*International Journal of Engineering Applied Sciences and Technology, 2024*
**Vol. 9, Issue 05, ISSN No. 2455-2143, Pages 68-77**
**Published Online September 2024 in IJEAST (http://www.ijeast.com)**

# A REVIEW ON CYBERSECURITY VULNERABILITY DISCOVERY AND MITIGATION MODEL IN SMART COMPUTING

Kavita U. Rahane
Research Scholar
Sanjivani College of Engineering Kopargaon, India
Savitribai Phule Pune University

A. B. Pawar
Research Guide
Sanjivani College of Engineering Kopargaon, India
Savitribai Phule Pune University

*Abstract*—**Smart computing links physical and digital objects which communicate online using sensors, software, and other technologies. It offers many advantages but lacks information security, it could potentially face serious problems. The number of smart computing devices are growing rapidly around the world, making them a target of many attackers, whose aim is to steal confidential data and threaten user's privacy. With features like confidentiality, access control, correctness, completeness, authentication, availability, and privacy. Data and services should be safeguarded in the ecosystem. It has particular traits and constraints, which make cybersecurity concerns exclusive. It is crucial to recognize these hazards and develop countermeasures to reduce the risks they pose. This document examined and classified the smart computing ecosystem's most prevalent dangers, security risks, and challenges. Also classified most common countermeasures to control vulnerabilities and the techniques that can be used to overcome them.**

*Keywords*—**Smart Home, Smart grid, Industrial IoT, machine learning, Artificial Intelligence, Blockchain.**

## I. INTRODUCTION

Over the past decades, impressive technological breakthroughs in smart computing commenced significant business opportunities for diverse areas. It intends to connect the physical world to the digital through the Internet. It provides great business opportunities in different smart sectors like cities, homes, grids, tourism, healthcare, and industrial IoTs [1]. Smart computing attempts to construct a novel environment in which a new process is derived by connecting the network of smart devices and machines to establish communication and collaboration. Traditional internet connectivity is exploited at the core of smart computing to connect, collect, and exchange data among the devices [2]. However, there are main concerns about cybersecurity due to massive data generation and complex heterogeneous environments. Cybersecurity is important for smart computing, as it can protect sensitive data and infrastructure. Discovering cybersecurity vulnerabilities and providing appropriate countermeasures against such issues have become increasingly more expensive. Currently, three main methods are used to detect and mitigate security threats: Authentication-based, Artificial intelligence-based and Blockchain-based. This document provides a review of various security vulnerabilities and solutions to mitigate such vulnerabilities [3].

Further document is organized as follows: Section 2 provides significance in this research field. Section 3 describes various challenges in cybersecurity vulnerability discovery. Section 4 classifies different types of cyber- attacks. Section 5 provides a survey on different vulnerability discovery and mitigation techniques along with their comparison. Section 6 gives research gaps and questions. Section 7 summarizes the conclusion.

## II. SIGNIFICANCE IN THIS RESEARCH FIELD

The multidisciplinary vision of smart computing in various environments greatly transform humans' daily routine life as smart. It exploits the Internet to innovate novel solutions for diverse business environments, government sectors, and various smart industries. A survey report in [4] depicts that nearly 15.14 billion devices will be connected through it worldwide in 2023. It is expected that the connection will increase to double by 29.42 billion in the year 2030. Among the 15 billion devices, China has more than 5 billion IoT devices. However, the data heterogeneity and complexity pose various cybersecurity challenges. Hence, effectively addressing the security concerns associated with smart

*International Journal of Engineering Applied Sciences and Technology, 2024*
**Vol. 9, Issue 05, ISSN No. 2455-2143, Pages 68-77**
**Published Online September 2024 in IJEAST (http://www.ijeast.com)**

computing is critical. The information and services provided in smart computing must be protected with strong security features: confidentiality, accuracy, access control, comprehensiveness, authentication, availability, and privacy. It has unique characteristics and limitations regarding cyber security threats. Due to ingenious attack behaviors, diverse security vulnerabilities are emerging daily in IoT [5]. Therefore, learning about the security vulnerabilities posed by smart computing technology and determining optimal solutions to mitigate such risks is essential. Analysis of the security vulnerability discovery and the countermeasures used to defend against them is very important [6].

## III. CYBERSECURITY VULNERABILITY DISCOVERY AND CHALLENGES

The vulnerability discovery of cybersecurity represents a process used to determine the weaknesses and flaws in networks or software applications and computer systems related to smart computing that cybers-attackers could exploit. The vulnerability discovery methods involve assessing, scanning, and testing over such environment and uncovering the vulnerabilities by effectively accessing the risky level they pose. Once the methods discover the vulnerabilities, the countermeasures can effectively address and mitigate the attacks to elaborate the security posture of the entire system or application. Due to smart computing's heterogeneous and resource-limitation characteristics, vulnerability discovery models must meet several challenges as provided below:

- The attackers utilize zero-day exploits, ingenious tactics, and polymorphic malware to evolve their strategies which is very difficult to discover.
- It is a large-scale network that constructs a massive smart device system. Detecting the vulnerabilities in such a system is complex and time-consuming.
- It is unknown to the public and software vendors. Thus, it makes vulnerability discovery highly challenging.
- Due to the high complexity and size of the environment, the vulnerability discovery models may be affected by high false positives and negatives. Sometimes, the error may happen due to humans. Thus, it makes the discovery process very challenging.
- The smart computing system size increases the challenges of vulnerability discovery. Hence, efficient and scalable models are needed without affecting performance. Also, the collection of real-world data is highly challenging.
- It utilizes heterogeneous technologies for communication which evolves day by day. Thus, it poses novel security issues to the discovery models.
- The collaboration among the large-scale heterogeneous systems can share the advanced vulnerability models. Therefore, collaboration with privacy-preserved information-sharing methods is vital for effective vulnerability discovery.

