International Journal of Advanced Engineering and Management Research

Vol. 10, No. 06; 2025

ISSN: 2456-3676

Investigating a Vulnerability Assessment on Security of Iot Application Layer Protocol: Using Agricultural Sector as Case Study

Seun Mayowa Sunday
ADEY Innovations Limited,
Stone House, GL10 3EZ, Gloucester, United Kingdom

doi.org/10.51505/ijaemr.2025.1522 URL: http://dx.doi.org/10.51505/ijaemr.2025.1522

Received: Nov 22, 2025 Accepted: Dec 02, 2025 Online Published: Dec 15, 2025

Abstract
This work proposes a machine-learning-based vulnerability identification and mitigating framework and explores the weaknesses in IoT application layer protocols, especially in the agriculture sector. By use of a systematic literature review (SLR), the study reveals shared hazards including man-in-the-middle attacks, Denial of Service (DoS) attacks, and Distributed Denial of Service (DDoS) attacks. The suggested system detects, categorises, and responds to these hazards efficiently using adaptive machine learning models and real-time traffic analysis. By means of simulated attack scenarios, evaluation of the framework shows its capacity to greatly improve the security of IoT settings by providing real-time protection and flexibility to meet changing threats. With recommendations for additional developments to increase its applicability across different IoT contexts, this research helps the field by offering a specialised, IoT-oriented security framework that meets the special difficulties of securing IoT devices.

Keywords: IoT security, application layer protocols, machine learning, vulnerability detection, real-time analysis, DoS attacks, DDoS mitigation, cybersecurity framework.

1. Introduction

The Internet of Things (IoT) is a promising technology that offers solutions that are both efficient and trustworthy, and it is working towards modernizing several different fields. To automatically maintain and monitor agricultural farms with minimal input from humans, technologies based on the Internet of Things are currently being developed (Farooq et al, 2019). In its most basic form, the Internet of Things (IoT) is an integration of various devices that communicate, sense, and interact with their internal and external states through the integrated technology that IoT contains. Smart cities, homes, cars, electronics, healthcare, transportation, wearables, farming, and a great lot more are just a few of the huge variety of services IoT offers. The exponential rate of expanding use of these gadgets has produced a lot of data that must be handled and examined. Though they simplify people's lives, these gadgets also expose a range of security risks and issues (Iqbal, 2020). These not only make consumers worried about implementing them in delicate surroundings, such as e-health and smart farming, but they also pose hazards for the IoT's future development in the coming years.

Vol. 10, No. 06; 2025

ISSN: 2456-3676

According to Farooq et al (2020), the primary uses of IoT in agriculture include Precision Farming, Livestock Management, and Greenhouse Monitoring, which are categorized into various monitoring sectors. The monitoring of these applications is facilitated by various IoT-based sensors and devices, which utilize wireless sensor networks (WSNs) to enable farmers to gather pertinent data through sensing devices. IoT-based configurations utilise cloud services to analyse and interpret remote data, enabling researchers and agriculturists to make more informed decisions. In Figure 1.1, a schematic diagram illustrates agricultural trends that enable secure, cost-effective communication between greenhouses, livestock, farmers, and fields. Using wireless devices, IoT agricultural networks provide real-time crop and animal monitoring. The graphic displays two sensor kits (Libelium Smart Agriculture Xtreme IoT Vertical Kit and Crop/ Plant Monitoring Sensor Kit) that monitor soil moisture, leaf wetness, temperature, humidity, productivity, and air movement. The MooMonitor sensor tracks animal health, reproduction, feeding, rumination, and resting. Agriculture servers, gateways, and databases maintain records and give on-demand services to authorized users.

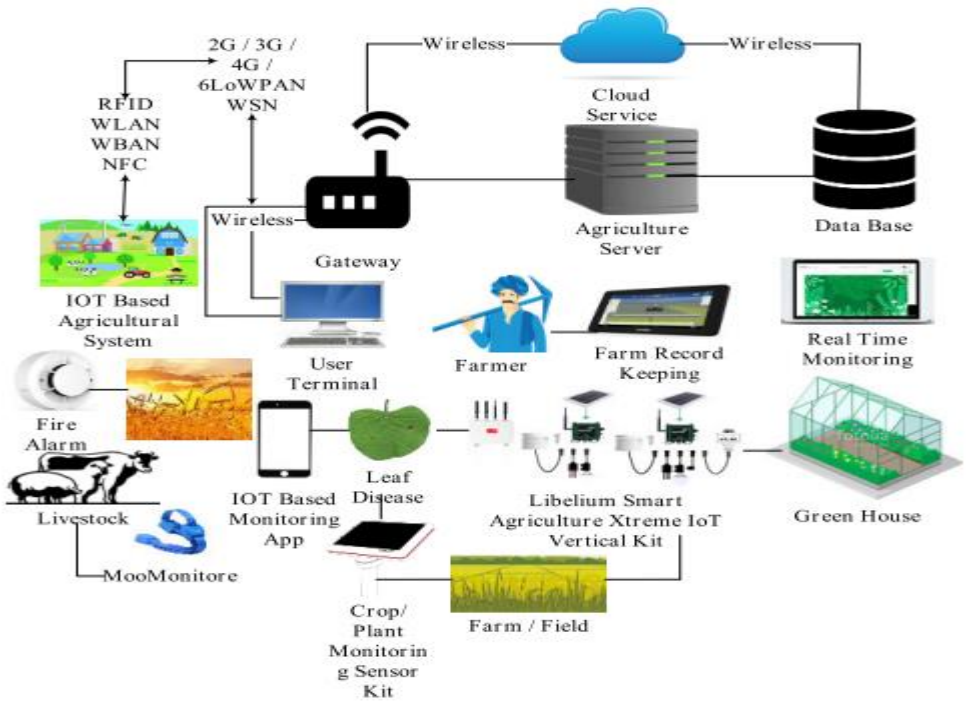


Figure 1. Agricultural Trend (Farooq et al, 2019)

Nevertheless, contemporary IoT systems possess applications that are special to certain contexts. These applications necessitate the meticulous identification of sensors and settings, prompt data collecting and optimization, and control based on rules. These results were the shift from conventional mechanical farming methods to intelligent farming, due to the substantial resources needed to achieve AI optimization (Maraveas et al, 2022).

Vol. 10, No. 06; 2025

ISSN: 2456-3676

ICT systems are the most common cybercrime tool for stealing money, IP, corporate secrets, and other assets. Cybersecurity is the set of techniques, skills, and procedures that safeguard networks, computers, programs, and data against viruses, attacks, damage, and unauthorised access. Ransomware, endpoint attacks, phishing, third-party attacks, supply chain attacks, artificial intelligence and Machine Learning-driven attacks, crypto-jacking, cyber physical attacks, state sponsored attacks, IoT attacks, threats to smart devices, and attacks on connected, semi-autonomous, or autonomous vehicles are emerging daily. These cyber-attacks have increased terrorism, financial ruin, and bodily injuries or fatalities (Demestichas et al, 2020).

The fast advancement and adoption of intelligent communication technologies, together with the incorporation of the Internet of Things (IoT) and the digitalization and automation of corporate processes, provide fresh vulnerabilities and hazards in terms of information and communication technology (ICT) security in the worldwide market. Attacks on diverse smart agricultural systems can result in significant security concerns within the dynamic and dispersed cyber-physical environment. Such threats and assaults have the potential to cause significant disruptions to networked enterprises (Demestichas et al, 2020). In their study, Myrutyunjay et al. (2024) emphasized that the use of Artificial Intelligence (AI) and Machine Learning (ML) in agriculture gives rise to important problems surrounding data privacy and confidentiality. Given that these technologies depend on extensive agricultural data, it is imperative to prioritize data protection since agricultural systems are susceptible to cyberattacks and data breaches.

Digvijaysinh (2019) also opined that the severity of hacking risks in IoT environments is heightened due to attackers' attempts to gain control of equipment such as traffic lights, door locks, autos, or pacemakers. With the increasing number of internet-connected gadgets and their interconnectivity, hackers have a greater capacity to have harmful effect on the physical environment. However, during the initial stages of automation, the field of information technology (IT) was the exclusive target of security vulnerabilities. Operational Technology (OT) was segregated and uncomplicated to configure. Both the Information Technology (IT) and Operational Technology (OT) sectors require cybersecurity in the present day due to their seamless integration. The presence of numerous dispersed production facilities, primarily in the agricultural sector, provided attackers with more targets to exploit, hence facilitating their ability to gain access, assume control, and jeopardise the safety of machinery (Kristen, 2021).

The significance of cybersecurity is growing as computers permeate all aspects of our lives in this age of the Internet and information and communication technology (ICT) systems. The ramifications of this have wide-ranging effects on individuals and systems that rely on technology and its security. The networked digital devices that are part of an IoT system encompass many technologies and computer equipment. The use of IoT systems is increasingly widespread in key sectors of the economy, including agriculture (Dorairaju, 2021). Hence the need for urgent security consciousness in the operation of IoT in agriculture.

Vol. 10, No. 06; 2025

ISSN: 2456-3676

To ensure the security of sensitive information, farmers and technology providers must address concerns over data ownership, sharing, and access rights. This will help foster trust and compliance with data protection regulations. These research gaps motivate this study, which investigates and assesses potential vulnerabilities in IoT application layer protocols, particularly in the agricultural framework.

1..2 Aims and Objectives

Aim: This study aims to conduct a literature review to investigate vulnerabilities in IoT application layer protocols and develop a framework for vulnerability assessment.

