Spectrum of Engineering Sciences
ISSN (e) 3007-3138 (p) 3007-312X Volume 4, Issue 3, 2026

SECURING IOT ENVIRONMENTS: A HOLISTIC INVESTIGATION OF CYBER THREATS, VULNERABILITIES, AND TECHNOLOGICAL IMPLICATIONS

Gohar Abbas*[1], Muhammad Mustafa[2], Asad Ullah[3], Aamir Aftab[4]

*[1,2,3,4] *Gomal Research Institute of Computing (GRIC), Faculty of Computing, Gomal University, Dera Ismail Khan, Pakistan*

*[1]gohar@gu.edu.pk, [2]attleramustafa@gmail.com, [3]asadullahbkr@gmail.com, [4]aamiraftab877@gmail.com

DOI: http://doi.org/10.5281/zenodo.22630850

Keywords
Internet of Things (IoT), Cybersecurity, IoT Security Threats, MIoT-SD Framework.

Article History
Received: 03 January 2026
Accepted: 10 February 2026
Published: 09 March 2026

Corresponding Author: *
Gohar Abbas

Abstract

As a result of the swift development of the Internet of Things (IoT), the world has just passed another stage of technical evolution that joined different fields together, including healthcare, academia, manufacturing, and infrastructure. Nonetheless, this explosive development has resulted in severe cyber security defects as well since IoT environments would be appealing to the hackers, data breaches, and manipulations of the systems. This paper used a multi-method research design as it involves a Systematic Literature Review (SLR), surveys in quantitative studies, semi-structured qualitative interviews to investigate cybersecurity threats and protection in IoT systems. The SLR that analyzed 61 articles in credible electronic libraries found typical threats like malware, phishing, and DDoS attacks, unauthorized access, and poor encryption. Defining 210 IoT stakeholders among them system engineers, IT administrators, and policymakers, a survey indicates that missing user training, budget limitations, and difficulties in implementation are the main problems. Expert interviews emphasized on industry issues with security, especially on compliance and inadequate security infrastructures. To address these concerns, this paper is proposing the Multi-layered IoT Security and Defense (MIoT-SD) model that puts emphasis on four levels of security, namely, Device Security, Network Security, Application and Platform Security and Governance and Awareness. The model will deliver a scalable framework to support the improvement of IoT ecosystem security, the finer threat detection, the ability to respond to incidents faster, as well as the increased compliance and awareness to the end-users. The study provides important perspectives on the IoT security and proposes effective ways of mitigating the current threats as they arise.

I. INTRODUCTIN

Internet has changed the lives of man into a global village in which knowledge and cultural exchange and sharing of information can be done easily. This networking is based on workforce connections among computers and mobile gadget and the increasing number of digitalized systems [1]. There are huge new opportunities in many areas due to networks created with the help of wired and wireless communication this. Nevertheless, it also includes some concerns about cybersecurity, since the data security will become one of the major concerns in such a fast-connected world. Some of the outstanding developments in this context include the Internet of Things IoT [2]. The Internet of Things is the Internet of objects

adding sensors and networks. This enormous IoT structure entails every type of devices including home use objects and industrial as well as they are interconnected in their collection, analysis, and transfer of information autonomously with the passing of IoT in different spheres of life like home automation, health, farming and industrial revolutions, the IoT has become an instrument of economic and social prosperity [3]. The next fact is a solid sign that IoT is rapidly expanding because of its geographical distribution in different countries of the world. It is projected that by 2027, the number of IoT connected devices will increase rapidly as globally there are currently 50 billion IoT connected devices and the implication is that economic impact will be at up to 11.1 trillion dollars annually. This projected growth is further argument in supporting the fact that IoT is going to transform productivity, decision making and general operations [4]. Industries have adopted the IoT to accomplish real-time data monitoring, predictive analytics, and automation, and it has been adopted into the smart city, precision agriculture, and so many other industries. With the increasing size and complexity of the networks of IoT devices, there are, however, new and, in many aspects, different levels of cybersecurity threats and risks to which specific solutions are needed [5]

The heterogeneity of the IoT devices and their deployment is one of the key IoT security challenges. The majority of IoT devices are developed with the focus on shape and utility, performance, and cost but not on security. This design philosophy exposes IoT systems to any form of cyber-attacks as such gadgets are unable to sustain complex security mechanisms unlike normal computing devices. Thus, IoT networks are in constant attack susceptible to hackers interested in accessing them unconnected or stealing data or even tampering with systems of utmost importance [6]. The rate of cybercrime perpetrated against IoT is on the rise and the security provisions against IoT systems need to be enhanced.

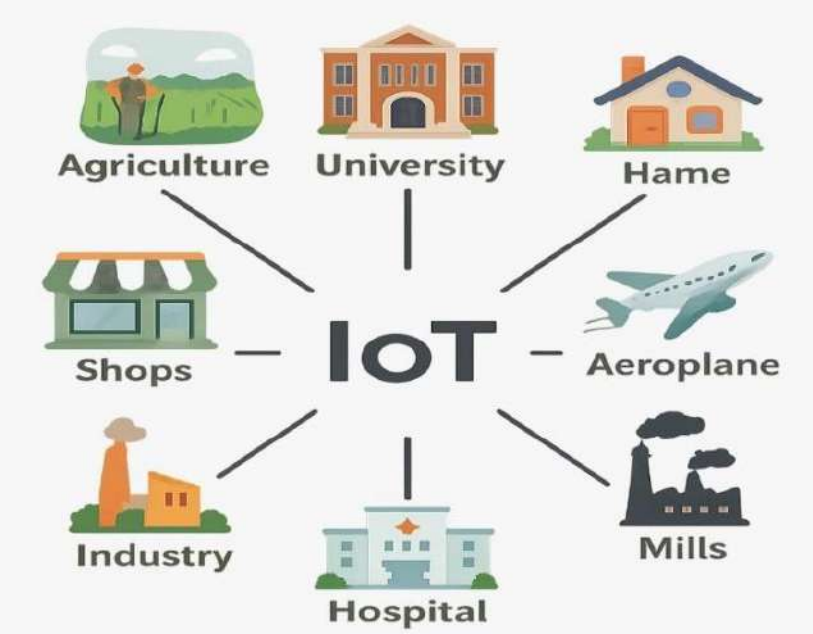


Figure-1.1 Internet of Things

Threats that are advanced against the IoT environments are many and ever-changing and, therefore, can be learned as categories. The IoT devices can be subjected to various kinds of attacks, including DDoS attacks, data breaches, malware, and Ransomware with incisive consequences in many industries. As an example, the incident with healthcare IoT devices can result

in disclosure of personal data of patients, and the incident with industrial IoT can result in lost operations and, subsequently, great financial and operational losses [7]. Just like in any other computing discipline, traditional cyber security solutions have proven effective in most of the traditional IT systems, but they are not compatible with IoT. As such, there is a need to introduce new measures, such as AI techniques, which are designed to respond IoT-specific threats will be required [8]. Owing to the opaque, dynamic, and open nature of the IoT system, cybersecurity becomes complex and complicated. A majority of IoT devices have limited CPU and memory resources, therefore, they serve as an impediment in offering such security mechanisms as encryption and multi-factor authentication. Secondly, the constant interaction of various stakeholders and elements of the IoT networks almost makes it impossible to protect such systems. Once IoT devices penetrate such domains that are central to the functioning and stability of a country, including transport, power, and health care, securing them becomes a matter of great concern. Without appropriate level of protection accorded to IoT networks this world would be subjected to tremendous risks, including, breach of essential services and gross violation of privacy and safety [9].