## IV. CYBERSECURITY ATTACK CLASSIFICATION

The smart computing network comprises a multi-source database and diverse application areas. Thus, it poses a variety of cybersecurity attacks. The vulnerabilities occur at different levels: device level, application level, software level, hardware level, protocol level, network level, and data level. The cybersecurity attacks are classified as shown in Figure 1.

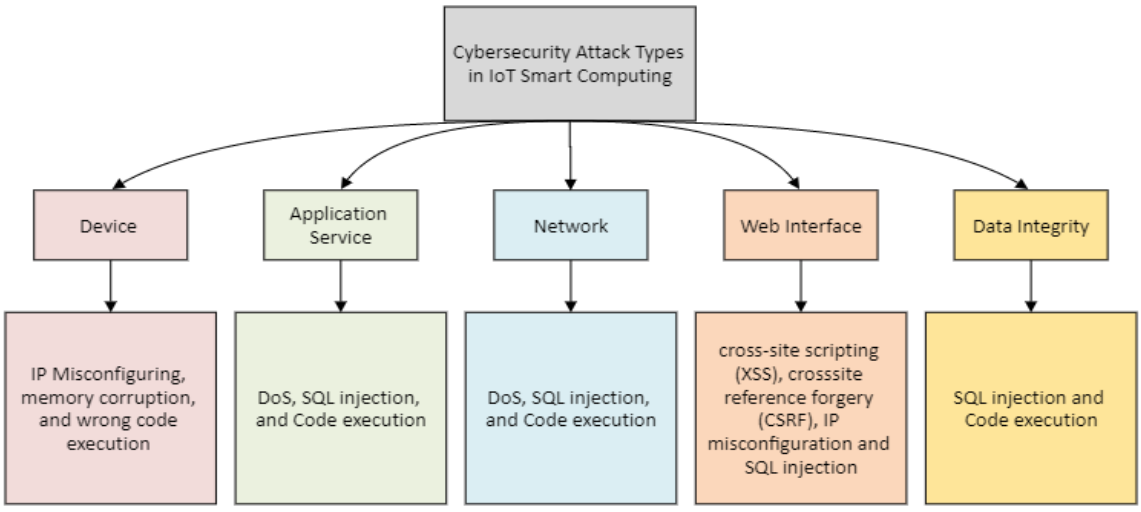


**Figure 1: Cybersecurity Attack Classification**

- Device attack includes:

a. IP misconfiguration refers to errors or oversights in the configuration of network settings, including IP addresses, subnets, and gateways, on smart devices or within the network infrastructure. Common IP misconfiguration issues include - Default Credentials, Incorrect Firewall Rules, Open Ports, and Improper VLAN Segmentation. These all can result in unauthorized access, data breaches,

or disruption of device functionality.

b. Memory corruption vulnerabilities can occur when a software bug or programming error allows an attacker to manipulate a device's memory in unintended ways. These vulnerabilities can lead to various security issues, including Buffer Overflows, Use-After-Free, and Memory Leaks.
c. Wrong code execution refers to situations where smart devices execute code or commands incorrectly, often due to software bugs or security vulnerabilities. This can result in unexpected behaviours, system crashes, or security breaches. Examples include - Insecure Firmware Updates, Code Injection, Command Injection.

- Application service attack includes:

a. The aim of Denial of Service (DoS) attacks is to interrupt the availability of smart application services by overwhelming it with excessive traffic. This can render the service unavailable to legitimate users.
b. SQL injection is a an attack where malicious SQL queries are inserted into user inputs or smart device inputs that interact with a database. If the application does not properly validate or sanitize these.
c. Code execution vulnerabilities in application services can occur when attackers are able to run arbitrary code on the server or within the application itself. This can lead to unauthorized access, data breaches, or even complete compromise of the smart computing application.

- Network attack includes:

a. A DoS attack seeks to stop a network service from being available by flooding it with excessive traffic. This can cause the service to become slow or completely unavailable to legitimate users.
b. SQL injection is an attack where malicious SQL queries are inserted into input fields or data sent to a network service. If the service does not properly validate or sanitize these inputs, attackers can manipulate the database and potentially gain unauthorized access or modify data.
c. Code execution vulnerabilities in network services occur when attackers can run arbitrary code on the server or within the network service itself.