Objectives:

1. To conduct a Literature Review of existing research on IoT application layer protocols in agriculture and their associated vulnerabilities.
2. To analyse and evaluate Vulnerability Data while utilising data from reviewed studies to identify common vulnerabilities and attack vectors.
3. To create a framework that incorporates findings from the literature review, utilising techniques for vulnerability detection and analysis.
4. Based on the framework, to suggest effective strategies to mitigate identified vulnerabilities in IoT application layer protocols in the agricultural sector.

1.3. Research Questions

1. How many existing research on IoT application layer protocols and their associated vulnerabilities are to be reviewed?
2. What common vulnerabilities and attack vectors in IoT application layer protocols can be identified from the reviewed studies?
3. How can a thorough framework be built to include the results of the literature review and vulnerability detection methods to improve the security of agricultural IoT applications?
4. Based on the framework, what efficient solutions may be suggested to reduce found vulnerabilities in IoT application layer protocols in the agricultural sector?

2. Method

2.0 Introduction

This section provides a detailed description of the methods adopted throughout the course of the research to accomplish the objectives of the study. It covers the research philosophy and approach, the research design, the systematic literature review (SLR) process used, the search strategy, criteria for study selection, data extraction procedures, quality evaluation, data synthesis, ethical considerations, and limitations.

The study is grounded in a pragmatic research philosophy that prioritises the practical usefulness of research outcomes and supports the combination of quantitative and qualitative evidence.

Vol. 10, No. 06; 2025

ISSN: 2456-3676

A systematic literature review is used as the primary research approach, complemented by a three-phase research design involving SLR, vulnerability simulation, and framework development.

2.1 Identify Subsections

The method section is organised into clearly labelled subsections that collectively describe how the study was conducted and how data were obtained, processed, and analysed.

- The research philosophy and methodology underpin the overall approach to investigating IoT application layer vulnerabilities.
- The search strategy, inclusion and exclusion criteria, and PRISMA flow describe how relevant studies were identified and selected.
- Data extraction, quality assessment, data synthesis, and analysis explain how evidence was systematically organised and interpreted.
- The research design outlines the three phases: systematic literature review, vulnerability simulation, and framework development.
- The ethical considerations and limitations clarify how integrity, transparency, and rigour were maintained, as well as constraints of the approach.

This structure ensures that the study can be understood, evaluated, and replicated by other researchers.

2.2 Participant Characteristics

Because this study is a systematic literature review rather than a human-subject experiment, the "participants" in this context are the research articles and studies included in the review.
The characteristics of included "participants" (studies) were defined as follows:

- Articles focusing on IoT application layer protocols.
- Studies addressing vulnerabilities in IoT systems or related attack vectors.
- Peer-reviewed journal or conference articles.
- Publications written in English.
- Articles proposing frameworks or methodologies for vulnerability assessment in IoT.
- Empirical studies providing sufficient methodological details.
- Publications from the last ten years (2015–2025).

The following types of studies were excluded:

- Articles focusing solely on non-application layer protocols.
- Studies addressing general cybersecurity without a specific focus on IoT.
- Non-peer-reviewed articles, editorials, and opinion pieces.
- Publications in languages other than English.
- Studies with insufficient methodological detail or unclear findings.
- Duplicate articles or multiple publications of the same study.

Vol. 10, No. 06; 2025

ISSN: 2456-3676

Screening was carried out at two levels:
(i) Initial screening based on titles and abstracts to remove clearly irrelevant papers, and
(ii) Full-text review of remaining articles to confirm that they met all inclusion criteria.

2.3 Sampling Procedures

The sampling procedures in this research refer to how the relevant studies were identified, screened, and selected for inclusion in the SLR.

2.3.1 Publication Database Sources

In order to ensure comprehensive coverage and minimise selection bias, multiple bibliographic databases were used. Relying on a single database in SLRs can miss important studies; therefore, more than one database is recommended for a true systematic review.

The following academic databases were selected based on their extensive coverage of computer science, cybersecurity, engineering technology, and information systems research:

- Scopus
- ACM Digital Library
- Wiley Online Library

These sources collectively provided a broad and multidisciplinary foundation for identifying literature on IoT application layer vulnerabilities and security frameworks.

2.3.2 Search Terms and Keywords

A structured search strategy was developed based on the research objectives and questions. The process followed recommendations for systematic searching by defining:

- Core concepts (e.g., vulnerabilities, IoT, application layer, attack vectors).
- Suitable databases.
- Well-organised search queries using combinations of keyword phrases and synonyms.

Search phrases were constructed and iteratively refined to maximise relevant retrieval while minimising noise. Examples of search strings (applied mainly in the TITLE-ABS-KEY fields) included:

- (vulnerabilities AND IoT AND application AND layer AND protocols)
- ("vulnerabilities" AND "IoT" AND "application layer")
- ("vulnerabilities" AND "IoT" AND "application layer protocol")
- ("attack vectors" AND "IoT" AND "application layer")
- ("attack vectors" AND "IoT" AND "application layer protocol")
- ("vulnerabilities" AND "attack vectors" AND "IoT" AND "application layer")

Boolean operators (AND, OR) were used to refine the search. The search criteria were gradually improved based on initial results to ensure that all relevant material was captured and aligned with the research objectives.

Vol. 10, No. 06; 2025

ISSN: 2456-3676

2.3.3 Inclusion and Exclusion Criteria

To guarantee that only pertinent and high-quality studies were incorporated in the systematic literature review, detailed inclusion and exclusion criteria were developed. Identified studies were screened based on their titles, abstracts, keywords, and full texts following these criteria (summarised conceptually in the PRISMA flow):

- **Inclusion criteria** focused on scope (IoT application layer), topic (vulnerabilities and assessment), empirical nature, timeframe, and language.
- **Exclusion criteria** filtered out irrelevant layers, general cybersecurity without IoT focus, non-peer-reviewed material, non-English publications, poor methodological clarity, and duplicates.

The selection procedure consisted of:

1. **Initial Screening:**
   Titles and abstracts were evaluated to determine if studies met the inclusion criteria (Carrera-Rivera et al., 2022).
2. **Full-Text Review:**
3. For studies passing the initial screen, the full text was obtained and evaluated in detail against the inclusion/exclusion criteria. Only those that satisfied all criteria and demonstrated sufficient methodological rigour were included in the final synthesis.

2.3.4 The PRISMA Flowchart

The study followed the PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) protocol to provide a transparent and systematic record of the literature selection process. The four main PRISMA stages used were:

1. **Identification:**
2. Records were identified using the formulated search keywords in the selected databases. The number of records from each database was recorded in an Excel file to support tracking and management throughout the review.
3. **Screening:**
4. Duplicate records were removed. Remaining titles and abstracts were screened to exclude clearly irrelevant studies.
5. **Eligibility:**
6. The full text of potentially relevant articles was reviewed in detail to confirm that they met the inclusion criteria and contained adequate methodological information. Articles that failed these checks or scored poorly in quality assessment were excluded.
7. **Inclusion:**
8. All articles that passed the previous stages were included in the final analysis and synthesis.

This process ensured a rigorous, transparent, and reproducible selection of studies.

Vol. 10, No. 06; 2025

ISSN: 2456-3676

2.3.5 Sample Size, Power, and Precision

In the context of this systematic review, "sample size" refers to the number of studies selected after the PRISMA process, rather than human participants. Although traditional power calculations are not applicable in the same way as in experimental designs, precision was supported by:

- Using multiple relevant databases.
- Applying clearly defined inclusion and exclusion criteria.
- Using a structured and iterative search strategy.
- Conducting quality assessment with a validated tool (JBI checklist).

These measures collectively enhance the reliability and robustness of the evidence base assembled.

2.3.6 Measures and Covariates

The "measures" in this study are the data items extracted from each included article. A standardised data extraction template was used to collect:

- Study code
- Authors and citation
- Year of publication
- Research objectives
- Key findings
- Limitations of the studies
- Identified vulnerabilities in IoT application layer protocols
- Methodologies used for vulnerability assessment
- Elements relevant to the development of a vulnerability assessment framework

This structured approach reduced bias and facilitated synthesis.

2.3.7 Research Design

The research design combines systematic literature review with experimental research in three primary phases:

Phase 1 – Systematic Literature Review (SLR):

Data from prior empirical work on IoT application layer vulnerabilities were collected and synthesised. This established the current state of knowledge, recurring vulnerabilities, emerging threats, and gaps in existing assessment methodologies (Ali et al., 2022; Coiduras-Sanagustín et al., 2024).