In order to address these issues, cybersecurity of the IoT has been taking a crucial role as it is dedicated to the development of new mechanisms and strategies that could be implemented into IoT networks. Among all the mentioned approaches, the ones based on AI offer one of the greatest opportunities to achieve the removal of a threat in real-time. With the help of AI solutions, as an instrument of machine learning and methods of anomaly detection, it is possible to process large amounts of data generated by IoT devices and show that such relationships have a scheme that indicates potential security breaches to make IoT networks more stable when exposed to a cyber-attack [10]. Based on this study, the knowledge on the existing threats, challenges and counter-measures that pertain to the IoT-based systems will be provided with respect to the cybersecurity of the IoT networks. The objectives of the research are the following ones: to identify the trends in security of IoT, to categorize security threats at each level of IoT architecture, and to evaluate the level of maturity of IoT cybersecurity systems. In addition, this study aims to present the potential improvements to the IoT security because new technologies emerge and different cybersecurity threats are being discovered. Hence, this study is oriented at securing the IoT environment and can be massively used in technological evolvement without any harm [11]. The security concerns brought about by the IoT have been looked at by many scholars since in most networks, there exist vulnerabilities that should be addressed by way of methods. The literature review was applied to identify the applicational areas of IoT, security models and privacy issues as well as the systematic review of the IoT security issues relative to the architectural layers of the IoT architecture [12]. The list of severe cybersecurity threats to IoT environments, as well as consistent effective countermeasures, were recently reviewed.

However, given the intricacy and the extended influence of IoT, a survey of the state-of-the-art security aspects in IoT is still lacking; this should comprise security examinations on each of its architectural levels and explore of proper countermeasures to each of the application layer protocols. This study attempts to address such a gap by following a step-by-step methodology to evaluate risks, issues and opportunities related to cybersecurity IoT systems [13]. With the world getting increasingly interconnected, security through IoT has never been significant, not to mention the context of connected devices and systems. The event of the IoT devices is massive and has disclosed a lot of potential opportunities that the enemies might exploit advantageously. Placing IoT technology into the goal of the numerous industries, including healthcare, transportation, and industrial automation, it is also crucial to design a unified approach towards the protection of cybersecurity [14]. This paper proceeds with research on IoT cybersecurity in IoT network security threats, challenges, and countermeasures in a bid to strengthen IoT networks to accommodate challenges of a fast-changing future world of IoT [15, 16, 17].

2. MOTIVATION

In recent years, several significant cybersecurity incidents have impacted various industries globally. These incidents highlight the vulnerabilities in their systems and the need for stronger, more robust cybersecurity measures. Below is a summary of key cybersecurity incidents along with the resolutions implemented:

Ransomware Attack on Government Agency (City of San Diego, Government, USA, 2024). A ransomware attack targeted the City of San Diego's government agency, demanding a ransom for stolen data. The city responded by enhancing its incident response protocols to ensure faster and more efficient recovery in the face of future attacks. [18]

Phishing Targeting Telecom Customers (Telenor, Telecom, Pakistan, 2023). Telenor was attacked by phishing, aiming to steal customer credentials. In response, the company implemented multi-factor authentication (MFA), reinforcing security and making it harder for attackers to exploit user information. [19]

Data Breach in Government Database (National Database Registration Authority, Government, Pakistan, 2023). The National Database Registration Authority (NADRA) in Pakistan faced a data breach, leading to data ransom demands. The organization responded by improving its database security, ensuring that sensitive national records are better protected. [20]

Data Breach in Education (University of California, Education, USA, 2024). The University of California experienced a data breach involving a ransom demand for stolen data. The university responded by enhancing its data protection strategies to ensure that future breaches are prevented and academic data remains secure. [21]

Malware Attack on Logistics (FedEx, Logistics, USA, 2024). FedEx suffered a malware attack that resulted in data theft. The company bolstered its network security in response, aiming to prevent similar malware attacks and secure its logistics operations from future cyber threats. [22]

Phishing Attack on Banking Sector (Citibank, Banking, USA, 2024). Citibank fell victim to a phishing attack that led to credential theft. In response, the bank launched customer awareness programs to educate users on phishing risks and enhance overall security awareness. [23]

Cyberattack on Retail Giant (Kroger, Retail, USA, 2024). Kroger, a leading retail company, experienced a cyberattack involving data ransom demands. The company implemented enhanced cybersecurity protocols to safeguard sensitive customer and business data from future attacks. [24]

Phishing Attack on Social Media (Instagram, Social Media, USA, 2024). Instagram was targeted by a phishing attack aimed at stealing user credentials. The company responded by educating users about phishing and implementing measures to protect accounts from future fraudulent activity. [25]

Data Breach at Telecom Company (Vodafone, Telecom, UK, 2024). Vodafone experienced a data breach where attackers demanded ransom for the stolen data. The company responded by improving its data protection strategies, ensuring that similar breaches are prevented in the future. [26]

Cyber Espionage on Financial Services (Goldman Sachs, Banking, USA, 2024). Goldman Sachs experienced a cyber espionage attack with a focus on stealing sensitive financial information. The company responded by enhancing its security protocols, focusing on protecting critical financial data and systems from further exploitation. [27]

3. RESEARCH METHODOLOGY:

The study was a mixed methods approach that addressed the issues of cybersecurity threats, challenges, and protective solutions in Internet of Things (IoT) context of different industries. This was done using the method of merging the quantitative and qualitative methods of research in an attempt to bring out a full analysis of the topic. The results were made in the form of quantitative data collected using a Systematic Literature Review (SLR) and structured questionnaires and subject to statistical analysis of current cybersecurity practices in IoT. In parallel, the qualitative inquiry was gained through the framework of semi-structured interviews with all the major stakeholders of the research providing rich and contextual knowledge of the practical

realities and needs presented in the area. The consideration of these techniques gave a possibility to conduct a resilient analysis of current situation in cybersecurity in the Internet of Things and find key issues as well as examine existing or suggested solutions. The structured review of peer reviewed literature was conducted through the SLR, whereas the questionnaires obtained the measurable data on a larger audience. Conversely, interviews were deep, multi-dimensional and provided the experience on the ground coupled with the expertise of those working in the IoT security realm. This three-fold approach in the sources of data made the results not only complete and based on the ground but also not only dependent on theoretical issues as such, but also on practical realities required both at academic and industrial levels.

