoing research focused on developing viable solutions.

Deep Learning Approaches in IoT

Deep learning approaches are increasingly being integrated into the IoT networks to enhance the key aspects addressed in this research as below.

Applications

Deep learning architectures are utilized to enhance a variety of IoT applications, encompassing predictive maintenance, anomaly identification, and instantaneous data analysis. By analyzing large volumes of IoT data, deep learning models can identify patterns and make accurate predictions, thereby enhancing the functionality and performance of IoT applications (51).

Security Concerns

Deep learning approaches contribute to addressing security concerns in IoT by enabling the development of advanced intrusion detection systems, malware detection, and threat intelligence. Deep learning classifiers are adept at scrutinizing network traffic and device behavior to pinpoint potential security threats and irregularities, thereby reinforcing the general security stance of IoT settings (52).

Attack Mitigation

Deep learning techniques aid in mitigating attacks on IoT systems by enabling proactive threat detection and rapid response. Through continuous monitoring and analysis of IoT data, deep learning models can detect and mitigate various attacks, including DDoS attacks, ransomware, and unauthorized access attempts, thereby enhancing the resilience of IoT systems (30).

Secure Routing

In the context of secure routing, deep learningis utilized to enhance the trust and reliability of routing decisions. By analyzing the behavior and communication patterns of IoT devices, deep learning models can contribute to the development of more robust and adaptive routing protocols, thus improving the overall security and efficiency of data transmission in IoT networks (53).

Discussion

This section consolidates the major findings from each section to provide a holistic perception of the IoT landscape and key issues to be addressed in future. Section 2's exploration of IoT applications, including emerging technologies, underscores the vast potential and diverse applications of IoT in various sectors. Section 3 brings to light the critical security concerns within IoT, highlighting the evolving nature of security challenges, vulnerabilities, and privacy issues that necessitate vigilant security measures. In Section 4, the focus on attack mitigation strategies reveals the importance of proactive and adaptive approaches to safeguard IoT systems against cyber threats. Section 5's examination of secure routing in IoT emphasizes the need for robust and efficient routing mechanisms to ensure data integrity and network resilience. The introduction of deep learning approaches in Section 6 marks a significant advancement in addressing IoT security and operational challenges, showcasing the potential of AI-driven solutions.

Future research in IoT routing protocols is poised to address several key aspects to enhance their efficiency and adaptability in diverse environments. This includes the development and analysis of advanced protocols like focusing on performance metrics and optimizing for large-scale network efficiency. There's a growing focus on studying the latest solutions to routing challenges in Low-power and Lossy Networks (LLNs) in IoT applications, which necessitates more in-depth research into tailored routing strategies. Emerging trends in IoT also demand comprehensive reviews and analysis of the current routing protocols to identify and address future challenges, thereby providing vital comprehension for new researchers in this field. Research in IoT-based Wireless Sensor Networks (WSNs) for applications like smart home systems using simulation platforms is another promising area, where ad-hoc routing protocols and their efficiency in real-world scenarios can be explored. Additionally, there is a need for innovative research in congestion management strategies for IoT-based WSNs to ensure effective and efficient routing processes.

Conclusion

This review aims to encapsulate key insights from a thorough exploration of the IoT technologies. It undertakes a comprehensive examination of IoT applications, highlighting emerging trends and underscoring the substantial scope and potential impact of IoT across various sectors. Attention is directed towards the critical security concerns, emphasizing the need to address escalating security challenges, vulnerabilities, and privacy issues inherent in IoT systems. The discourse on attack mitigation strategies accentuates the necessity for robust and proactive approaches to combat evolving cyber threats. Furthermore, an analysis of secure routing in IoT is conducted, underlining the significance of maintaining data integrity and network resilience within IoT ecosystems. This review also delves into the integration of deep learning techniques, showcasing the potential of advanced technologies in boosting the security and efficiency of IoT. The interplay between technological advancements and security challenges in the realm of IoT is a major focus, highlighting the dynamic nature of this field. The review concludes by asserting the imperative for ongoing research and development in IoT, particularly in enhancing security protocols and harnessing emerging technologies, to adeptly navigate the ever-changing landscape of IoT applications and threats.

Abbreviations

Nil.