Phase 2 – Vulnerability Simulation:

Based on SLR findings, selected vulnerabilities were simulated in a controlled testbed environment. This experimental phase enabled deeper understanding of vulnerability

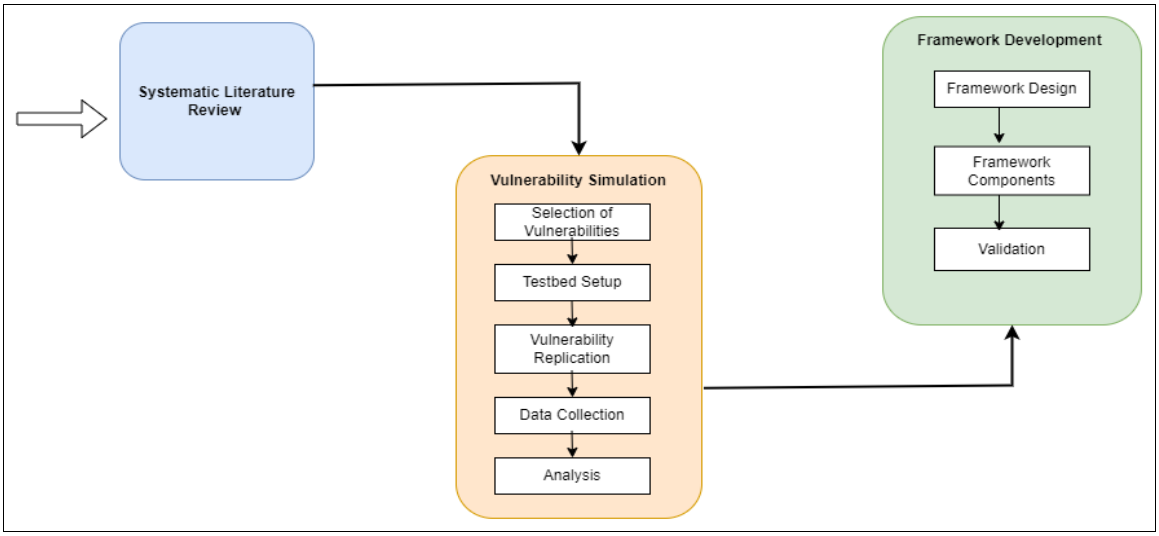
Vol. 10, No. 06; 2025

ISSN: 2456-3676

mechanisms, their exploitation, and impacts. It involved selecting vulnerabilities, configuring the testbed, replicating attacks, collecting data, and analysing the results.

Phase 3 – Framework Development:

Insights from both the SLR and simulation phases were integrated to develop a comprehensive framework for IoT application layer vulnerability assessment.
This design bridges the gap between theoretical understanding and practical implementation in IoT security.



2.3.8 Experimental Manipulations or Interventions

Although no human participants were involved, the study did employ experimental simulations of IoT application layer vulnerabilities as the equivalent of "interventions":

- Vulnerabilities identified in the SLR were selected and replicated in a controlled environment.
- A testbed was set up to simulate IoT systems and protocols.
- Attack vectors were executed against the testbed to observe behaviour, performance impact, and possible assessment points.

These manipulations enabled the researcher to observe how specific vulnerabilities manifest and how they can be systematically evaluated within the proposed framework.

Vol. 10, No. 06; 2025

ISSN: 2456-3676

2.4 Data Extraction

Data extraction involved systematically gathering relevant information from each included study (Carrera-Rivera et al., 2022). A standardised extraction form ensured consistency and completeness (Pollock et al., 2023). The form captured:

- bibliographic details,
- research aims,
- vulnerabilities considered,
- IoT protocols,
- assessment methods,
- reported findings,
- and study limitations.

The structured template also supported quality checks and minimised extraction errors.

Table 3.3. Data Extraction Template.

Study Code	Authors/ Citation	Year of publication	Research Objectives	Key Findings		Limitations of the studies
				Identified vulnerabilities in IoT application layer protocols	Methodologies for vulnerability assessment	
…	…	…	…	…	…	…

2.5 Quality Assessment

Quality assessment was conducted using the Joanna Briggs Institute (JBI) Critical Appraisal Checklist for Systematic Reviews and Research Syntheses (JBI, 2017). This tool, comprising 11 criteria, evaluates:

- clarity of review questions,
- appropriateness of search strategy,
- adequacy of inclusion criteria,
- rigour in study selection,
- quality of data extraction and synthesis,
- and transparency of reporting.

Each study was rated (Yes/No/Unclear/Not applicable), and only those that met a defined standard were included in the final synthesis. This ensured that the conclusions were based on methodologically robust evidence.

Vol. 10, No. 06; 2025

ISSN: 2456-3676

2.6 Research Data Synthesis

Data synthesis aimed to combine the results of multiple investigations to answer the research questions and build a comprehensive understanding of IoT application layer vulnerabilities and assessment frameworks. A narrative synthesis approach was used, complemented by thematic analysis (Ade-Ojo et al., 2022; Senneseth et al., 2022).
Key steps included:

1. Organising extracted data into categories (e.g., types of vulnerabilities, protocols, assessment methods, framework components).
2. Identifying patterns and relationships across studies, including recurring vulnerabilities, common weaknesses, and methodological trends.
3. Developing an initial synthesis describing these patterns and comparing consistencies and inconsistencies across studies.
4. Analysing connections across contexts and methods to understand the conditions under which certain vulnerabilities or frameworks are more or less effective.
5. Evaluating the strength and reliability of the synthesis by considering quality scores and performing sensitivity checks where necessary (Paul and Barari, 2022).

2.7 Data Analysis

The data analysis combined narrative synthesis, thematic analysis, and software-assisted analysis:

- **Narrative synthesis** provided an overarching summary of existing research on IoT application layer vulnerabilities, affected protocols, and mitigation methods.
- **Thematic analysis** identified recurring themes, patterns, and mechanisms contributing to vulnerabilities and influencing the effectiveness of assessment methods (Naeem et al., 2023).
- **Quantitative analysis** using **SPSS** allowed examination of trends, frequencies, and relationships in the extracted quantitative data (Sen and Yildirim, 2022).
- **Qualitative data analysis** using **MAXQDA** supported coding, organisation, and interpretation of textual data from the selected studies (Rädiker and Gizzi, 2024; Paulus, 2022).

These analytical strategies informed the design of the final vulnerability assessment framework.

2.8 Ethical Considerations

Ethics remained a critical component of the research process, even though the study focused primarily on existing literature and technical documentation. The following ethical principles guided the work:

- **Intellectual property rights:** all sources were properly cited and acknowledged (Khan et al., 2022).

Vol. 10, No. 06; 2025

ISSN: 2456-3676

- **Reproducibility and transparency:** search strategies, selection criteria, and extraction methods were documented to enable replication (Rethlefsen and Page, 2022).
- **Bias prevention:** pre-defined inclusion/exclusion criteria and structured quality assessment were used to minimise selection and interpretation bias (Taquette and Souza, 2022).
- **Responsible reporting:** results were reported comprehensively and accurately, including both strengths and limitations of the evidence.
- **Confidentiality:** any non-public technical documents or sensitive information encountered (e.g., in white papers) would be treated with strict confidentiality and not disclosed without proper authorisation.

2.9 Limitations

Although the methodology was carefully constructed to ensure rigour and completeness, several limitations must be acknowledged:

1. **Language bias:**
2. Restricting the review to English-language publications may have excluded relevant studies published in other languages, potentially narrowing the global perspective (Samer Mheissen et al., 2024).
3. **Publication bias:**
4. Systematic reviews are vulnerable to publication bias, as studies with significant or positive findings are more likely to be published. This may over-represent certain methods or outcomes (Afonso et al., 2023).
5. **Heterogeneity of primary studies:**
6. The wide range of IoT applications, protocols, and contexts can lead to substantial heterogeneity, limiting the ability to derive highly generalisable conclusions (Uttley et al., 2023).
7. **Subjectivity in data extraction and synthesis:**
8. Despite using structured tools and procedures, data extraction and synthesis inherently involve researcher judgement, which may subtly influence interpretation (Paul and Barari, 2022).

These limitations do not invalidate the study but should be considered when applying the findings in practice or in future research.

3. Results

3.0 Introduction

This section presents the results of the study in three main parts:
(1) findings from the systematic literature review (SLR) on IoT application-layer vulnerabilities,
(2) the simulation of a DDoS attack on an IoT environment, and
(3) the design and development of an IoT application-layer vulnerability assessment framework based on the SLR and simulation outcomes.

Vol. 10, No. 06; 2025

ISSN: 2456-3676

3.1 Systematic Literature Review Results

3.1.1 PRISMA Flow and Study Selection

The selection of studies for the SLR followed the PRISMA process, which comprises four phases: identification, screening, eligibility, and inclusion.
After applying the search strategy and inclusion/exclusion criteria across the three databases (Scopus, ACM Digital Library, and Wiley Online Library), the flow of records through each PRISMA stage was documented in a flow diagram (see *Figure 3.1*).

Following the full screening process, **18 studies** were finally judged to be sufficiently relevant and of adequate quality to be included in the SLR.