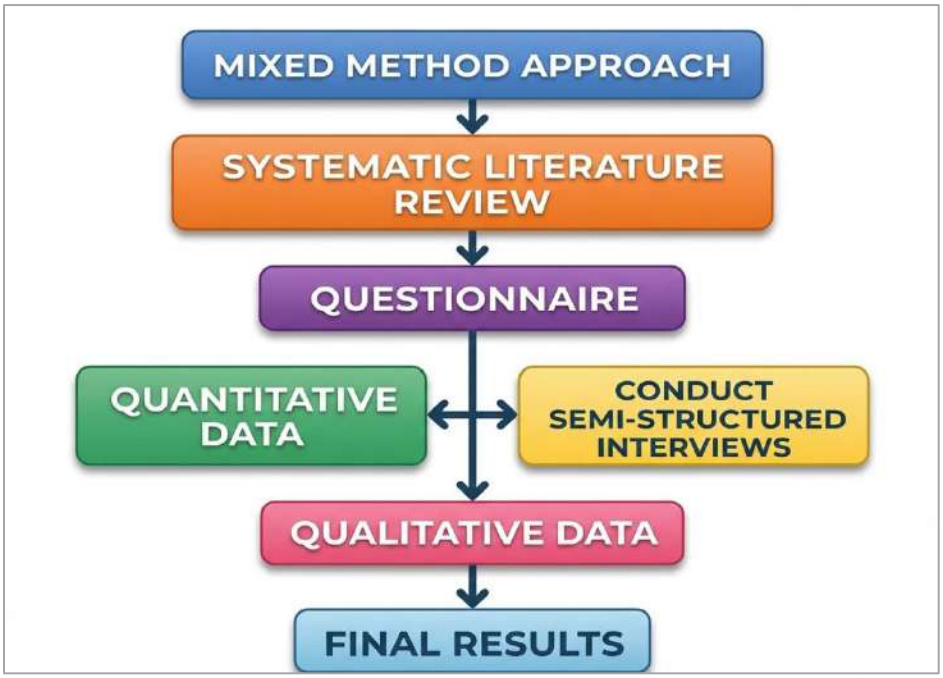


Figure 2. Methodology Flowchart

A. Systematic Literature Review (SLR)

The evaluation of the current state of cybersecurity in the IoT was done based on a Systematic Literature Review. The initial search conducted on 121 papers available in databases such as IEEE and ACM identified 61 high-quality papers by eliminating duplicates and low-quality research. The review targeted threat, vulnerability, and protection methods on healthcare, finance and manufacturing. Such keywords as IoT security and cyber threats were used in the selection process. The review established the basic comprehension and questionnaire and interview formulation. It gave big picture macro-industry perspective of cybersecurity problems and control measures.

1) **Questionnaire**

An SLR-based structured questionnaire was constructed. It gathered information about demographics, the nature of cybersecurity threats that the participants had to deal with, efficiency of security measures they have installed, and what kind of challenges they had to manage. Effectiveness was rated on a 5-point scale. The survey was sent through online means such as email, WhatsApp, and Google Forms. IT administrators, system engineers, and device manufacturers were considered target groups. The survey gave quantitative knowledge about practical cybersecurity applications and concerns in different industries.

2) **Semi-Structured Interviews**

Semi-structured interviews were conducted with key industry stakeholders such as cybersecurity consultants, policymakers, and system engineers. These interviews explored contextual and sector-specific issues that quantitative methods might overlook. Conducted through multiple channels including WhatsApp, video conferencing, and face-to-face meetings, each session lasted between 20–30 minutes. Interview topics included current threats, effectiveness of existing security measures, and recommendations for improving IoT security. The qualitative insights enriched the quantitative findings, offering deeper perspectives and expert opinions.

3) **Quantitative Data**

The number of data were calculated on the basis of SLR and questions. The trends in the IoT cybersecurity practices were summarized using descriptive statistics. The correlations between the forms of threats and effectiveness of security measures were identified with the help of inferential statistics. The presented numeric analysis offered evidence-based answers regarding the current situation with the cybersecurity of IoT. The use of statistical analysis made it possible to conduct a serious study of practical tasks and identify their gap and potential. The findings fed into feasible, evidence-based suggestions on making cybersecurity better.

4) **Qualitative Data**

The thematic analysis was performed on qualitative data gathered with the help of interviews. Coding transcripts was used to identify the repetitive themes, which included gaps in training, lack of resources, and how the stakeholders would improve. This discussion has revealed sector specific obstacles and facilitators to successful IoT cybersecurity. Such themes as Awareness and Training and Resource Constraints identified some areas to improve. These perceptions essentially filled in the gap that was missing in the quanitative data and informed model building and future suggestions. 1) Analysis of results The results were both a quantitative and a qualitative distribution in order to analyze them in a detailed manner. Statistical information demonstrated commonalities of the practices, and interviews allowed the discovery of context-specific details. The trends and the challenges were well pictured in the charts and graphs, and the findings were easily accessible. The data types were integrated so there could be triangulation, which led to simple results that could be more valid. There were significant trends, and they were directed at the technical and organizational spheres that should be improved. This step formed the foundation towards the roll-out of a custom cybersecurity framework.

Table 2: Research Design Overview

Component	Approach	Purpose
Qualitative Data	Semi Structured Interviews	Contextual insights into stakeholder challenges
Quantitative Data	SLR and Questionnaires	Statistical analysis of cybersecurity practices

A. KEY APPROACH USED IN THIS STUDY ARE DISCUSSED AS UNDER

1) DEFINITION OF RESEARCH SCOPE:

We have established in our research that there is need to search the patterns and gaps that can be applicable in the security issues, threats, attacks and challenges. As a result, it will have no other choice than to use some research questions (RQ) of the primary researches, which were formulated after analyzing pertinent literature.

Research Questions

RQ1. Which are the common cybersecurity measure used in IoT environment?

RQ2. How effective are these measure in safeguarding IoT environment?

RQ3. What challenges do organization encounter in the implementation of cybersecurity measure in IoT environment?

RQ4. What implementation can be made to current cybersecurity practice to better protect IoT environment?

2) QUERY STRING

Effective query strings were created using Boolean operators, AND, OR to make certain that the literature review is systematic and quite thorough. The application of these strings was done on scholarly databases including the IEEE Xplore, Springer Link, Elsevier, ACM Digital Library and Science Direct. Keywords and the other phrases were identified in existing literature on the basis of analysis of titles, abstracts, author keywords. The approach was used to find studies devoted to the problem of cybersecurity, threats, and counteract in the realm of IoT. The major search strings were: **"Cybersecurity in IoT environments" AND "Attacks" AND "Threats" AND "Challenges" AND "Intrusions"**, and **"IoT cybersecurity measures" AND "Technological advancement" AND "security issues"**, among others.

3) SEARCH TERMS:

Keywords or index term is very crucial in the development of the search query. Table No.2 gives us the most important terms and their substitutes which the studies of the popular researchers delivered to us.

4) KEYWORD IDENTIFICATION

These are the keywords of the corresponding types regarding the assessment of cybersecurity activities in IoT systems:

5) SEARCH QUERY

("Cybersecurity" OR "Security") AND ("Internet of Things" OR "IoT") AND ("Threats" OR "Attacks" OR "Vulnerabilities" OR "Challenges" OR "Intrusion Detection" OR "Privacy") AND ("Solutions" OR "Models" OR "Frameworks")

Table 3. Keyword identifications

Keywords Identification	
Category	**Keywords**
IoT Device Security	Data protection, Device safety, Data confidentiality, Encryption, Data privacy
Network Security for IoT	Secure communications, Malware, Phishing, cyber threats, Network system security, and device security
System Administrator Security in IoT	Endpoint security, Firewalls, Access control, Monitoring, Patch management, Network and device security,
Compliance in IoT Environments	Data compliance, Regulatory standards, IoT compliance, Privacy standards, Best practices
Cybersecurity Architecture Keywords	
Category	**Keywords**
Security Threats in IoT	Phishing, Data breaches, Ransomware, Social engineering, Cybersecurity threat, Malware
Network Security in IoT Environments	Network security, VPNs, firewalls,Cloud security, Wireless security, Secure communications
Device Security in IoT	Multi factor authentication, Device security, BYOD, Mobile device security, Malware protection
Cloud & On premises Deployment in IoT	On premises security, Cloud based environment, IoT Cloud implementation, Secure data repository

6) Online Databases

The following table reflects the list of online databases that I explored the search queries to retrieve the corresponding list of articles that should be utilized in my systematic literature review.