Acknowledgement

Nil.

Author Contributions

Azmera Chandu Naik: Conceptualization and Writing Draft. Madhu Kumar Vanteru: Investigation, Methodology, literature review. Bandru Sanjeev: Conceptualization, formal analysis, conclusion. Sravan Kumar V: Introduction, Writing Draft. Karthik Kumar Vaigandla: Conceptualization, Investigation, Supervision, Writing, review and editing. All authors made an equal contribution. All the authors have read and approved the final version of the manuscript.

Conflict of Interest

The authors declare that there is no conflict of interest.

Ethics Approval

Not applicable.

Funding

This article does not contain any funding

References

1. Guerrero-Ulloa G, Rodríguez-Domínguez C, Hornos MJ. Agile methodologies applied to the development of Internet of Things (IoT)-based systems: A review. Sensors. 2023 Jan 10;23(2):790.
2. Rezaee N, Zanjirchi SM, Jalilian N, Bamakan SM. Internet of things empowering Operations Management; A systematic review based on bibliometric and content analysis. Telematics and Informatics Reports. 2023 Aug 29:100096.
3. Manyika J, Chui M, Bisson P, Woetzel J, Dobbs R, Bughin J, Aharon D. Unlocking the Potential of the Internet of Things. McKinsey Global Institute. 2015 Jun 1;1.
4. Younan M, Houssein EH, Elhoseny M, Ali AA. Challenges and recommended technologies for the industrial internet of things: A comprehensive review. Measurement. 2020 Feb 1;151:107198.
5. Hou KM, Diao X, Shi H, Ding H, Zhou H, de Vaulx C. Trends and challenges in AIoT/IIoT/IoT implementation. Sensors. 2023 May 25;23(11):5074.
6. Nayana GH, Koithyar A, Dhanush J, Vikas R, Gowda MC, Kumar A, Naik AR. IoT Based Intelligent Home Automation Using Automated Smart Devices. In2023