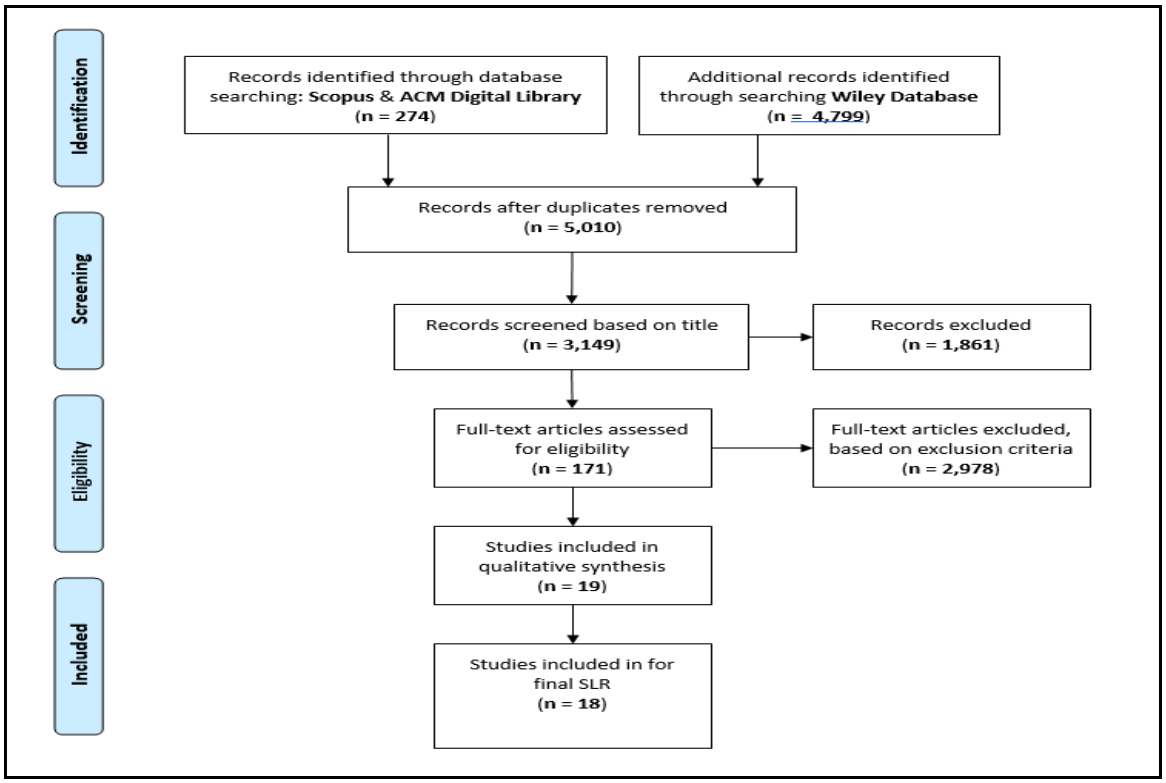


Figure 3.1. PRISMA flow diagram for SLR article selection (Source: Author).

3.1.2 Database Contributions

The 18 included articles were distributed across the three databases as follows:

- **Scopus** – 9 articles (50%)
- **ACM Digital Library** – 5 articles (28%)
- **Wiley Online Library** – 4 articles (22%)

Vol. 10, No. 06; 2025

ISSN: 2456-3676

This distribution is illustrated in *Figure 3.2* and shows that Scopus contributed the largest share of the included studies.

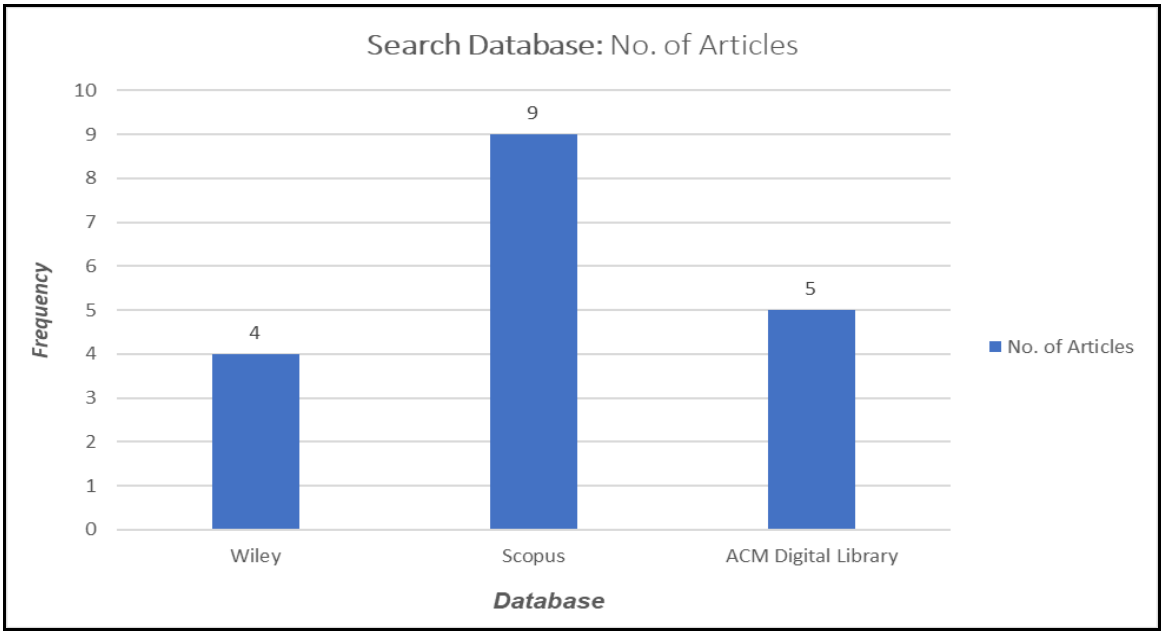


Figure 3.2. Number of included articles by database (Source: Author).

3.1.3 Publication Trend Over Time

The temporal distribution of the 18 included articles, over the period **2019–2024**, is shown in *Figure 3.3*. The trend can be summarised as:

- 2019 – 1 article
- 2020 – 4 articles
- 2021 – 0 articles
- 2022 – 5 articles
- 2023 – 4 articles
- 2024 – 4 articles

This pattern reflects growing research interest in IoT application-layer security, with a noticeable rise in the volume of publications from 2020 onwards.

Vol. 10, No. 06; 2025

ISSN: 2456-3676

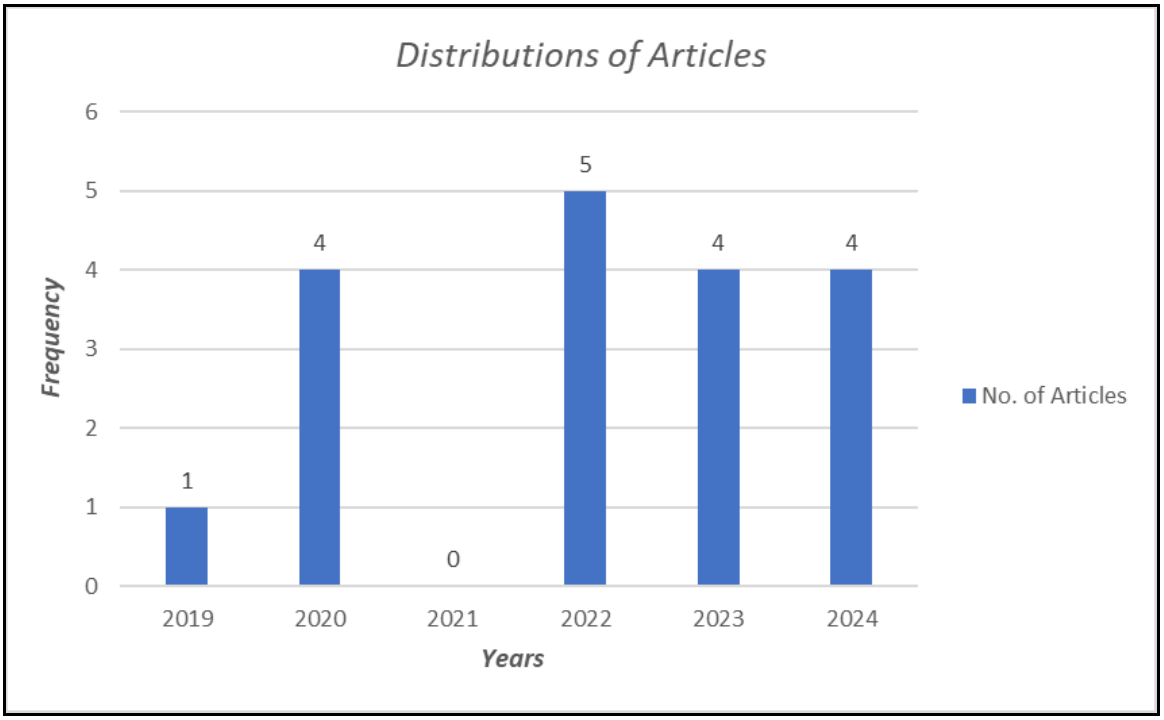


Figure 3.3. Yearly trend of included articles (Source: Author).

3.1.4 Quality Assessment of Selected Studies

The methodological quality of the included studies was assessed using the Joanna Briggs Institute (JBI) Critical Appraisal Checklist for Analytical Cross-Sectional Studies.

- Each study was evaluated against eight questions.
- A response of *"Yes"* was scored as 3, while *"No"*, *"Unclear"*, or *"Not applicable"* were scored as 0.

- Total scores were interpreted as:
- **≤ 4** – low quality
- **5–6** – moderate quality
- **≥ 7** – high quality

All 18 studies included in the final SLR achieved high-quality scores, with an average score of **7** or above. A summary of the JBI appraisal results is provided in *Table 3.1*.

Table 3.1. JBI Critical Appraisal scores for included studies (Source: Author).