7) Primary Search Strategy and Secondary Search Strategy

Peer reviewed articles, empirical studies and conference papers were the primary sources which examined the effectiveness of cybersecurity precautions in IoT setups. Reviews and Meta analyses were also used to make the context wider as secondary sources. The table below gives a summary of the number of articles that one retrieves on each of the 6 online databases with and without elimination of duplicates. The column marked as before duplicate removal reports the sum of articles that were delivered by each of the databases under consideration, and the column with after duplicate removal notes the amount of dissimilar articles that remained after the elimination of duplicates. This disaggregation illuminates how wide the search of literature that was done initially and the collection of relevant articles that were collected who was used to carry on with the rest of the analysis.

Table 4. Search Query

Category	Search Query
Compliance in IoT Environments	"Privacy compliance" AND "IoT data" OR "Regulatory standards for IoT"
Network Security	"Network security" AND "IoT networks" OR "Cloud security" AND "IoT environment"
System Administrator Security in IoT	"Endpoint security" AND "IoT networks" OR "Firewall" AND "Access control"
IoT Device Security	"IoT device security" AND "cybersecurity in IoT" OR "Data privacy in IoT"
Cybersecurity Threats in IoT	"Cybersecurity threats" AND "IoT systems" OR "Phishing attacks in IoT"
Network Security in IoT	"Network security in IoT" AND "cyber threats" OR "Wireless security"
Device Security in IoT	"Device security" AND "BYOD in IoT" OR "Mobile device threats" AND "IoT networks"
Compliance Solutions	"Data privacy compliance" AND "IoT security protocols" OR "Regulatory standards for IoT"
Threat Intelligence in IoT	"Threat intelligence" AND "IoT awareness" OR "Cybersecurity education" AND "IoT users"
Cloud & On premises Deployment	"Cloud based deployment" AND "IoT data" OR "On premises security" AND "IoT systems"
Security Measures	"Incident response" AND "IoT cybersecurity" OR "Security audits" AND "IoT data"

Table 5. Online Databases

Database Name	Description	Access Link
Web of Science	Database multidisciplinary citation journal articles published by journals or conferences and books in other subjects such as computer science.	https://www.webofscience.com
Scopus	It is a vast abstract and citation database, which covers the following fields of knowledge, computer science, engineering and technology.	https://www.scopus.com

Science Direct	It uses journals, book proceedings and books. A large dissemination of full text articles of various publishers in the field of science, technology, medicine, even in the field of computer science.	https://www.sciencedirect.com
ACM Digital Library	Journal, conference proceedings, magazines, full text database articles of associations of computing machinery (ACM).	https://dl.acm.org/
Springer Link	Springer books and journals, both full text articles and book chapters ridiculing books, proceedings of conferences and journals of computer science and allied topics.	https://link.springer.com
IEEE Xplore Digital Library	Full text article index of IEEE (Institute of Electrical and Electronics Engineers) publication i.e, journals, conference proceedings as well as standards.	https://ieeexplore.ieee.org

8) Study Selection Criteria

The research studies included in the systematic literature review were chosen after a thorough screening procedure that was meant to establish their relevance and quality. The research was started with a bottom-up approach by making a thorough search in various academic databases through established search terms in terms of relevance linked to cybersecurity, IoT setting. Redundancy was eliminated by eliminating duplicates. The title and abstract screening of the studies were then conducted to expel those that were not fit into the research goals directly. It was checked whether they had full-text access, and papers that are not available were ignored. Thereafter, the studies were evaluated according to quality standards such as the clarity of the purpose, rigor of methods as well as their meaningfulness to the domain of IoT cybersecurity. It also did not consider using the non-peer reviewed sources or those that were not scholarly rigorous enough. It led to a final collection of good quality studies, which are used as the basis of in-depth analysis.

9) INCLUSION CRITERIA

- Peer-reviewed journal or conference publications
- Published between 2018 and 2024
- Focused on cybersecurity threats, challenges, or solutions in IoT environments
- Available in full-text and written in English

Table 6. Search Results Papers

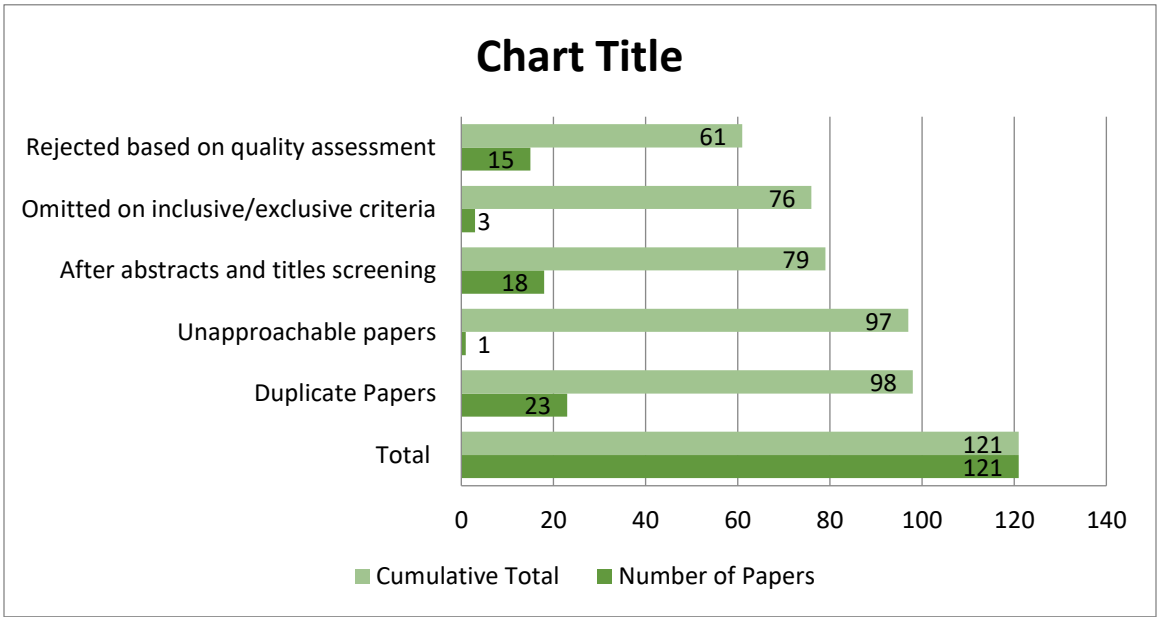
Database Name	Prior to the Duplicate Removal	Duplicate Removal
IEEE Xplore Digital Library	21	17
Web of Science	19	09
Scopus	19	12
Science Direct	21	15
Springer Link	20	11
ACM Digital Library	21	12
Total	**121**	**76**

Table 7. Quality Assessment Checklist

S. No	Question	Score (Y/N/A)
1	Are the findings based on multiple projects?	Y/N/A
2	How clear are the links between data, interpretation, and conclusions?	Y/N/A
3	Are all research questions answered adequately?	Y/N/A
4	Are negative results (if any) presented?	Y/N/A
5	Do the researchers discuss any problems with the validity/reliability of their results?	Y/N/A
6	Are statistical techniques used to analyze data adequately described and their use justified?	Y/N/A
7	Is the data collected adequately described?	Y/N/A
8	Is the purpose of the data analysis clear?	Y/N/A
9	Are the data collection methods adequately described?	Y/N/A
10	Are the variables considered by the study suitably measured?	Y/N/A
11	Are the estimation techniques used clearly described and their selection justified?	Y/N/A
12	Are the research aims clearly specified?	Y/N/A
13	Was the study designed to achieve these aims?	Y/N/A

Table 8. Summary of systematic literature review results.