- Web interface attack includes:

a. Cross-site scripting (XSS)occurs when an attacker inserts malicious scripts into web pages. These scripts can execute within the victim's browser, potentially getting fakely session cookies, user data, or performing other malicious actions on behalf of the user.
b. Cross-Site Request Forgery (CSRF) attacks involve misleading a user into making an unwanted request to a web application on which they are authenticated. This can result in actions being taken without user's permission.
c. IP misconfigurations can include issues like open ports, incorrect firewall settings, or failure to secure communication channels. These misconfigurations can make the web interface service vulnerable to unauthorized access or exploitation.
d. SQL injection occurs when an attacker inserts malicious SQL queries into user inputs or data that interacts with a database. If the application does not properly validate or sanitize these inputs, attackers can manipulate the database and potentially gain unauthorized access or modify data.

- Web Integrity attack includes:

a. In SQL injection attack the application doesn't properly authenticate inputs, the attacker can manipulate the SQL query, potentially gaining unauthorized access to the database or altering data.
b. Code execution vulnerabilities occur when attackers can execute arbitrary code within an application or system, potentially gaining unauthorized access or control over the system.

## V. LITERATURE SURVEY

Smart computing technology has become one of the important part of modern society and ensuring adequate security is crucial to improving efficiency. Numerous works have been introduced in the context of cybersecurity of smart computing [7][8]. For the clarity of the survey, the works are categorized into two parts: IoT security vulnerability discovery models and IoT cybersecurity countermeasures.

This section includes a thorough literature survey of the research done throughout the world by researchers to discover various vulnerability discovery model and mitigation techniques in smart computing. Using keywords like "Vulnerability in IoT" + "attacks on smart computing using AI, ML or Blockchain" + "vulnerability mitigation in smart devices" utilised the Publish and Perish tool to find all the publications. A total of 3147 publications addressing broad subjects in this domain were found. From 2016 through 2023, 225 publications were screened based on the number of citations. In order to go to the further study, at the initial stage 100 studies were eligible. From the 100 studies included; 46 were removed, leaving 54 for further survey.

The selected papers' publication years are listed in Figure 2 and ranges from 2016 to 2023; the majority of the papers were published in 2022.

*International Journal of Engineering Applied Sciences and Technology, 2024*
**Vol. 9, Issue 05, ISSN No. 2455-2143, Pages 68-77**
**Published Online September 2024 in IJEAST (http://www.ijeast.com)**

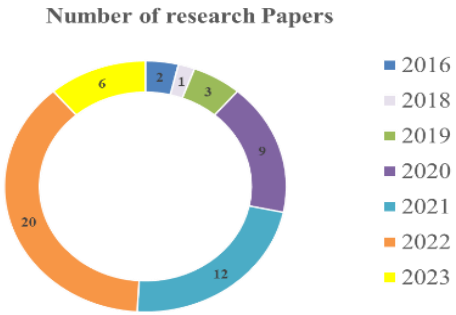


**Figure 2: Year wise published paper**

Emerging trends in vulnerability discovery and cybersecurity countermeasures drawn from the Perish tool's references is as described in section below.

### 5.1 Security Vulnerability Discovery Models

A lot of vulnerability discovery models are available in the literature. Among them, machine learning-based models receive significant attention[9]. To better understand the vulnerability discovery models and their tools, a study in[10] reviews the works proposed in the last ten years. In [11], the up-to-date and well-known cybersecurity risks are analyzed deeply to propose a framework to analyze software vulnerability with the assistance of machine learning. The main intention of the vulnerability discovery model in[12] is to elaborate on the predictive accuracy of existing discovery models. It introduces a Multiple Error Iterative Analysis Method (MEIAM) and Artificial Neural Network sign estimators. It utilizes the residual errors to optimize the vulnerability discovery models and assists in accurately predicting future trends of vulnerabilities across diverse datasets and strategies. In[13], the existing vulnerability strategies are discussed to propose a new time-based differential equation method for vulnerability discovery It is predicated on the idea that, within the software vulnerability life cycle, the local phenomena of vulnerability saturation exhibits an ever-increasing cyclic behavior. In order to find software vulnerabilities, it collects the vulnerability information from the National Vulnerability Database (NVD).The paper in[14] presents an EUFuzzer, a novel fuzzing tool that assists testers in Human-Machine Interface (HMI) vulnerability discovery.

### 5.2 Cybersecurity Countermeasures

The work in[15] gives an in-depth analysis of security by conducting systematic literature. It considers the generic smart computing architecture with its layers, security vulnerabilities and countermeasures to present the survey. Consequently, the work in[16] accesses and reviews the works related to cybersecurity attacks in the IoT environment and provides the most significant countermeasures that are highly useful to mitigate such cybersecurity attacks. The study in[17] highlights the core IoT security systems by determining the primary security problems and countermeasures that must be considered in the IoT environment. It also analyzes the various countermeasures proposed for cybersecurity to combat diverse attacks and assures information security by protecting the data loss in IoT-based systems. The study in[18] categorizes the types of IoT cybersecurity attacks by exploiting Artificial Intelligence (AI) techniques. The study shows that the researchers found that most of the works utilize the two types of AI algorithms: support vector machines (SVM) and random forest (RF), among all AI methods owing to the attack detection with high accuracy. The survey in[19] discusses the recent cyber security trend, technologies and presents the emerging cyber threats with challenges for the IoT environment. Also, it describes the research efforts presented to curb such threats and protect society worldwide. The cybersecurity threats and vulnerabilities of digital agriculture are discussed in[20]. By comprehensively reviewing the security works related to cybersecurity, this work decides that no existing works effectively address side-channel attacks (SCA), especially in digital agriculture.