		1	2	3	4	5	6	7	8	Overall	Weight	Appraisal
1	Abbasi et al., 2023	⊕	⊕	○	⊕	⊕	⊕	⊕	⊕	⊕	91.7	Included
2	Altulaihan et al., 2022	⊕	⊕	○	⊕	⊕	⊕	⊕	⊕	⊕	91.7	Included
3	Anand and Singh, 2023	⊕	⊕	○	⊕	⊕	⊕	⊕	⊕	⊕	91.7	Included
4	Aqeel et al., 2022	⊕	⊕	○	⊕	⊕	⊕	⊕	⊕	⊕	91.7	Included
5	Bharati and Podder, 2022	⊕	⊕	○	⊕	⊕	⊕	⊕	⊕	⊕	91.7	Included
6	Ferdows et al., 2020	⊕	⊕	○	⊕	⊕	⊕	⊕	⊕	⊕	91.7	Included
7	Kim and Park, 2023	⊕	⊕	○	⊕	⊕	⊕	⊕	⊕	⊕	91.7	Included
8	Lakshminarayana et al., 2024	⊕	⊕	○	⊕	⊕	⊕	⊕	⊕	⊕	91.7	Included
9	Lalit et al., 2022	⊕	⊕	○	⊕	⊕	⊕	⊕	⊕	⊕	91.7	Included
10	Narayanaswamy and Kumar, 2019	⊕	⊕	○	⊕	⊕	⊕	⊕	⊕	⊕	91.7	Included
11	Nebbione and Calzarossa, 2020	⊕	⊕	○	⊕	⊕	⊕	⊕	⊕	⊕	91.7	Included
12	Ozalp et al., 2022	⊕	⊕	○	⊕	⊕	⊕	⊕	⊕	⊕	91.7	Included
13	Pakmehr et al., 2024	⊕	⊕	○	⊕	⊕	⊕	⊕	⊕	⊕	91.7	Included
14	Patel et al., 2023	⊕	⊕	○	⊕	⊕	⊕	⊕	⊕	⊕	91.7	Included
15	Sharma and Bhushan, 2024	⊕	⊕	○	⊕	⊕	⊕	⊕	⊕	⊕	91.7	Included
16	Sredhar et al., 2024	⊕	⊕	○	⊕	⊕	⊕	⊕	⊕	⊕	91.7	Included
17	Srivastava et al., 2020	⊕	⊕	○	⊕	⊕	⊕	⊕	⊕	⊕	91.7	Included
18	Zhao et al., 2020	⊕	⊕	○	⊕	⊕	⊕	⊕	⊕	⊕	91.7	Included

Vol. 10, No. 06; 2025

ISSN: 2456-3676

3.1.5 Title Keyword Analysis

A word cloud was generated from the titles of the 18 selected studies to highlight frequently occurring terms. As shown in *Figure 3.4*, the most prominent keywords include:

- "IoT" – most frequent
- "application layer"
- "security"
- "DDoS"

These results confirm that the included studies strongly align with the focus on IoT application-layer security and related attack types.

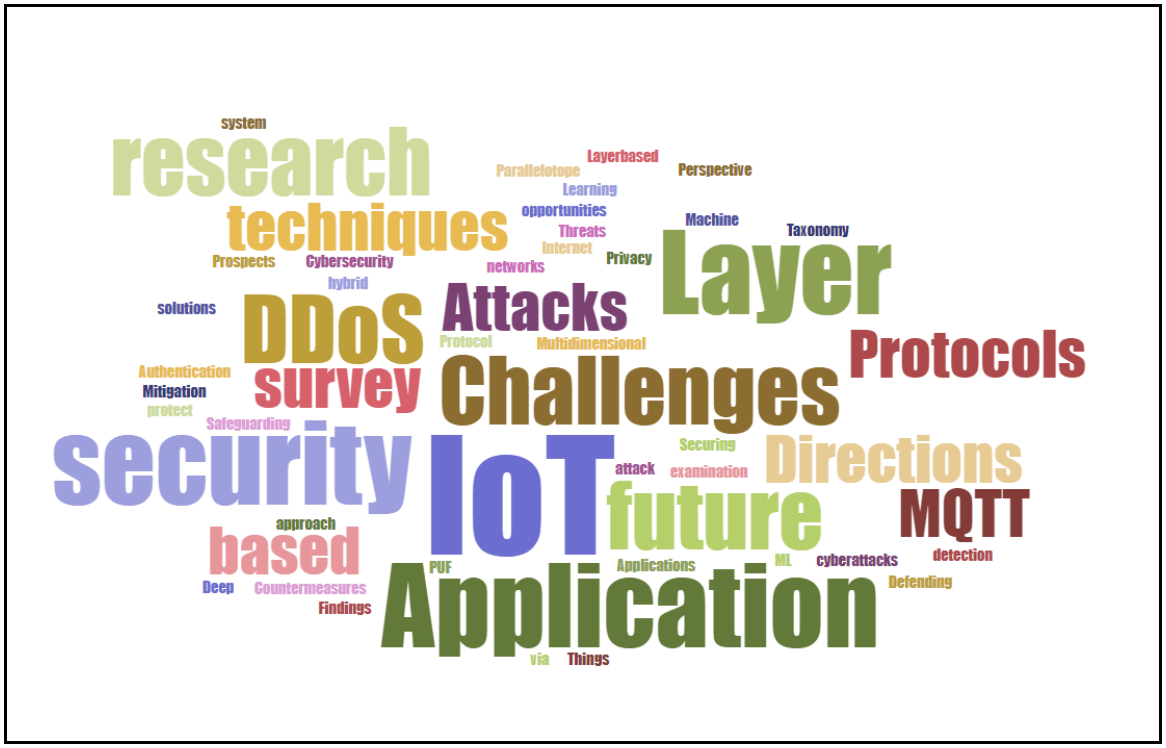


Figure 3.4. Word cloud of title keywords from included studies (Source: Author).

3.2 Vulnerability Analysis

A qualitative synthesis of the included studies was conducted to identify recurring IoT application-layer vulnerabilities and the methods used to assess or mitigate them. The results are summarised in the vulnerability synthesis table (*Table 3.2*), which captures:

- Study code and citation
- Year of publication
- Research objectives

Vol. 10, No. 06; 2025

ISSN: 2456-3676

- Key findings
- Identified vulnerabilities in IoT application-layer protocols
- Methodologies used for vulnerability assessment

Table 3.2. Qualitative synthesis of selected IoT application-layer vulnerability studies (Source: Author).

Vulnerability Type	Study Code
Botnet	[14], [17]
Ring of Death	[13]
UDP Fragmentation attack	[13]
TCP Flooding	[12], [13], [14]
Teardrop attack	[13]
Access Control, Node capturing	[7]
Radio interference	[4]
Trojan	[4], [6], [14]
Reprogramming, Malicious code injection	[2], [5], [7]
Denial of service (DoS)	[1], [2], [3], [5], [6], [8], [9], [10], [11], [12], [16]
Distributed Denial of Service (DDoS)	[2], [3], [5], [11], [12], [13], [14], [15], [17], [18].
Data Theft	[2], [5]
Sniffing, Eavesdropping	[2], [6], [7], [11], [15]
Phishing	[2], [10], [14]
Malware, Virus, Worms	[2], [4], [5], [6], [17]
Man-in-the-Middle (MiTM)	[1], [5], [8], [9]
Spoofing	[1], [9], [11]
Cross-site Scripting (XSS)	[2], [7]

Vol. 10, No. 06; 2025

ISSN: 2456-3676

3.2.1 Types of IoT Application-Layer Vulnerabilities

From the synthesis, multiple vulnerability types emerged across the application layer, including but not limited to:

- Botnet-based attacks
- Ring-of-Death attacks
- UDP fragmentation attacks
- TCP flooding
- Teardrop attacks
- Access control weaknesses and node capturing
- Radio interference
- Trojan attacks
- Reprogramming and malicious code injection
- Denial of Service (DoS)
- Distributed Denial of Service (DDoS)
- Data theft
- Sniffing and eavesdropping
- Phishing
- Malware, viruses, and worms
- Man-in-the-Middle (MitM) attacks
- Spoofing
- Cross-Site Scripting (XSS)

These vulnerability types and their associated studies are summarised in *Table 3.3*, which maps each vulnerability to the relevant study codes.

Study Code	Author(s)	Year	Research Objectives	Key Findings	
				Identified vulnerabilities in IoT application layer protocols	Methodologies for Vulnerability Assessment
[1]	Abbasi et al., 2023	2023	To determine the security prerequisites of the IoT application layer - Identify the security risks to the IoT application layer - Identify the current remedies to mitigate the security risks . - Identify unresolved problems and potential areas of further investigation in the	- Denial-of-Service (DoS) attacks (e.g., teardrop, LDoS, puppet, and smurf). - Man-in-the-middle attacks, - Spoofing attacks	The study is based on a three-layer IoT architecture as the reference model. It especially examines the application layer of this architecture. The study involves reviewing and analysing several IoT applications, such as smart grids, smart healthcare, ITS, smart agriculture, IIoT, and smart cities.

Vol. 10, No. 06; 2025

ISSN: 2456-3676

			security of the application layer in IoT.		
[2]	Altulaihan et al., 2022	2022	To categorise the threats associated with each layer of the IoT architecture, - To examine the latest strategies for mitigating IoT risks and discover prevalent approaches for safeguarding against cyberattacks on IoT devices	- Malicious code (e.g. SQL) injection - Cross-site scripting attack (XSS). - Data theft. - DoS and DDOS attack - Sniffing attack, and - Reprogramming attack. - Malware, phishing attacks.	A survey-based research study on the analysis of IoT cybersecurity threats
[3]	Anand and Singh, 2023	2023	To provide a thorough rundown of distributed denial of service (DDoS) attacks on Internet of Things (IoT) networks; Discuss the difficulties and security concerns with IoT networks.	- DOS attack. - DDoS attacks.	- By analysing the trend in Internet of Things security to find potential threats and challenges.
[4]	Aqeel et al., 2022	2022	The main purpose of this article is to examine the many forms of attacks that specifically target IoT devices. The primary objective is to comprehend the method by which these threats operate and provide a strategy for restoring the affected systems to their original state.	- Hardware Trojan - Radiofrequency interference attacks - Worms. - Viruses.	The research offers a comprehensive analysis of security risks and assaults on IoT systems, categorising them on a single platform. It aims to comprehend the level of harm caused by these threats and provide an explanation of their impact. This article examines the security concerns associated with the Internet of Things (IoT) and classifies and assesses them through comparative research. Furthermore, the research study suggests the implementation of cutting-edge technologies such