Stage of SLR	Number of Papers	Cumulative Total
Initial database search	121	121
Duplicate Papers	23	98
Unapproachable papers	1	97
After abstracts and titles screening	18	79
Omitted on inclusive/exclusive criteria	3	76
Rejected based on quality assessment	15	61
Final papers	**61**	



Graph 1: Graphical Representation of search result

10) Exclusion Criteria

To establish the studies that should be comprised the research, there was a predetermined combination of the stringent and pertinent criteria. The identified studies needed to be academic publications, but they had to be peer-reviewed, through trustworthy journals or well-known conferences. The papers published after 2018 and before 2024 were taken into consideration as the latest advances and issues were reflected. One of the core needs was the clear emphasis on the issue of cybersecurity in the IoT context, i.e., on the topic of cyber threats, attacks, vulnerabilities, and security issues. In addition, findings presented research that came up with pragmatic solutions, models, or frameworks that could potentially improve the security of IoTs. All the chosen studies were written in English and provided in a full-text form so that thorough analysis could be conducted.

11) Study Selection Process

It was performed in the following two stages. Which one is level screening, title and Abstract, while the other is Quality Assessment (QA)

i. Level screening, title and abstract

A stringent multi-phase screening procedure was adopted to identify studies that were relevant as well as having quality to be selected in this systematic literature review. An exhaustive search of high quality academic databases conducted using clear search fixtures on IoT security issues, threats and solutions produced 121 research papers. The initial stage of cleansing was the deletion of 23 duplicate entries in order to ensure the uniqueness of data. After that, one article was omitted because of the lack of full-text access, which was not providing an opportunity to appropriately assess the information. Thereafter the titles and abstracts of the rest of the articles were reviewed in order to determine relevance to the study objectives and 18 irrelevant studies were excluded. A rigorous quality evaluation followed to result in a methodologically rigorous and reliable evaluation, in the course of which 15 articles were discarded because they could not pass through basic standards of scholarly strictness like clarity of purpose, methodology, and relevance to the discipline. As the final result of all the screening and assessment phase 61 reasonable and contextually applicable studies were chosen to conduct in-depth analysis composed of the main body of this systematic literature review.

ii. Quality Assessment (QA)

All the studies in this study were thoroughly quality checked to check their quality relevance, reliability and academic integrity. Against the dimensions that are important in scholarly research, a 13-point quality checklist was employed in rating each paper under each dimension. This evaluation was started by the verification of whether the papers had clearly stated research goals and whether its theme was central to the key research questions of this work. The methodological soundness was seriously examined to make sure there were proper research designs and models used. Another essential index of validity was the data analysis and therefore, ensuring that there were tools and techniques used to actualize the results.

Table 9. Year Wise Table of Papers Selected in the Study and QA

Year	Before exclusion 03 Exclusion Inclusion Duplicate 23 Inaccessible Papers 01 Abstract and title screening 18 Rejected based on quality assessment 15	After Exclusion	In Numbers
2024	[11,31,49,73,90,94,**119**]	[11,31,49,90,94]	05
2023	[04,09,10,12,13,16,**17**,18,**42**,53,**58**,68,69,	[04,10,12,16,69,104]	06

	72,95,99,104,105,106]		
2022	[06,07,08,21,25,39,40,41,43,50,61,63,66,67,86,87,93,100,109]	[06,07,08,21,41,43,50,63,66,67,87,93,100]	13
2021	[15,19,23,24,26,30,33,34,37,38,44,48,55,56,57,60,65,71,75,76,77,82,83,84,85,88,96,98,111,112,113,116,118,121]	[23,30,33,34,37,48,55,57,60,77,83,84,96,111,112,116,118]	17
2020	[01,03,05,14,28,29,36,45,46,47,51,52,54,64,74,80,81,89,97,102,103,117]	[03,05,14,28,45,47,51,54,64,80,97,102]	12
2019	[20,22,27,32,35,59,62,70,78,79,91,92,101,107,108,110,114,115,120]	[22,35,70,78,91,110,120]	07
2018	[02]		01
TOTAL	**121**	**61**	**61**

Table 10. Download Summary of Paper General

Year	Paper Number	Total count
2024	[11,119,31,49,73,90,94]	07
2023	[04,09,10,12,13,16,17,18,42,53,58,68,69,72,95,99,104,105,106]	19
2022	[06,07,08,21,25,39,40,41,43,50,61,63,66,67,86,87,93,100,109]	19
2021	[15,19,23,24,26,30,33,34,37,38,44,48,55,56,57,60,65,71,75,76,77,82,83,84,85,88,96,98,111,112,113,116,118,121]	34
2020	[01,03,05,14,28,29,36,45,46,47,51,52,54,64,74,80,81,89,97,102,103,117]	22
2019	[20,22,27,32,35,59,62,70,78,79,91,92,101,107,108,110,114,115,120]	19
2018	[02]	01
Total		**121**

B. Questionnaire Development and Distribution

Through the knowledge gained in the SLR a structured questionnaire was created to collect quantitative information concerning security practices, effectiveness and challenges of different stakeholders. The questionnaire was made available online through email, WhatsApp groups, and through Google Forms to make it accessible and maximize response rates.

Table 11 Distribution of Questionnaires

Participants Fields	No of Participants
System Engineers	75
Device Manufacturers	60
IT Administrators	75
Total	**210**

Figure Questionnaire distribution

Table 12: Questionnaire Structure

Section	Description	Key Data Collected
Effectiveness of Cybersecurity Measures	Effectiveness ratings	Ratings on a 5 point Likert scale
Implementation Challenges	Key challenges	Budget constraints, awareness levels, technical expertise
Suggested Improvements	Recommendations for enhancement	Proposals for improving (IoT) cybersecurity
Demographic Information	Participant background	Age, gender, role, sector
Encountered Cybersecurity Threats	Types and frequency	Types of threats, frequency of encounters

C. Semi Structured Interviews

Semi-structured questionnaires, industrial professionals, advisors, and decision-makers were considered some of the key stakeholders, to which qualitative data on cybersecurity management, sector-specific challenges, and proposals to improve the situation were gathered.

Table 13: Interview Overview

Stakeholder Type	Number of Participants	Interview Method	Duration
Device Manufacturers	15	Email	20 - 30 minutes
System Engineers	20	Face to Face	20 - 30 minutes
Cybersecurity Consultants	20	WhatsApp, Telephone	20 - 30 minutes
Policymakers	15	Video Conferencing	20 - 30 minutes

Sample Interview Topics

Threats and Challenges: What are some more considerations your sector needs to make about internet of things cybersecurity?

Measures Effectiveness: Measures that are used in the modern world: how are they effective in relation to IoT?

Threats?" Recommendations on how to improve: What can be done or what new actions can be taken to intensify the IoT security?

4. RESULTS OF METHODOLOGY

A. SYSTEMATIC LITERATURE REVIEW

Twelve studies were included in the table representing the results of the Systematic Literature Review (SLR). As part of the review procedure, the research papers were initially retrieved in the number of 121. At the preliminary screening stage, 46 duplicate records were detected and 23 of these records were eliminated validating the number of 98 papers. After this, one article was eliminated as it was inaccessible leaving 97 usable articles. Screening of titles and abstract resulted in exclusion of 18 papers leaving 79 papers. Inclusion and exclusion criteria based on full-text review was used to eliminate 3 more papers resulting in a total of 76 papers. Another quality screening stage led to the removal of 15 papers. Consequently, 61 studies fitted all the criteria and were incorporated in the final analysis. The total accumulating column in the table gives the number of papers left at every phase of the review process.