Consequently, the work in[21] mainly intends to provide the security links missed in existing cybersecurity works to further improve cybersecurity in smart city environments. It accomplishes its aim by estimating the particular context information of each smart city environment and determining the specific security requirements. It proposes an architecture called Activity Network-Things (ANT)-centric introduces concept of “security in a zero-trust environment” to accomplish end-to-end data security in a smart city environment. It reduces the risks caused due to novel system interactions while neglecting the hassle of regular security model updating.

The work in[22] presents a mechanism with the assistance of deep neural architecture in which appropriate mitigation actions are automatically chosen optimally. Thus, the model countermeasures the cybersecurity attacks frequently faced by IoT networks. This work uses the AI method to optimize security-related Key Performance Indicators. The paper [23] analyzes a few common IoT smart medical systems, ome networks and wide area IoT networks. Further, it exploits such

analysis to design a simple method that considers the security vulnerabilities of each system individually and identifies the best mitigation method.

The IoT cybersecurity countermeasures are broadly classified into three types: authentication-based, artificial intelligence-based, and blockchain-based.

AI-based and blockchain-based models are highly important to cybersecurity detection. The paper [24] utilizes machine-learning strategies supporting vector machines, neural networks, and random forests to recognize jamming attacks. Similarly, the work in [25] exploits machine learning strategy to give protection against network-layer brute force attacks on the secure shell protocol.

It develops scalable detection methods with machine learning classifiers such as K-Nearest Neighbors decision trees and Naive Bayes, which may be efficient at attack prediction making.

The work in [26] describes various experiments which utilize machine learning strategies. It is inspired by the idea of "first difference" from statistics and economics to develop a novel classifier for attack detection in synchronized networks. It concludes that Artificial Neural Networks (ANNs) outperform conventional methods when detecting network security issues.

The work [27] removes hackers from the smart grid environment using machine learning methods.

The work in [28] creates an ensemble learning model with the assistance of deep neural networks and decision trees. It integrates a ten-fold cross-validation model for access.

The work in [29] introduces a novel authentication and encryption protocol designed with Quantum-Inspired Quantum Walks (QIQW). Further, it constructs a blockchain framework to ensure secure data transmission among devices. The primary advantage of the framework is secure data transmission and control of massive information generation. The security analysis of the framework demonstrates that it can provide security against two types of attacks: message attacks and impersonation attacks.

The study in [30] designs a novel Blockchain with Deep Learning-Empowered Cyber-Attack Detection (BDLE-CAD) model for critical infrastructures and industrial control systems. It mainly intends to detect the intrusion's existence in the network. The following Table 2 discusses the different vulnerability analysis and mitigation methods.

**Table 2: Comparison of Various vulnerability analysis and Mitigation Methods**

| Sr. No | Reference No. | Objectives | Technique used | Research Gaps |
|---|---|---|---|---|
| 1. | [9] | Static analysis of information systems for IoT cyber security | Machine-learning solutions | To analyze the vulnerability discovery in a decentralized IoT environment |
| 2. | [12] | Enhance the prediction accuracy of the Vulnerability discovery model | Multiple errors iterative analysis method and artificial neural network sign estimators | To consider multiple context information related to vulnerabilities |
| 3. | [13] | Predictive analytical model for software vulnerability discovery | New time-based differential equation model | Vulnerability saturation assumption increases the real-time prediction error rate. |
| 4. | [14] | Assists testers in Human Machine Interface (HMI) vulnerability discovery | EUFuzzer, a novel fuzzing tool | Not perfectly suitable for IoT protocols and reduces the testing accuracy in the IoT environment |
| 5. | [21] | Build an Activity-Network-Things (ANT)-centric architecture | Activity-Network-Things (ANT)-centric architecture | Lacks to provide detailed discussions about zero-day and recent vulnerabilities |
| 6. | [22] | To design countermeasures with automatic selection of mitigation strategy against IoT attacks | Novel Artificial Intelligence mechanism and Deep Neural Architecture | Do not offer complete protection against malicious twins |
| 7. | [23] | Analyze a few common IoT system styles | Analysis of general IoT attacks using a simple method | Lacks to analyze the zero-day vulnerabilities, which reduces the IoT |