Vol. 10, No. 06; 2025

ISSN: 2456-3676

					as blockchain, machine learning, and artificial intelligence to ensure the security, privacy, and functionality of IoT systems.
[5]	Bharati and Podder, 2022	2022	This article provides a comprehensive review of machine learning systems and the latest advancements in deep learning approaches to boost the security of IoT devices.	- Man-in-the-middle (MiTM) attack - Malware. - Denial of service (DoS) - DDoS attacks (including SYN floods). - Data privacy attacks. - Malicious Code Injection Attacks.	The research thoroughly examines the techniques to protecting IoT using DL and ML, providing a detailed analysis of the benefits, possibilities, and weaknesses of each strategy. It also covers many potential problems and constraints. Additionally, the research includes future works, recommendations, and proposals for using DL/ML in IoT security.
[6]	Ferdows et al., 2020	2020	The objective of this research is to provide an understanding of the application layer. The primary focus of IoT technology is security, specifically addressing significant issues at the application layer. Insufficient security measures make IoT devices vulnerable to targeted attacks, resulting in damage to the user.	- Denial-of-Service (DoS) - Sniffing attack - Trojan horses. - Worms and viruses.	The report presents a comparative examination of the performance of application layer protocols. In addition, the article examines the architectural implementations and security features of several application-layer protocols being utilised in IoT technologies. It also addresses conventional solutions.
[7]	Kim and Park, 2023	2023	To overcome the shortcomings of static taint analysis, by integrating concolic execution with dynamic taint analysis in IoT web environment.	- Cross-Site Scripting (XSS) - Access control attack. - Malicious Code Injections. - Sniffin	Using Cross-Site Scripting (XSS) vulnerability detection, to propose a strategy to enhance security for IoT application layers while minimising the needed analysis time. - Implementing a system of automated tools that conduct concolic runs of dynamic taint analysis while minimising false alarms - Finding weak spots in IoT web apps and enabling automated tracking of inputs that cause XSS attacks.

Vol. 10, No. 06; 2025

ISSN: 2456-3676

[8]	Lakshminarayana et al., 2024	2024	This study examines the many threats targeting the IoT application, MQTT, protocol and the accompanying defence techniques designed for IoT deployments that rely on MQTT.	- DoS attack. - Man-in-the-middle (MiTM) attack.	An application layer (i.e., MQTT) protocol attacks are classified and examined based on essential attributes that facilitate understanding of their execution. The text provides a comprehensive analysis of defence mechanisms, specifically emphasising methods for discovering weaknesses and blocking attacks on the MQTT protocol.
[9]	Lalit et al., 2022	2022	This study seeks to analyse the multitude of security risks associated with application layer protocols and explore a variety of attacks that can target the application layer.	- DOS attacks, - Spoofing - Man-in-middle attacks	It surveyed and highlighted the several risks that might lead to significant problems when transmitting data from the application layer to the end user. While providing recommendations to inspire the development of more energy-efficient and safe methods for sharing data in the shortest possible time within an IoT environment.
[10]	Narayanaswamy and Kumar, 2019	2019	The key objective of the article is to emphasise the advantages of the current security authentication methods in the Internet of Things (IoT) that operate at the Application Layer (AL), while also acknowledging the limitations in terms of security and defensive measures.	- Phishing. - DoS.	The author provides users with adequate information to make an informed decision on the choice of protocol depending on the application. The study facilitates future researchers in doing a comparison examination of the performance of each AL protocol. It also encourages additional research on developing more effective defensive measures to address the security challenges in the IoT context. The study examines the architectural implementations, security features, and advantages and disadvantages of several AL protocols that are presently utilised in an IoT setting.
[11]	Nebbione and Calzarossa, 2020	2020	Examined the security threats and attacks that impact the application layer protocols of IoT devices. And evaluate the Common Vulnerabilities	- DoS - Distributed Denial of Service (DDoS). - Eavesdropping. - Spoofing.	An evaluation of the safety specifications of the application layer protocol standards, including a thorough examination of the Common Vulnerabilities and Exposures

			and Exposures (CVEs) that affect products and services using these protocols.		(CVEs) documented in the National Vulnerability Database from 2014 to the present, spanning a period of 6 years.
[12]	Ozalp et al., 2022	2022	This paper examines the notion of security in IoT devices by analysing the security needs and layer designs in the cloud layer, application layer, network layer, data layer, and physical layer of IoT devices.	- DDoS - TCP flooding	The analysis focuses on potential vulnerabilities and attacks against IoT devices, followed by a classification of IoT threats and an explanation of security needs based on several levels.
[13]	Pakmehr et al., 2024	2024	This article provides a thorough analysis of the impact of DDoS assaults on the Internet of Things (IoT), resulting in substantial damage to current infrastructure.	- HTTP/POST flood. - UDP fragmentation attack. - Teardrop attack. - Ping of death. - DDoS attacks.	The study explores several approaches to identify and mitigate this particular (DDoS) form of assault. Ultimately, this work proposes an extensive avenue of investigation in the realm of IoT security, specifically focused on analysing methods to adjust to existing obstacles and forecasting forthcoming patterns.
[14]	Patel et al., 2023	2023	1. Offering a comprehensive examination of Internet of Things (IoT) technologies and the communication protocols associated with them. 2. Categorising the IoT-layered architecture into perception, network, and application levels and examining security breaches linked to each tier. 3. Analysing IoT security solutions and identifying unresolved challenges and potential areas for further study in IoT networks.	- HTTP flooding. - Trojan horse. - DDoS. - Phishing attack. - Botnet	Analysed the security threats on IoT using the IoT-layered architecture. Exploration of security solutions and research difficulties in the field of Internet of Things (IoT)

Vol. 10, No. 06; 2025

ISSN: 2456-3676

[15]	Sharma and Bhushan, 2024	2024	To create a policy for authentication using PUF technology, developing an Intrusion Detection System (IDS) with the capability to promptly identify and counteract harmful network activity, as well as implementing measures to safeguard the IoT application layer protocol (MQTT) broker against Distributed Denial of Service (DDoS) assaults.	- DDoS attack. - Node capturing. - Eavesdropping.	A machine learning-powered Intrusion Detection System (IDS) that categorises incoming data as either malicious or non-malicious, while also monitoring and recording information on connected and authorised devices. And an authentication technique based on Physical Unclonable Functions (PUFs) that creates credentials (username and password) for end devices.
[16]	Sredhar et al., 2024	2024		- DoS - SYN Flood.	
[17]	Srivastava et al., 2020	2020	To understand the causes of vulnerabilities in IoT and provide a detailed discussion on IoT architecture and security challenges.	- Distributed denial-of-service (DDoS) attack. - Malware and SpytBots (e.g. Mirai, LUABOT, etc).	A survey-based research study on the analysis of IoT security threats and vulnerabilities.
[18]	Zhao et al., 2020	2020	The objective is to provide clear definitions for "attack utility" and "defence utility" and employ them as metrics for evaluating network security. Next, choose suitable metrics and do simulation tests to assess the effects of AL-DDoS assaults. Propose a computation model utilising hyperparallel principles to estimate the impact of AL-DDoS assaults and defence, and validate the precision of this model.	- Denial of Service (DDoS) attacks.	Provide a clear understanding of AL-DDoS attack and defence utility from both sociological and network perspectives. Additionally, it proposes the use of six metrics - network throughput rate, TCP data segment transmission rate, IP datagram transmission rate, transaction failure rate, average traffic arrival time, and server CPU utilisation - to assess the impact of AL-DDoS attacks. Providing a calculating model that utilises the notion of hyperparallel to create a multidimensional space for measuring the effectiveness of assault and defence strategies.

Vol. 10, No. 06; 2025

ISSN: 2456-3676

3.2.2 IoT Application Layer Vulnerability

Vulnerability Type	Study Code
Botnet	[14], [17]
Ring of Death	[13]

Table 3.3.1 Summary of identified IoT application-layer vulnerability types and supporting studies (Source: Author).

Vulnerability Type	Study Code
Botnet	[14], [17]
Ring of Death	[13]
UDP Fragmentation attack	[13]
TCP Flooding	[12], [13], [14]
Teardrop attack	[13]
Access Control, Node capturing	[7]
Radio interference	[4]
Trojan	[4], [6], [14]
Reprogramming, Malicious code injection	[2], [5], [7]
Denial of service (DoS)	[1], [2], [3], [5], [6], [8], [9], [10], [11], [12], [16]
Distributed Denial of Service (DDoS)	[2], [3], [5], [11], [12], [13], [14], [15], [17], [18].
Data Theft	[2], [5]
Sniffing, Eavesdropping	[2], [6], [7], [11], [15]
Phishing	[2], [10], [14]

Vol. 10, No. 06; 2025

ISSN: 2456-3676

Malware, Virus, Worms	[2], [4], [5], [6], [17]
Man-in-the-Middle (MiTM)	[1], [5], [8], [9]
Spoofing	[1], [9], [11]
Cross-site Scripting (XSS)	[2], [7]

A visual representation of the distribution and frequency of these vulnerabilities is provided in *Figure 3.5*.