IEEE International Conference on Contemporary Computing and Communications (InC4). IEEE. 2023 Apr 21;1:pp. 1-5.
7. Kumar KM, Chaudhury S. Development of a Smart Home Automation System using IoT enabled Devices. In2022 IEEE 19th India Council International Conference (INDICON). IEEE. 2022 Nov 24; pp. 1-5.
8. Gilani SM, Usman M, Daud S, Kabir A, Nawaz Q, Judit O. SDN-based multi-level framework for smart home services. Multimedia Tools and Applications. 2024 Jan;83(1):327-47.
9. Huang J, Gao H, Wan S, Chen Y. AoI-aware energy control and computation offloading for industrial IoT. Future Generation Computer Systems. 2023 Feb 1;139:29-37.
10. Wu H, Chen J, Nguyen TN, Tang H. Lyapunov-guided delay-aware energy efficient offloading in IIoT-MEC systems. IEEE Transactions on Industrial Informatics. 2022 Sep 15;19(2):2117-28.
11. Khang A, Gupta SK, Rani S, Karras DA, editors. Smart Cities: IoT Technologies, big data solutions, cloud platforms, and cybersecurity techniques. CRC Press; 2023 Nov 30.
12. Mishra P, Singh G. Internet of medical things healthcare for sustainable smart cities: current status and future prospects. Applied Sciences. 2023 Aug 1;13(15):8869.
13. Vaigandla KK. Communication Technologies and Challenges on 6G Networks for the Internet: Internet of Things (IoT) Based Analysis. In2022 2nd International Conference on Innovative Practices in Technology and Management (ICIPTM). IEEE. 2022 Feb 23;2:pp. 27-31.
14. Shah V, Khang A. Internet of Medical Things (IoMT) driving the digital transformation of the healthcare sector. InData-Centric AI Solutions and Emerging Technologies in the Healthcare Ecosystem. CRC Press. 2023 Aug 24: pp. 15-26.
15. Patel U, Patel R, Kadecha P. An IOT-Aided Smart Agritech System for Crop Yield Optimization. InPrecision Agriculture for Sustainability. Apple Academic Press. 2024 Feb 13: pp. 433-452.
16. Humayun M, Jhanjhi NZ, Hamid B, Ahmed G. Emerging smart logistics and transportation using IoT and blockchain. IEEE Internet of Things Magazine. 2020 Jun 25;3(2):58-62.
17. Dhingra S, Madda RB, Gandomi AH, Patan R, Daneshmand M. Internet of Things mobile–air pollution monitoring system (IoT-Mobair). IEEE Internet of Things Journal. 2019 Mar 8;6(3):5577-84.
18. Marinakis V, Doukas H. An advanced IoT-based system for intelligent energy management in buildings. Sensors. 2018 Feb 16;18(2):610.
19. Savukynas R. Internet of Things information system security for smart devices identification and authentication. In2020 9th Mediterranean Conference on Embedded Computing (MECO). IEEE. 2020 Jun 8: pp. 1-5.
20. Patel ND, Mehtre BM, Wankar R. A Snort-based secure edge router for smart home. International Journal of Sensor Networks. 2023;41(1):42-59.
21. Li Z, Tian Y, Zhang W, Liao Q, Liu Y, Du X, Guizani M. RR-LADP: A privacy-enhanced federated learning scheme for internet of everything. IEEE Consumer Electronics Magazine. 2021 Feb 17;10(5):93-101.
22. Gayathri R, Usharani S, Mahdal M, Vezhavendhan R, Vincent R, Rajesh M, Elangovan M. Detection and mitigation of iot-based attacks using snmp and moving target defense techniques. Sensors. 2023 Feb 3;23(3):1708.
23. Ibrahim RF, Abu Al-Haija Q, Ahmad A. DDoS attack prevention for internet of thing devices using ethereum blockchain technology. Sensors. 2022 Sep 8;22(18):6806.
24. Tariq U, Ahmed I, Bashir AK, Shaukat K. A critical cybersecurity analysis and future research directions for the Internet of Things: A comprehensive review. Sensors. 2023 Apr 19;23(8):4117.
25. Hussain MZ, Hanapi ZM. Efficient secure routing mechanisms for the low-powered IoT network: A literature review. Electronics. 2023 Jan 17;12(3):482.
26. Darabkh KA, Al-Akhras M, Zomot JN, Atiquzzaman M. RPL routing protocol over IoT: A comprehensive survey, recent advances, insights, bibliometric analysis, recommendations, and future directions. Journal of Network and Computer Applications. 2022 Nov 1;207:103476.
27. Airehrour D, Gutierrez JA, Ray SK. SecTrust-RPL: A secure trust-aware RPL routing protocol for Internet of Things. Future Generation Computer Systems. 2019 Apr 1;93:860-76.
28. Yadav R, Vaigandla KK, Ghantasala GP, Singh R, Gangodkar D. The Block Chain Technology to protect Data Access using Intelligent Contracts Mechanism Security Framework for 5G Networks. In2022 5th International Conference on Contemporary Computing and Informatics (IC3I). IEEE. 2022 Dec 14: pp. 108-112.
29. Lin L, Tian Y, Liu Y. A blockchain-based privacy-preserving recommendation mechanism. In2021 IEEE 5th international conference on cryptography, security and privacy (CSP). IEEE. 2021 Jan 8: pp. 74-78.
30. Bolhasani H, Mohseni M, Rahmani AM. Deep learning applications for IoT in health care: A systematic review. Informatics in Medicine Unlocked. 2021 Jan 1;23:100550.
31. Hussain F, Hussain R, Hassan SA, Hossain E. Machine learning in IoT security: Current solutions and future challenges. IEEE Communications Surveys & Tutorials. 2020 Apr 8;22(3):1686-721.
32. Hossain MS, Chisty NM, Hargrove DL, Amin R. Role of Internet of Things (IoT) in retail business and enabling smart retailing experiences. Asian Business Review. 2021;11(2):75-80.
33. Ur-Rehman A, Gondal I, Kamruzzaman J, Jolfaei A. Vulnerability modelling for hybrid industrial control system networks. Journal of grid computing. 2020 Dec;18:863-78.
34. Scarfò A. The cyber security challenges in the IoT era. InSecurity and Resilience in Intelligent Data-Centric Systems and Communication Networks. Academic Press. 2018 Jan 1: pp. 53-76.
35. Torres N, Pinto P, Lopes SI. Security vulnerabilities in LPWANs—an attack vector analysis for the IoT ecosystem. Applied Sciences. 2021 Apr 2;11(7):3176.