| | | | | |
|---|---|---|---|---|
| | | | | performance significantly |
| 8. | [29] | Presents a new authentication and encryption-based cybersecurity model for IoT smart cities | Quantum-inspired quantum walks and new cryptographic algorithms with quantum hash functions | Lack to provide strong security against unauthorized or harmful access to the network. |
| 9. | [30] | Designs a novel BC with deep learning empowered cyber-attack detection | Enhanced chimp optimization-based feature selection (ECOA-FS), deep neural network and optimizer | Lacks to include vulnerability discovery analysis, and thus, it reduces the detection performance |
| 10. | [31] | Determine and classify the main dangers and weaknesses in IoT ecosystem and examine how these dangers might affect IoT systems and the data they handle. | Communication protocols, Cyber Security tools | Privacy preserving, Ethical considerations |
| 11. | [32] | Identify and categorize the major security challenges faced and identify the limitations and shortcomings of current security practices within the IoT domain. | Smart devices, Messaging protocol | Research efforts should be directed towards security and privacy of service discovery protocols |
| 12. | [33] | Emerging trends and advancements in IoT application layer protocols.<br>Provide insights into the practical considerations for selecting the right protocol for specific IoT applications. | Wireless communication technologies, and sensors are capable of generating and transmitting data. | Scalability and Resource Constraints, security and privacy, Machine learning and AI Integration |
| 13. | [34] | Limitations and potential conflicts between safety and security goals. | Smart devices, Cyber-physical system, integrated development tools. | To develop balanced solutions, investigate the trade-offs and potential conflicts between safety and security goals. |
| 14. | [35] | Address and analyze the threat of IoT botnets in the context of IoT networks. | IoT botnet, | Implementing robust security measures to protect IoT threats from botnet attacks. |
| 15. | [36] | Identify and analyze security threats specific to IoT environments for recognizing and mitigating DDoS attacks | IoT security threats, attack recognition | Highlighting the requirement for strong security measures to safeguard the availability and integrity |
| 16. | [37] | Attacks at various levels such as application, Perception and Transportation layer. | Blockchain | Greater security and privacy may be provided by new protocols and algorithms. |
| 17. | [38] | Secure IoT implementation by IoT framework. | Anticipating upcoming trends and technologies in IIoT and their potential impact on cybersecurity. | Necessary to conduct penetration testing, and evaluate attributes for finding each attack type characteristics.. |
| 18. | [39] | Identifying the nature of IoT | Improve IoT security by Fog | Improving the safety of |

| | | | | |
|---|---|---|---|---|
| | | networks' primary security concerns and threats. | computing and block chain. | each layer's risks. |
| 19. | [40] | To reveal current IoT threats. | Development and deployment of a novel honeypot (IoTPOT) for capturing and analyzing IoT threats. | All emerging IoT threats and analysis of mitigation strategies. |
| 20. | [41] | Developing theoretical framework for dealing with IoT hazards. | Creation of a conceptual framework for analyzing and dealing with IoT hazards. | The framework's practical implementation and real-world effectiveness |
| 21. | [42] | Analyze security attacks in IoT. | Analysis of existing security attacks in IoT environments. | Novel solutions or countermeasures for IoT security attacks. |
| 22. | [43] | To explore the use of blockchain for IoT security. | Investigation of how blockchain technology can enhance IoT security. | Practical implementation challenges and scalability issues related to blockchain in IoT security |
| 23. | [44] | To monitor social media for IoT cyber threats. | Utilization of social media monitoring for identifying and tracking IoT cyber threats. | To cover the limitations or challenges of relying on social media for threat detection. |
| 24. | [45] | To give a general understanding of the IoT security environment. | Comprehensive review and analysis of the IoT security landscape. | Delve into specific security solutions or practical implementation strategies. |
| 25. | [46] | To understand the industrial network intrusion detection solutions that use machine learning. | Examining and analyzing IDS based on machine learning for industrial IoT networks. | Implementing machine learning-based IDS in industrial IoT contexts. |
| 26. | [47] | To create a sophisticated IDS for Internet of Things security concerns. | Development of an intelligent IDS to counter IoT cyber threats. | Potential limitations or challenges of implementing IDS in diverse IoT environments. |
| 27. | [48] | To classify IoT threats using the Analytic Hierarchy Process (AHP). | Utilization of AHP methodology for classifying IoT threats and vulnerabilities. | Limitations or challenges associated using AHP for IoT threat classification. |
| 28. | [49] | To offer a thorough analysis of IoT threats, problems, and solutions. | IoT threats and attacks are reviewed and categorized, along with difficulties and potential remedies. | Emerging threats or the latest solutions in the rapidly evolving IoT security landscape. |
| 29. | [50] | To develop an IoT threat detection system using network statistics and GANs (Generative Adversarial Networks). | Utilization of GANs and network statistics for IoT threat detection. | Practical challenges or limitations of implementing GAN-based threat detection in IoT environments. |
| 30. | [51] | To assess human susceptibility to IoT threats in home environments. | Investigation of human factors contributing to IoT security vulnerabilities in home settings. | Guidelines for improving human resilience to IoT threats in home contexts. |
| 31. | [52] | Two-stage deep learning models for effective vulnerability detection, which includes identifying security weaknesses | Deep Learning | Addressing data imbalance, ensuring generalization across different systems and defending against |

| | | | | |
|---|---|---|---|---|
| | | and software flaws. | | adversarial attacks. |
| 32 | [53] | Combining semantic graphs and residual graph convolutional networks with edge attention to find weaknesses in smart contracts, especially in blockchain-based platforms like Ethereum. | Residual Graph Convolutional Networks, Semantic Graphs, and Edge Attention. | Addressing complex vulnerabilities, reducing false positives, ensuring generalization and defending against adversarial attacks. |
| 33. | [54] | To assess vulnerabilities in demand-response systems within smart grids, particularly when integrated with renewable energy sources. | Smart grid, Demand response, cyber attacks | Uncovering unknown vulnerabilities, developing effective detection methods. |

## VI. RESEARCH GAP ANALYSIS

The major research gaps not filled in the existing studies are as follows.