SLR Key Findings and Research Questions

The SLR was guided by the following research questions, and were summarized by the answers to the conducted research:

Table 14. Research Questions and Answers from SLR

RQ1. Which are the common cybersecurity measure used in IoT environment?	1. Unauthorized access: Lack of appropriate or strong authentication protocols. 2. DDoS (Distributed Denial of Service) attacks: IoT appliances employed in botnets to spam the networks. 3. Man-in-the-Middle (MITM) Attacks: Injection of electronic devices. 4. Data flows and leakages: Exceeding of sensitive information because of ineffective methods of security. 5. Malware Injection: Insertion of malware in order to use exploits in the devices. 6. Firmware Tampering: Adjusting the device firmware so as to introduce backdoors and expose vulnerabilities. 7. Insider Threats: Utillization of access to network or devices by highly trusted staff such as an employee in IT departments

RQ2. How effective are these measure in safeguarding IoT environment?	Authentication and Access Control: Between somewhat and weakly effective, with many users having passwords that are too weak and with inexperience of using multi-factor authentication (MFA). 2. Enormous protection of data encryption averts the use by the wrong hands, but inadequacy of processing power renders many IoT devices incapable of offering encryptions with high degrees of safety. 3. The effectiveness due to the resulting effectiveness in firmware and patch management is low to moderate since practices related to firmware update and patch installations vary. 4. The effectiveness of SIEM + IDS in combination is moderate or low due to the fact that organizations do not have the required tracking capabilities and response mechanisms. 5. End users and developers are exposed to low to moderate effectiveness of security training since they have insufficient level of security awareness. 6. Regulatory Compliance has the moderate effect because the applications of EU and US IoT manufacturers to various compliance regulations differ.
RQ3. What challenges do organization encounter in the implementation of cybersecurity measure in IoT environment?	1. Lack of appropriate financial resources is another problem where the organization can hardly afford comprehensive cybersecurity solutions. 2. Limited Awareness: Inadequate awareness regarding the threats and practice of security of IoT to users and developers. 3. Resistance to change is likely to be caused by the staff members refusing to adopt new measures and procedures of security. 4. This makes it hard to secure the IoT devices since they have small processing power and have limited memory size. 5. Various manufacturers and platforms providers do not have uniform security requirements to IoT devices and networks. 6. There exist threats in incorporating security provisions due to their inability to conform to established IoT infrastructure systems and network designs.

RQ4. What implementation can be made to current cybersecurity practice to better protect IoT environment	1. Authentication should go through a fortification program, including Multi-Factor Authentication (MFA) and viable password theories. 2. The organization ought to develop automated solutions that support routine firmware update as well as installation of system patches. 3. Real-Time Security Monitoring: Need to invest in Security information and event management (SIEM) systems, also known as intrusion detection systems (IDS) to monitor at all times. 4. A joint train of both users and application developers is undertaken to reduce the number of human errors besides improving the practice of security measures. 5. Privacy and Data Consent Management: Develop adherence to data protection rules e.g. GDPR and apply the concepts of privacy-by-design. 6. Tight firewalls should be executed between various segments and protocols like TLS and VPN just to protect sensitive IoT items. 7. In order to be in accordance with regulations in their operations, modern systems are required to adhere to the privacy and security standards.

2. Distribution of Questionnaires

The research data is built on 210 responses where questionnaire was mailed to 75 IT Administrators, 75 System Engineers, and 60 Device manufactures found in Pakistani Educational institutions and other educational environments of various countries overseas were contacted with the same inquiries that are: - "Cybersecurity Threats, Measures, and Improvement in Universities across the globe". The information that was obtained shows the understanding of such key stakeholders and their issues as regards to academic cybersecurity practice and policies.

Questionnaire Survey Results Responses

In the questionnaire, quantitative data on the threats to cybersecurity, quantitative data on the measures, and quantitative data on the challenges affecting several stakeholders of IoT were taken. The common threats, perceived effectiveness of the existing security measures, and implementation issues of cybersecurity are illustrated through the findings below.

Table 15. Survey Results Summary

Question	Response Distribution / Findings
1. **Which kind of cybersecurity threats have you experienced in your IoT setting?**	Phishing: 35% Ransomware: 25% DDoS Attacks: 20% Firmware Tampering: 15% Malware: 30% Unauthorized Access: 40%

2. **What do you think is the most serious risk to IoT systems in terms of cybersecurity?**	Phishing: 35% Malware: 30% Ransomware: 25% Unauthorized Access: 10%
3. **Do you think the modern IoT cybersecurity measures are effective enough and appropriate to meet such threats?**	Effective: 50% Neutral: 30% Ineffective: 20%
4. **Which cybersecurity precautions do you already use in your IoT setting?**	Device Authentication and Access Control: 70% Data Encryption: 65% Regular Firmware and Software Updates: 60% Intrusion Detection Systems (IDS): 50% Security Information and Event Management (SIEM): 40%
5. **Which of these do you view as most effective in preventing cybersecurity threats?**	Device Authentication and Access Control: 30% Data Encryption: 25% Regular Updates/Patch Management: 20% Intrusion Detection Systems (IDS): 15%
6. **Which are the problems your organization has had in applying IoT cybersecurity processes?**	Budget Constraints: 45% Limited Awareness: 40% Resistance to Change: 15%
7. **Ranking in terms of 1 to 5, what are the following challenges to your organization?**	Budget Constraints: Mean = 4.1 (Significant) Lack of Skilled Professionals: Mean = 3.5 (Moderate) Resistance to Change: Mean = 3.2 (Moderate) Lack of Awareness/Training: Mean = 4.0 (Significant) Integration Challenges: Mean = 3.4 (Moderate)
8. **What are some recommendations that you can give towards making IoT in your organization secure?**	Stronger Authentication and Access Control: 55% Regular Firmware and Software Updates: 50% Real-time Security Monitoring: 45% Enhanced Training for Users and Developers: 60% Increased Investment in Cybersecurity Tools: 40%
9. **How do you think it is possible to make the most significant improvement so that IoT systems could be secured?**	Stronger Authentication Measures: 35% Better Data Protection and Encryption: 30% Enhanced User Awareness and Training: 20% Real-time Security Monitoring: 15%
10. **Is there anything to add about the IoT cybersecurity practices in your company?**	Most respondents highlighted the need for allocating more funds, conducting regular employee training programs, and enforcing cybersecurity policies more strictly. Additionally, the necessity for real-time monitoring systems and better network segmentation was recognized.

3. Semi Structured Interview Results

Therefore, the semi-structured interviews provided the quality information input of the representatives of cybersecurity operators and administrators and policy makers. The same list of questions relating to the current cybersecurity level of the participants, issues that the participants faced, and recommendations that one can make to maximize cybersecurity were posed to all.

Significant Results of Semi Structured interviews:

Barriers: The frequent barriers that were cited were: budget constrained and low awareness of

such practices and resistance to change was often noted.

Recommendations: Money should be paid to satisfy the staff due to frequent training carried out, new policies introduced and the availability of an in-house personnel team.

Stakeholder Perceptions: There were some differences perceived among the technical and the administrative personnel; the former was concerned with the security tools and materials available and the latter was concerned with policy support.