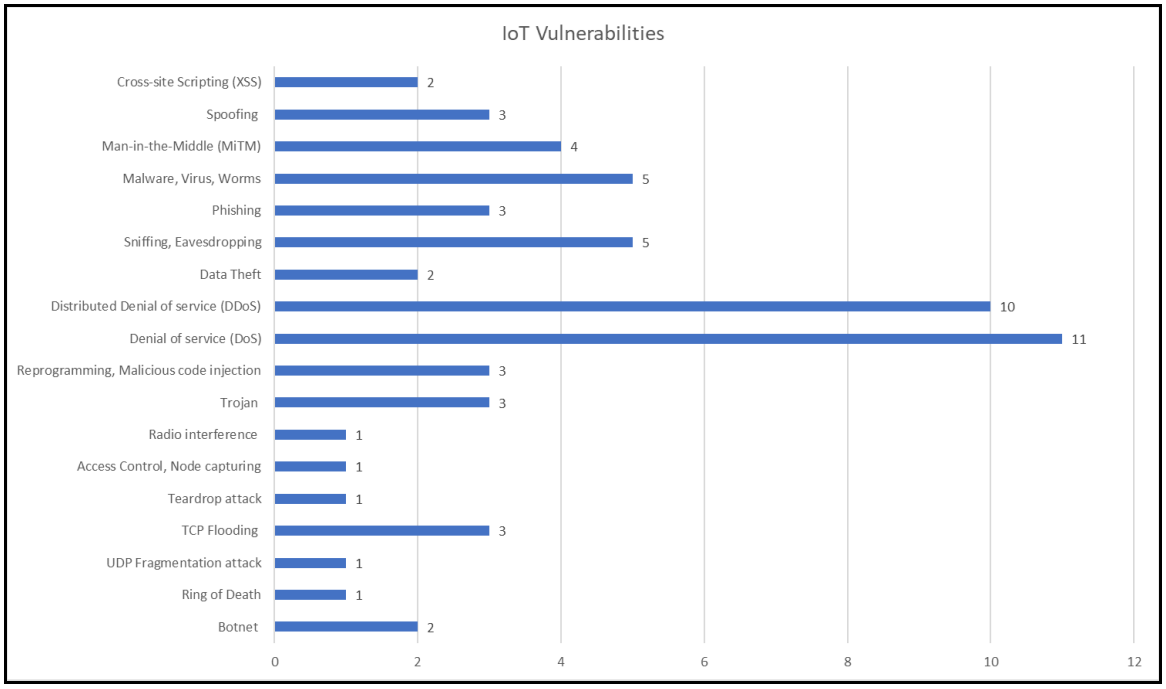


Figure 3.5. Application-layer vulnerability analysis (Source: Author).

The analysis shows that DoS and DDoS attacks are among the most frequently reported and widely studied threats, highlighting their critical importance in IoT application-layer security.

3.3 Simulation of DDoS Attack

Given the dominance of **DDoS-related vulnerabilities** in the SLR findings, a DDoS attack was selected for simulation in a controlled environment to better understand its behaviour and to inform framework design.

Vol. 10, No. 06; 2025

ISSN: 2456-3676

3.3.1 Simulation Setup

The simulation environment consisted of:

- A **target machine** running **Ubuntu OS**, representing the IoT server.
- A host machine running **Windows 11**, used to launch the attack.
- The **Low Orbit Ion Cannon (LOIC)** tool was built and executed using Visual Studio after temporarily disabling antivirus on the host system.

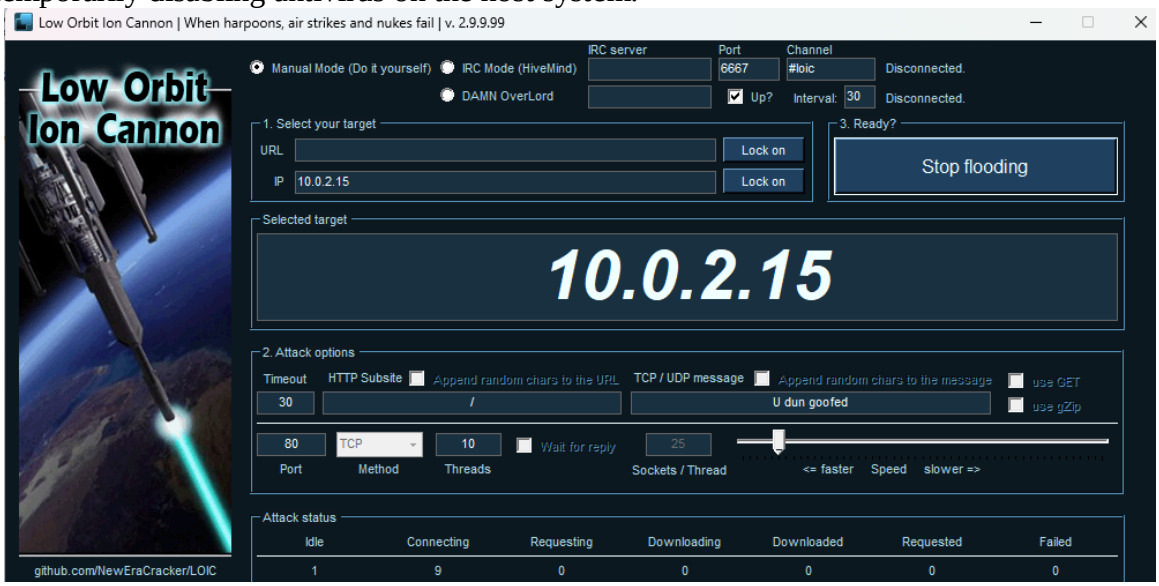


Figure 3.6a. LOIC setup and target configuration (Source: Author).

3.3.2 Monitoring the Attack

The DDoS attack traffic directed at the target machine was monitored using **Wireshark**. This allowed the inspection of network packets, detection of abnormal traffic patterns, and confirmation of the attack's impact prior to mitigation.

Vol. 10, No. 06; 2025

ISSN: 2456-3676

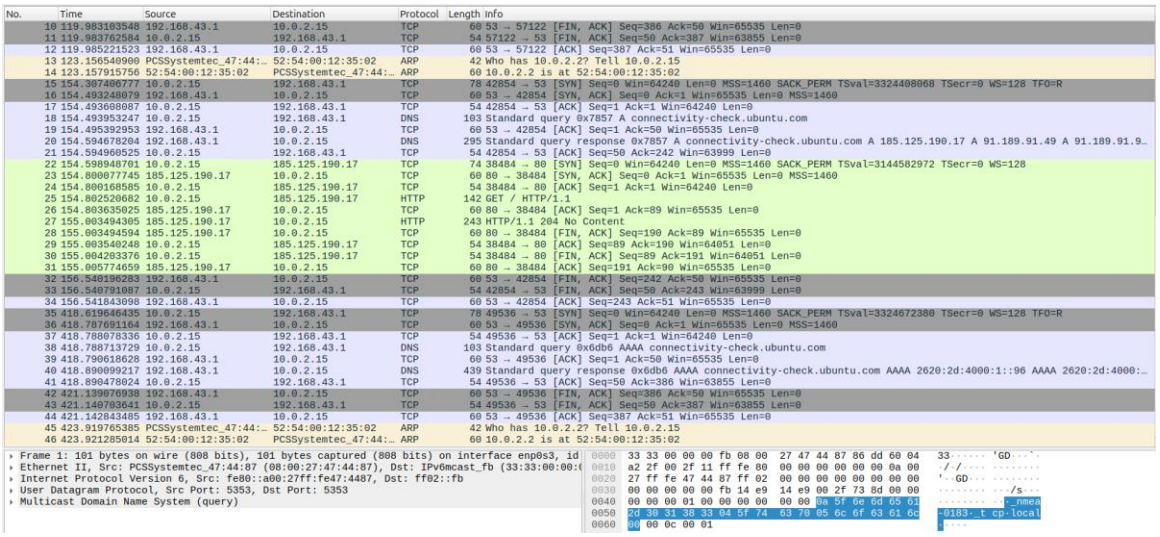


Figure 3.6b. Wireshark capture of network traffic during DDoS attack (Source: Author).

3.3.3 Mitigation

Mitigation was implemented by configuring **iptables** rules on the target machine to:

- limit the rate of incoming requests from the attacking host, and
- block or throttle malicious traffic originating from the attacker's IP (e.g., 10.0.2.15).

```
Chain INPUT (policy ACCEPT 11643 packets, 12M bytes)
num   pkts bytes target     prot opt in     out     source               destination
1        0     0 ACCEPT     6    --  *      *       0.0.0.0/0            0.0.0.0/0           tcp dpt:80 limit: avg 2/min burst 100
2        0     0 DROP       6    --  *      *       0.0.0.0/0            0.0.0.0/0           tcp dpt:80
3        0     0 LOG        6    --  *      *       0.0.0.0/0            0.0.0.0/0           tcp dpt:80 limit: avg 2/min burst 100 LOG flags 0 le
vel 4 prefix "DDos-Dropped:"
4        0     0 LOG        6    --  *      *       10.0.2.15            0.0.0.0/0           tcp dpt:80 limit: avg 2/min burst 100 LOG flags 0 le
vel 4 prefix "DDoS-Dropped: "
5        0     0 DROP       6    --  *      *       10.0.2.15            0.0.0.0/0           tcp dpt:80

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
num   pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
num   pkts bytes target     prot opt in     out     source               destination
```

Figure 3.6c. Example iptables configuration used to limit malicious requests (Source: Author).

The simulation demonstrated that simple yet carefully configured network-layer rules can significantly reduce the effectiveness of volumetric DDoS attacks at the application layer.

Although the experiment applied iptables for mitigation, this is consistent with industry recommendations for edge-level blocking in agricultural IoT deployments where resource-constrained devices cannot execute complex ML models locally (Mishra et al, 2025). The ML module therefore, acts as a decision engine to guide rule enforcement rather than replace existing network controls.