- The statistical models consume more time and high resources for vulnerability discovery. The machine learning models are lacking in real-world smart computing performance.
- Most existing works fail to effectively discover cybersecurity vulnerabilities, especially zero-day vulnerabilities and unknown attacks in smart computing environments. Zero-day vulnerability prediction is very important to accomplish better performances.
- The performance of the machine and deep learning algorithms integrated into existing methods are not evaluated with the most recent general datasets. They only evaluate performances with fundamental datasets or synthetic datasets.
- The existing security vulnerability discovery model lacks strong security against unauthorized or harmful access to the network.
- Most existing schemes try to fit the existing security methods with the smart computing environment. But in reality, it is a proliferated technology, and it is essential to develop novel methods only suitable for the smart environment.
- The existing solutions fail to deal with the most ingenious and novel attackers. It also fails to consider the multiple smart computing characteristics during the design of the security algorithm.

### 6.1 Research Questions

**RQ1:** What types of cybersecurity attacks occurred over the smart computing environment, and why is it vital to perform vulnerability discovery before mitigation?
**RQ2:** What are the different vulnerability discovery models, and how to analyze different cybersecurity vulnerabilities in smart computing environments?
**RQ3:** What are the countermeasures mainly proposed and why is it essential to analyze the research gaps?
**RQ4:** Why is it significant to develop a novel cybersecurity solution highly adaptable for a resource-limited smart computing environment?
**RQ5:** How to design a countermeasure against various types of smart computing cybersecurity vulnerabilities?

## VII. CONCLUSION

The heterogeneous technology utilization, complex data generation, different types of novel attacks, and resource-limited tiny smart device characteristics increase the cybersecurity challenges in this environment. Hence, effective analysis of security vulnerabilities and a detailed review of available countermeasures are crucial in deciding appropriate security solutions for the smart computing environment. The vulnerability discovery models should consider the most recent and zero-day attacks during discovery to accomplish accurate analysis models. The security mechanism design should satisfy the following security requirements: data confidentiality, access control, correctness, completeness, authentication, availability, and user privacy level. No effective single security solution can accommodate smart computing's expanded range of needs. The security mechanism also considers the resource limitation characteristics. A good cybersecurity model must accomplish a better tradeoff between network performance and security level. Also, it needs to consider the security requirements of diverse applications to improve the contribution of smart computing development worldwide.

## VIII. REFERENCES

[1] K. Shafique, B. A. Khawaja, F. Sabir, S. Qazi, and M. Mustaqim, “Internet of things (IoT) for next-generation smart systems: A review of current challenges, future trends and prospects for emerging 5G-IoT scenarios,” IEEE Access, vol. 8, pp. 23022–23040, 2020.

[2] A. Goudarzi, F. Ghayoor, M. Waseem, S. Fahad, and I. Traore, "A Survey on IoT-Enabled Smart Grids: Emerging, Applications, Challenges, and Outlook," Energies, vol. 15, no. 19, 2022.

[3] R. O. Andrade, S. G. Yoo, L. Tello-Oquendo, and I. Ortiz-Garcés, "A comprehensive study of the IoT cybersecurity in smart cities," IEEE Access, vol. 8, pp. 228922–228941, 2020.

[4] "IoT Connected Devices Worldwide." [Online]. Available:https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/

[5] I. Lee, "Internet of Things (IoT) cybersecurity: Literature review and IoT cyber risk management," Futur. Internet, vol. 12, no. 9, 2020.

[6] T. M. Fernández-Caramés and P. Fraga-Lamas, "Teaching and learning iot cybersecurity and vulnerability assessment with shodan through practical use cases," Sensors, vol. 20, no. 11, 2020.

[7] U. Inayat, M. F. Zia, S. Mahmood, H. M. Khalid, and M. Benbouzid, "Learning-based methods for cyber-attacks detection in IoT systems: a survey on methods, analysis, and future prospects," Electronics, vol. 11, no. 9, 2022.

[8] R. J. Raimundo and A. T. Rosário, "Cybersecurity in the internet of things in industrial management," Appl. Sci., vol. 12, no. 3, 2022.

[9] I. Kotenko, K. Izrailov, and M. Buinevich, "Static analysis of information systems for IoT cyber security: a survey of machine learning approaches," Sensors, vol. 22, no. 4, 2022.

[10] L. Cui, J. Cui, Z. Hao, L. Li, Z. Ding, and Y. Liu, "An empirical study of vulnerability discovery methods over the past ten years," Comput. Secur., vol. 120, 2022.

[11] G. Jie, K. Xiao-Hui, and L. Qiang, "Survey on Software Vulnerability Analysis Method Based on Machine Learning," in IEEE First International Conference on Data Science in Cyberspace (DSC), 2016.