Table 16. Semi-Structured Interviews Results

Question	Findings from Semi-Structured Interviews
RQ1. What are the most common IoT cybersecurity threats?	Phishing constantly came up in the series of interviews. Ransomware and Malware were also found as a common danger. Some of the participants mentioned Data breaches and Unauthorized Access.
RQ2. How effective are current IoT cybersecurity measures?	The respondents gave conflicting views. The respondents thought the technical control methods of encryption and access control yielded positive outputs. Security monitoring systems and incident response frameworks in real time need to be improved based on the opinions of many respondents. Lack of readiness by the users to utilize new securities protocols denied the security measures of the organization the chance to maximize their potentials
RQ3. What implementation challenges do organizations face?	There are a number of hurdles in implementations that organizations face in their work. The central obstacle to the implementation of the highest level of security is the limitation on the budget based on the reflections of various actors involved in this study. The company had a lack of proper knowledge mostly on new emerging security threats. According to the information provided by the participants, workers demonstrated their reluctance to implement both new security procedures and technologies.
RQ4. What improvements are recommended for IoT cybersecurity practices?	In their work, organizations experience a number of obstacles in implementations. The major hindrance to the establishment of the maximum security is restraint on the budget as per the considerations of the different actors around this research. The firm lacked adequate knowledge particularly in the new emerging security issues. Workers showed their unwillingness to use both new security procedures and technologies as it was

	described in the information presented by the participants.

4) Comparative Analysis of SLR, Survey, and Interview Findings

The results of the SLR are given a joint and complementary analysis together with the results of the questionnaire survey and interviews made as a part of this study.

Table 17. Comparative Analysis of SLR, Survey, and Interview Findings

Aspect	SLR Findings	Survey Findings	Interview Findings
Common IoT Cybersecurity Threats	Malware, Phishing, Unauthorized Access, Ransomware	Unauthorized Access (40%) Additional threats like DDoS attacks (20%, Firmware Tampering (15%) Phishing (35%), Malware (30%) and Ransomware (25%)	Phishing, Malware, Ransomware, Data Breaches, Unauthorized Access
Effectiveness of Current IoT Cybersecurity Measures	Such technical controls as access control, patch management, and encryption demonstrated to be partially effective. Real-time monitoring and incidence response would need to be improved.	30% rated them as neutral, 20% as ineffective and 50% of respondents found measures effective.	Mixed opinions: Some considered encryption and access control effective, but real-time monitoring and incident response need improvement.
Implementation Challenges	Budget constraints, lack of awareness, and resistance to change	Budget constraints (45%), Limited Awareness (40%), Resistance to Change (15%)	Budget constraints, awareness gaps, resistance to change, lack of skilled professionals
Recommended Improvements for IoT Cybersecurity	Improved user/developer training. Use repetitive updates and patch management. Employment of hi-tech protection equipment. Tougher authentication and access control	Enhanced training (60%), Stronger authentication (55%), Regular updates (50%), Real-time monitoring (45%)	Frequent training programs for users and developers. Regular updates and patch management. Investment in real-time monitoring systems.

The given table demonstrates consistent research findings of Systematic Literature Review (SLR), Questionnaire Survey and Semi- Structured Interviews on the following topics: threats to cybersecurity of IoT and the current level and performance of protection and implementation barriers with the corresponding recommendations.

Table 20. Suggested solutions based on the comparative analysis of SLR, Survey, and Interview findings

Aspect	Suggested Solutions
IoT Cybersecurity Threats	It is recommended that the Security Information and Event Management tools to be used, in addition to the advanced Intrusion Detection Systems to identify Phishing and Malware and Ransomware attacks early. Multi-factor authentication plus biometrics authentication are security barrier against Unauthorized Access and Data Breaches. The organization must continuously receive threat intelligence that notices different sources to be cautious of modernizing techniques of attack.
Effectiveness of Current IoT Cybersecurity Measures	Invest funds to come up with systems that enable monitoring of the security status at every moment throughout all times of the day. All the IoT devices along with their software should attain their security patches regularly. Regular checks on vulnerabilities surrounding IoT systems should be combined with immediate patching routines of the vulnerabilities to prevent exploits.
Implementation Challenges	Cybersecurity also needs more funding when it comes to installing new security measures that consist of top-of-the-line encryption and artificial intelligence-based control and data safety software. Through the pledge to awareness campaigns, all stakeholders who will include the users and developers and the administrators will be trained continuously on cybersecurity of the IoT. Implementation of new cybersecurity technologies will be successful when middle-management is given the concentrated support of the top management as such a correlation reduces the employee resistance to change.
Recommended Improvements for IoT Cybersecurity	This group ought to start educative initiatives that would entail training of both the developers and the users on advanced risks of security in IoT and how to secure them. Standardization of security measures ought to produce a uniform security specification that will provide a similar level of protection to all the IoT devices. Data encryption systems ought to have an absolute encryption that covers both storage of information and transfer of the information hence securing IoT data confidentiality and its integrity. The organization must also perform periodic security audits as well as risk assessment that records the vulnerabilities that enable them improve their security practices. Critical IoT devices should have a separate network space and their security such as VPN and TLS protocols should be applied to communication as well.

The proposed solutions are made based on the requirements that are extracted out of crucial data obtained by the SLR and Survey in connection with the IoT security recommendations with the aim of formulating more effective cybersecurity practices of IoT.

V. Future work

As the present research has revealed, IoT cybersecurity should be addressed using a complex principle, which incorporates high-level technical solutions and establishes friendly policy and training models alongside. The mixed method design brought success in hosting the complexity of the problem. The model realized caterers to major weaknesses as it is also flexible across industries. A further research study may involve conducting automatic policies based on blockchain or AI. Longitudinal studies should also be encouraged to evaluate the effect of the model over the time. It is always essential to continue interacting with the stakeholders so that they can be sustainable and effective.

- The integration of technical and organizational components improves overall security posture and resilience.
- User training and awareness significantly reduce risks related to human error and insider threats.
- The model is adaptable to various IoT sectors with differing resource constraints and threat profiles.

VII. CONCLUSION

The study has been carried out on the interactive security issues that emerge in the context of Internet of Things IoT scenario. The study used a combination of Systematic Literature Review (SLR) analysis skills and the quantitative survey and qualitative interviewing techniques to investigate critical cybersecurity issues and explore the existing protective measures in the healthcare and education and industrial domains. The Systematic Literature Review revealed that encryption and IDS as well as threat detection solutions based on AI are a reality whilst standard operating frameworks and cross-platform capabilities are inefficient in the area. Device disparity together with inadequate resources and constraints in user knowledge continue to hamper all security efforts. The results of the surveys provided the practical evidence related to the way the representatives of the IoT community evaluate the effectiveness of the security systems existing today. This survey found out that organizations are not comfortable with their security solution despite the fact that standards employed are not in tandem with the carried out performance rates especially when operating in a limited budgetary environment. The training of the users program with regulatory enforcement and individual threats mitigation strategies relating to each industry became important areas of feedback based on the responses to the interview questions.

In general, the results favor a multi-layered and context-sensitive security framework, which consists of technical, organizational, and behavioral layers, confirming that not a single intervention can secure all the aspects of IoT systems. The suggested framework of the present study combines the best approaches at various levels starting with secure design of devices and continuing to user education and cyber threats intelligence thus providing the comprehensive roadmap to improving cybersecurity in the IoT landscape.