36. Gheisari M, Wang G, Khan WZ, Fernández-Campusano C. A context-aware privacy-preserving method for IoT-based smart city using software defined networking. Computers & Security. 2019 Nov 1;87:101470.
37. Bao Y, Qiu W, Tang P, Cheng X. Efficient, revocable, and privacy-preserving fine-grained data sharing with keyword search for the cloud-assisted medical IoT system. IEEE Journal of Biomedical and Health Informatics. 2021 Jul 30;26(5):2041-51.
38. Lomotey R, Rickabaugh J, Slivkanich N, Orji R. Data verification and privacy in IoT architecture. In2019 IEEE World Congress on Services (SERVICES). IEEE. 2019 Jul 8; 2642: pp. 66-71.
39. Bao Y, Qiu W, Cheng X. Efficient and fine-grained signature for IIoT with resistance to key exposure. IEEE Internet of Things Journal. 2021 Feb 1;8(11):9189-205.
40. Knights VA, Gacovski Z. Methods for Detection and Prevention of Vulnerabilities in the IoT (Internet of Things) Systems. https://www.intechopen.com/chapters/88775
41. Garg S, Kumar V, Payyavula SR. Identification of internet of things (IoT) attacks using gradient boosting: a cross dataset approach. Telematique. 2022 Nov 30;21(1):6982-7012.
42. Rueda-Rueda JS, Portocarrero JM. Framework-based security measures for Internet of Thing: A literature review. Open Computer Science. 2021 Jan 1;11(1):346-54.
43. Karie NM, Sahri NM, Yang W, Valli C, Kebande VR. A review of security standards and frameworks for IoT-based smart environments. IEEE Access. 2021 Sep 3;9:121975-95.
44. López-Aguilar P, Batista E, Martínez-Ballesté A, Solanas A. Information security and privacy in railway transportation: A systematic review. Sensors. 2022 Oct 11;22(20):7698.
45. Airehrour D, Gutierrez J, Ray SK. Secure routing for internet of things: A survey. Journal of Network and Computer Applications. 2016 May 1;66:198-213.
46. Rui K, Pan H, Shu S. Secure routing in the Internet of Things (IoT) with intrusion detection capability based on software-defined networking (SDN) and Machine Learning techniques. Scientific Reports. 2023 Oct 21;13(1):18003.
47. Verma A, Deswal S. FOG-RPL: Fog Computing-based Routing Protocol for IoT Networks. Recent Advances in Electrical & Electronic Engineering (Formerly Recent Patents on Electrical & Electronic Engineering). 2024 Feb 1;17(2):170-80.
48. De Masi G. The impact of topology on Internet of Things: A multidisciplinary review. In2018 Advances in Science and Engineering Technology International Conferences (ASET). IEEE. 2018 Feb 6: pp. 1-6.
49. Muzammal SM, Murugesan RK, Jhanjhi NZ, Hossain MS, Yassine A. Trust and mobility-based protocol for secure routing in Internet of Things. Sensors. 2022 Aug 18;22(16):6215.
50. Almusaylim ZA, Alhumam A, Jhanjhi NZ. Proposing a secure RPL based internet of things routing protocol: A review. Ad Hoc Networks. 2020 Apr 15;101:102096.
51. Nandhini PS, Kuppuswami S, Malliga S, DeviPriya R. Enhanced Rank Attack Detection Algorithm (E-RAD) for securing RPL-based IoT networks by early detection and isolation of rank attackers. The Journal of Supercomputing. 2023 Apr;79(6):6825-48.
52. Al-Amiedy TA, Anbar M, Belaton B, Bahashwan AA, Hasbullah IH, Aladaileh MA, Mukhaini GA. A systematic literature review on attacks defense mechanisms in RPL-based 6LoWPAN of Internet of Things. Internet of Things. 2023 Jul 1;22:100741.
53. Kumar S, Kumar M, Azmea CN, Vaigandla KK. BCSDNCC: A Secure Blockchain SDN framework for IoT and Cloud Computing. International Research Journal of Multidisciplinary Technovation. 2024 Apr 16;6(3):26-44.