[12] G. Jabeen, S. Rahim, G. Sahar, A. A. Shah, and T. Bibi, "Optimization of vulnerability discovery models using multiple errors iterative analysis method: An optimization of vulnerability discovery models," Proc. Pakistan Acad. Sci. A. Phys. Comput., vol. 57, no. 3, pp. 47–60, 2020.

[13] N. R. Pokhrel, N. Khanal, C. P. Tsokos, and K. Pokhrel, "Cybersecurity: a predictive analytical model for software vulnerability discovery process," J. Cyber Secur. Technol., vol. 5, no. 1, pp. 41–69, 2021.

[14] J. Men et al., "Finding sands in the eyes: vulnerabilities discovery in IoT with EUFuzzer on human machine interface," IEEE Access, vol. 7, pp. 103751–103759, 2019.

[15] A. Bekkali, M. Essaaidi, M. Boulmalf, and D. Majdoubi, "Systematic Literature Review of Internet of Things (IoT) Security," Adv Indynamical Syst. Appl., vol. 21, pp. 25–39, 2022.

[16] A. M. Albalawi and M. A. Almaiah, "Assessing and reviewing of cyber-security threats, attacks, mitigation techniques in IoT environment," J. Theor. Appl. Inf. Technol, vol. 100, pp. 2988–3011, 2022.

[17] T. M. Ghazal, M. A. Afifi, and D. Kalra, "Security vulnerabilities, attacks, threats and the proposed countermeasures for the Internet of Things applications," Solid State Technol, vol. 63, pp. 31–45, 2020.

[18] M. Abdullahi et al., "Detecting Cybersecurity Attacks in Internet of Things Using Artificial Intelligence Methods: A Systematic Literature Review," Electronics, vol. 11, 2022.

[19] A. B. Pandey, A. Tripathi, and P. C. Vashist, "A survey of cyber security trends, emerging technologies and threats," in Cyber Security in Intelligent Computing and Communications, 2022, pp. 19–33.

[20] A. N. Alahmadi, S. U. Rehman, H. S. Alhazmi, D. G. Glynn, H. Shoaib, and P. Solé, "Cyber-Security Threats and Side-Channel Attacks for Digital Agriculture," Sensors, 2022.

[21] J. Fan et al., "Understanding Security in Smart City Domains From the ANT-centric Perspective," IEEE Internet Things J., 2023.

[22] A. Mpatziakas, A. Drosou, S. Papadopoulos, and D. Tzovaras, "IoT threat mitigation engine empowered by artificial intelligence multi-objective optimization," J. Netw. Comput. Appl., vol. 203, 2022.

[23] M. Gromov, D. Arnold, and J. Saniie, "Tackling Multiple Security Threats in an IoT Environment," in IEEE International Conference on Electro Information Technology (eIT), 2022, pp. 290–295.

[24] T. Berghout, M. Benbouzid, and S. Muyeen, "Machine learning for cybersecurity in smart grids: A comprehensive review-based study on methods, solutions, and prospects," Int. J. Crit. Infrastruct. Prot, vol. 38, 2022.

[25] J. Luo, "A Bibliometric Review on Artificial Intelligence for Smart Buildings," Sustainability, vol. 14, 2022.

[26] T. Mazhar et al., "Analysis of Challenges and Solutions of IoT in Smart Grids Using AI and Machine Learning Techniques: A Review," Electronics, vol. 12, 2023.

[27] H. Szczepaniuk and E. K. Szczepaniuk, "Applications of Artificial Intelligence Algorithms in the Energy Sector," Energies, vol. 16, 2023.

[28] M. E. Zamponi and E. Barbierato, "The Dual Role of Artificial Intelligence in Developing Smart Cities," Smart Cities, vol. 5, pp. 728–755, 2022.

[29] A. A. Abd El-Latif, B. Abd-El-Atty, I. Mehmood, K. Muhammad, S. E. Venegas-Andraca, and J. Peng, "Quantum-inspired blockchain-based cybersecurity: securing smart edge utilities in IoT-based smart cities," Inf. Process. Manag., vol. 58, no. 4, 2021.

[30] M. Ragab and A. Altalbe, "A Blockchain-based

architecture for enabling cybersecurity in the internet-of-critical infrastructures," C. Mater. Contin, vol. 72, pp. 1579–1592, 2022.

[31] Y. Choudhary, B. Umamaheswari, and V. Kumawat, "A study of threats, vulnerabilities and countermeasures: An IoT perspective," Shanlax Int. J. Arts, Sci. Humanit., vol. 8, pp. 39–45, 2021.

[32] G. Nebbione and M. C. Calzarossa, "Security of IoT Application Layer Protocols: Challenges and findings," Futur. Internet, vol. 12, p. 55, 2020.

[33] N. Bibi, F. Iqbal, S. Akhtar, R. Anwar, and S. Bibi, "A Survey of Application Layer Protocols of Internet of Things," Int. J. Comput. Sci. Netw. Secur., vol. 21, pp. 301–311, 2021.

[34] D. Mitra, S. Goswami, D. Hati, and S. Roy, "Comparative Study Of IoT Protocols," Pjaee. Smart Appl. Data Anal. Smart Cities, vol. 17, p. 2020, 2021.