Acknowledgments

This was an independent research that was not sponsored by an agency, facility or public organization. It was a complete self-governed research and was not assisted by any external aid, in terms of funding and resources.

Author Contributions

Conceptualization and Supervision: Gohar Abbas, Dr. Mudasir Mahmood.

Research, Authoring, and Revising: Dr. Muhammad Farhan.

Each of the authors has read and accepted the final copy of the manuscript.

Conflict of Interest

These authors assert that they do not have a conflict of interest with regard to the current work on Securing IoT Environments: A Holistic Investigation of Cyber Threats, Vulnerabilities, and Technological Implications.

Ethics Approval

This paper was fully self-administered and the information provided was through an in-depth self-diagnosis using the Google scholar literature

search. Since all figures and diagrams were made separately by the authors, no other ethics approval was necessary.

Funding
The authors confirm that the study on the topic of the article, titled, "Securing IoT Environments: A Holistic Investigation of Cyber Threats, Vulnerabilities, and Technological Implications, was never funded by any organization, whether public, commercial, or non-profit.

REFERENCES

G. Knieps, "Digitalization technologies: The evolution of smart networks," in *A Modern Guide to the Digitalization of Infrastructure*, Cheltenham, UK: Edward Elgar Publishing, 2021, pp. 43–58.

G. Lampropoulos, K. Siakas, and T. Anastasiadis, "Internet of Things in the context of Industry 4.0: An overview," *Int. J. Entrepreneurial Knowl.*, vol. 7, no. 1, pp. 4–19, 2019.

I. Batra, C. Sharma, A. Malik, S. Sharma, M. S. Kaswan, and J. A. Garza-Reyes, "Industrial revolution and smart farming: A critical analysis of research components in Industry 4.0," *The TQM Journal*, 2024.

O. Peter, A. Pradhan, and C. Mbohwa, "Industrial Internet of Things (IIoT): Opportunities, challenges, and requirements in manufacturing businesses in emerging economies," *Procedia Comput. Sci.*, vol. 217, pp. 856–865, 2023.

D. Ghelani, T. K. Hua, and S. K. R. Koduru, "Cyber security threats, vulnerabilities, and security solutions models in banking," *Authorea Preprints*, 2022.

E. Stracqualursi, A. Rosato, G. Di Lorenzo, M. Panella, and R. Araneo, "Systematic review of energy theft practices and autonomous detection through artificial intelligence methods," *Renew. Sustain. Energy Rev.*, vol. 184, p. 113544, 2023.

X. V. Nguyen et al., "Prevalence and financial impact of claustrophobia, anxiety, patient motion, and other patient events in magnetic resonance imaging," *Top. Magn. Reson. Imaging*, vol. 29, no. 3, pp. 125–130, 2020.

L. Qudus, "Advancing cybersecurity: Strategies for mitigating threats in evolving digital and IoT ecosystems," *Int. Res. J. Mod. Eng. Technol. Sci.*, vol. 7, pp. 3195–3201, 2025.

M. M. Nair and A. K. Tyagi, "Privacy: History, statistics, policy, laws, preservation and threat analysis," *J. Inf. Assur. Secur.*, vol. 16, no. 1, 2021.

K. Kimani, V. Oduol, and K. Langat, "Cyber security challenges for IoT-based smart grid networks," *Int. J. Crit. Infrastruct. Prot.*, vol. 25, pp. 36–49, 2019.

I. H. Sarker, A. I. Khan, Y. B. Abushark, and F. Alsolami, "Internet of Things (IoT) security intelligence: A comprehensive overview, machine learning solutions and research directions," *Mob. Netw. Appl.*, vol. 28, no. 1, pp. 296–312, 2023.

M. Aly, F. Khomh, M. Haoues, A. Quintero, and S. Yacout, "Enforcing security in Internet of Things frameworks: A systematic literature review," *Internet Things*, vol. 6, p. 100050, 2019.

P. Radanliev, D. De Roure, C. Maple, J. R. Nurse, R. Nicolescu, and U. Ani, "AI security and cyber risk in IoT systems," *Front. Big Data*, vol. 7, p. 1402745, 2024.

O. G. Swathika, A. Karthikeyan, K. Rout, and S. Hatkar, "Cybersecurity deployment in smart grids: Critical review, applications, protection and challenges," *IEEE Access*, 2024.

S. Ksibi, F. Jaidi, and A. Bouhoula, "A comprehensive study of security and cyber-security risk management within e-Health systems: Synthesis, analysis and a novel quantified approach," *Mob. Netw. Appl.*, vol. 28, no. 1, pp. 107–127, 2023.

T. Zhukabayeva, L. Zholshiyeva, N. Karabayev, S. Khan, and N. Alnazzawi, "Cybersecurity solutions for Industrial Internet of Things–Edge Computing integration: Challenges, threats, and future directions," *Sensors*, vol. 25, no. 1, p. 213, 2025.

A. Salam, "Internet of things for sustainability: Perspectives in privacy, cybersecurity, and future trends," in *Internet of Things for Sustainable Community Development: Wireless Communications, Sensing, and Systems*, Cham, Switzerland: Springer Int. Publ., 2024, pp. 299–326.

P. Ewoh and T. Vartiainen, "Vulnerability to cyberattacks and sociotechnical solutions for health care systems: systematic review," *J. Med. Internet Res.*, vol. 26, p. e46904, 2024.

S. Wassermann, M. Meyer, S. Goutal, and D. Riquet, "Targeted Attacks: Redefining Spear Phishing and Business Email Compromise," arXiv preprint arXiv:2309.14166, 2023.

J. Li, W. Xiao, and C. Zhang, "Data security crisis in universities: Identification of key factors affecting data breach incidents," *Humanities and Social Sciences Communications*, vol. 10, no. 1, pp. 1-18, 2023.

A. P. Ortiz and A. E. Arenas, "An Analysis of Data Breach Notifications in the Educational Sector: A Situational Crisis Communication Theory Perspective," 2024.

E. Seid, S. Satheesh, O. Popov, and F. Blix, "FAIR: cyber security risk quantification in logistics sector," *Procedia Comput. Sci.*, vol. 237, pp. 783-792, 2024.

W. Yuspin, A. O. Putri, A. Fauzie, and J. Pitaksantayothin, "Digital Banking Security: Internet Phishing Attacks, Analysis and Prevention of Fraudulent Activities," *Int. J. Safety & Security Eng.*, vol. 14, no. 6, 2024.

S. Prajapat, A. S. Gaur, P. Soni, N. Nagar, and P. Goswami, "Cyber Attacks and Review of Recent Data Breach Incidents Their Trends and Measures," in *The International Conference on Computing, Communication, Cybersecurity & AI*, Cham: Springer Nature Switzerland, 2024, pp. 549-576.

F. P. E. Putra, A. Zulfikri, G. Arifin, and R. M. Ilhamsyah, "Analysis of phishing attack trends, impacts and prevention methods: literature study," *Brilliance: Research of Artificial Intelligence*, vol. 4, no. 1, pp. 413-421, 2024.

A. S. Karandikar, "Cybersecurity in Telecom: Protecting Software Systems in the Digital Age," *Int. J. Comput. Eng. Technol. (IJCET)*, vol. 15, no. 5, pp. 658-665, 2024.

M. E. Susila and A. A. Salim, "Cyber espionage policy and regulation: A comparative analysis of Indonesia and Germany," *Padjadjaran Jurnal Ilmu Hukum (Journal of Law)*, vol. 11, no. 1, pp. 122-144, 2024.