[35] S. Dange and M. Chatterjee, "IoT botnet: The largest threat to the IoT Network," Adv. Intell. Syst. Comput., vol. 22, pp. 137–157, 2019.

[36] M. H. Ali et al., "Threat analysis and distributed denial of service (DDoS) attack recognition in the internet of things (IoT)," Electronics, vol. 11, p. 494, 2022.

[37] A. Gerodimos, L. Maglaras, and N. Ayres, "IoT: Communication protocols and security threats," Preprints, vol. 25, p. 2021110214, 2021.

[38] K. Tsiknas, D. Taketzis, K. Demertzis, and C. Skianis, "Cyber threats to industrial IoT: A survey on attacks and countermeasures," IoT, vol. 2, pp. 163–186, 2021.

[39] I. Ahmad, M. S. Niazy, R. A. Ziar, and S. Khan, "Survey on IoT: Security threats and applications," J. Robot. Control, vol. 2, pp. 38–49, 2021.

[40] Y. M. Pa, S. Suzuki, K. Yoshioka, T. Matsumoto, T. Kasama, and C. Rossow, "IoTPOT: A novel honeypot for revealing current IoT threats," J. Inf. Process., vol. 24, pp. 522–533, 2016.

[41] M. Harbers, M. Bargh, R. Pool, J. Van Berkel, and S. Choenni, "A conceptual framework for addressing IoT threats: 49 Challenges in meeting challenges," in Proceedings of the 51st Hawaii International Conference on System Sciences, Hilton Waikoloa Village, HI, USA, Jan. 2018.

[42] A. Anjum, A. Siddiqua, S. Sabeer, S. Kondapalli, C. Kaur, and K. Rafi, "Analysis Of Security Threats, Attacks In The Internet Of Things," Int. J. Mech. Eng., vol. 6, pp. 2943–2946, 2021.

[43] S. Haque, K. Kumar, M. Haque, M. Faizanuddin, E. Shakeb, and A. Singh, "Blockchain Technology for IoT Security," Turkish J. Comput. Math. Educ., vol. 12, pp. 549–554, 2021.

[44] S. Alevizopoulou, P. Koloveas, C. Tryfonopoulos, and P. Raftopoulou, "Social Media Monitoring for IoT Cyber-Threats," in Proceedings of the 2021 IEEE International Conference on Cyber Security and Resilience (CSR), Rhodes, Greece, Jul. 2021.

[45] E. Schiller, A. Aidoo, J. Fuhrer, J. Stahl, M. Ziörjen, and B. Stiller, "Landscape of IoT security," Comput. Sci. Rev., vol. 44, p. 100467, 2022.

[46] A. Borcherding, L. Feldmann, M. Karch, A. Meshram, and J. Beyerer, "Towards a better understanding of machine learning based network intrusion detection systems in Industrial Networks," in Proceedings of the 8th International Conference on Information Systems Security and Privacy, Feb. 2022.

[47] K.-H. Le, M.-H. Nguyen, T.-D. Tran, and N.-D. Tran, "IMIDS: An intelligent intrusion detection system against Cyber Threats in IoT," Electronics, vol. 11, p. 524, 2022.

[48] I. A. Mohamed, A. B. Aissa, and L. F. Hussein, "Classification for IoT Threats Based on the Analytic Hierarchy Process," Int. J. Sci. Technol. Res., vol. 9, pp. 4860–4867, 2020.

[49] R. R. Krishna, A. Priyadarshini, A. V Jha, B. Appasani, A. Srinivasulu, and N. Bizon, "State-of-the-art review on IoT threats and attacks: Taxonomy, challenges and solutions," Sustainability, vol. 13, p. 9463, 2021.

[50] F. Shaikh, N. Ghani, and E. Bou-Harb, "IoT Threat Detection Leveraging Network Statistics and GAN." 2019. [Online]. Available: https://www.researchgate.net/publication/335540870_IoT_Threat_Detection_Leveraging_Network_Statistics_and_GAN

[51] E. K. Parsons, E. Panaousis, and G. Loukas, "How secure is home: Assessing human susceptibility to IoT threats," in Proceedings of the 24th Pan-Hellenic Conference on Informatics, Athens, Greece, Nov. 2020.

[52] M. M. Alhafi, M. Hammade, and K. Al Jallad, "Vulnerability Detection Using Two-Stage Deep Learning Models," J Curr. Trends Comp Sci Res, vol. 2, no. 2, pp. 77–83, 2023.

53] D. Chen, L. Feng, Y. Fan, S. Shang, and Z. Wei, "Smart contract vulnerability detection based on semantic graph and residual graph convolutional networks with edge attention," J. Syst. Softw., vol. 202, p. 111705, 2023, doi: https://doi.org/10.1016/j.jss.2023.111705.

[54] D. Tang, Y.-P. Fang, and E. Zio, "Vulnerability analysis of demand-response with renewable energy integration in smart grids to cyber attacks and online detection methods," Reliab. Eng. Syst. Saf., vol. 235, p. 109212, 2023, doi: https://doi.org/10.1016/j.ress.2023.109212.