Vol. 10, No. 06; 2025

ISSN: 2456-3676

3.4 Design and Development of the IoT Vulnerability Assessment Framework

Based on the combined insights from the **SLR** and **DDoS simulation**, an IoT application-layer **vulnerability assessment framework** was designed. The aim of this framework is to systematically detect, classify, and mitigate application-layer attacks in IoT environments using machine learning.

The framework architecture is illustrated in *Figure 3.7* and comprises several interconnected components.

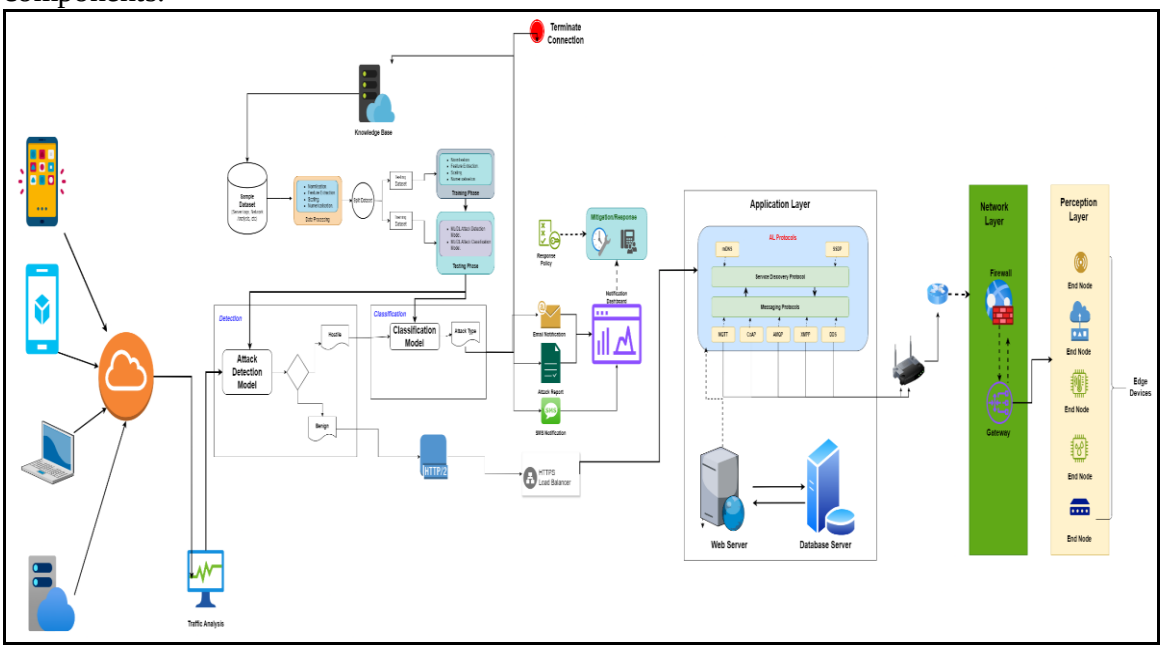


Figure 3.7. Proposed IoT application-layer vulnerability assessment framework (Source: Author).

3.4.1 Framework Overview

The framework is intended to:

- operate in heterogeneous IoT environments,
- monitor **application-layer traffic** in real time,
- detect and classify known and emerging attack types, and
- trigger suitable **mitigation and response** mechanisms.

It integrates traffic analysis, machine learning–based detection and classification, visualisation and reporting, a knowledge base, and response mechanisms, mapped onto the IoT perception–network–application architectural layers.

Vol. 10, No. 06; 2025

ISSN: 2456-3676

SLR findings confirmed that machine learning and deep learning approaches are particularly effective for building robust detection and assessment systems, which informed the design of the ML components in this framework.

3.4.2 Traffic Analysis

The **traffic analysis** module continuously monitors application-layer network traffic, extracting relevant features and behaviour patterns from incoming requests.
Its key functions include:

- real-time inspection of request flows,
- detection of anomalous or suspicious traffic,
- forwarding suspicious traffic to ML models for deeper analysis.

By integrating dynamic traffic analysis with machine learning, the framework supports **adaptive and near real-time threat detection** in IoT environments.

3.4.3 Machine Learning Models for Attack Detection and Classification

This part of the framework uses ML models tailored to IoT application-layer protocols to detect and classify attacks.

Note on Machine Learning Implementation

The machine learning component of the framework is designed as a conceptual and extensible module informed by existing datasets rather than a fully deployed classifier in this study. The purpose of this module is to demonstrate how detected IoT traffic can be processed for classification in real time. Although the current simulation validates traffic detection and mitigation using real network activity, the ML layer is proposed for future integration using publicly available IoT intrusion datasets such as CIC-IoT2023 and Bot-IoT, which contain application-layer traffic relevant to MQTT, CoAP and HTTP. This allows the framework to remain scalable and adaptable without requiring large, agriculture-specific datasets at this stage.

3.4.3.1 Data Processing

Raw traffic and attack-related data are subject to a data processing pipeline that includes:

- data cleaning,
- normalisation,
- feature extraction and selection.

The goal is to transform raw network/application requests into structured feature vectors suitable for ML model training and inference, ensuring that inputs are in appropriate formats and scales.

Vol. 10, No. 06; 2025

ISSN: 2456-3676

3.4.3.2 Attack Detection Model

The **attack detection model** operates as a first-layer filter that:
- analyses incoming application or network requests,
- identifies suspicious or anomalous behaviours, and
- forwards flagged instances to the more complex classification model.

This division of labour reduces computational overhead on the classifier, improves throughput, and lowers latency for real-time detection.

3.4.3.3 Classification Model

The **classification model** receives traffic flagged as suspicious and assigns it to specific attack categories (e.g., DoS/DDoS, phishing, spoofing, MitM, malware-based attacks).

By characterising threats more precisely, this model supports:
- more targeted mitigation strategies,
- better understanding of attack patterns, and
- improved situational awareness for security analysts.

In a full deployment, the classification stage can be implemented using supervised learning models such as Random Forest, XGBoost, or Deep Learning models such as CNN-LSTM, which have shown high accuracy (>96%) in IoT anomaly detection (Bharati & Podder, 2022; Sharma & Bhushan, 2024). These models are suitable due to their ability to distinguish subtle protocol-level behaviors in MQTT/HTTP/CoAP-based traffic without manual pattern engineering.

3.4.4 Visualisation and Reporting

The framework includes components for visualising attack-related data and generating reports. These outputs:
- provide security analysts with intuitive views of ongoing and historical attacks,
- highlight trends and patterns in detected threats, and
- improve interpretability of ML model decisions.

Combining advanced visualisation with ML results helps address the common challenge of explainability in AI-driven security systems.

3.4.5 Knowledge Base

The **knowledge base** stores:
- attack signatures and patterns,
- known vulnerabilities,
- protocol-specific weaknesses,
- historical incidents and their classifications.

Vol. 10, No. 06; 2025

ISSN: 2456-3676

It is used to:
- support ML model training and retraining,
- provide contextual information during classification,
- Keep the system up-to-date with evolving IoT threats.

Maintaining an up-to-date knowledge base is critical given the rapid evolution of IoT attack techniques.

3.4.6 Mitigation and Response

Based on the output of the classification model, the **mitigation and response** component initiates appropriate actions, such as:
- integration with **network controls** (e.g., firewalls, access control lists) to block or rate-limit malicious traffic,
- automatic termination of malicious requests before they reach critical application services,
- alert generation for administrators or security teams, and
- logging of incidents for further analysis and model improvement.

As represented in the framework, once a request is classified as malicious and logged in the knowledge base, it is blocked before accessing the IoT application layer, preventing successful intrusion.

3.4.7 Network Layer

In the framework, the **network layer** is responsible for the secure transmission of data between the perception and application layers. It includes:
- **Gateways**, which aggregate data from sensors and handle protocol conversion between local devices and central services.
- **Firewalls and routing devices**, which enforce security policies, control access, and filter unwanted traffic.

Only requests that have been analysed and classified as **benign** by the application-layer components are forwarded through the network layer towards edge devices, thereby reducing the risk of propagating attacks across the IoT infrastructure.

3.4.8 Perception Layer

The **perception layer** comprises the physical elements of the IoT environment that collect data from the real world, such as:
- **End nodes** (e.g., temperature sensors, soil moisture sensors, environmental monitors), and
- **Edge devices**, which perform initial processing and filtering close to the data source.

Vol. 10, No. 06; 2025

ISSN: 2456-3676

End nodes and edge devices together enable efficient and low-latency data acquisition and pre-processing. Within the framework, they receive only those requests that have been validated as harmless by the application and network layers, thereby enhancing overall system security.

4. Discussion

4.0 Introduction

This section presents the evaluation of the developed machine-learning-based IoT application-layer vulnerability assessment framework. The analysis includes (1) evaluation of the framework using simulated attack scenarios to demonstrate its detection and mitigation capabilities, and (2) a comparative analysis between the developed framework and the widely used National Institute of Standards and Technology Cybersecurity Framework (NIST CSF) to highlight strengths, weaknesses, and areas for improvement.

The goal is to demonstrate the practical effectiveness, adaptability, and relevance of the proposed framework within real IoT security contexts.

4.1 Framework Evaluation

The evaluation of the developed framework was conducted using controlled and simulated IoT attack scenarios. This allowed the assessment of the system's ability to:

- detect IoT application-layer threats in real time,
- classify attack types accurately, and
- mitigate malicious traffic through automated response actions.

4.1.1 Simulated Attack Scenario

To evaluate performance, the framework was tested against a simulated botnet-driven DDoS attack, which is one of the most frequently occurring IoT application-layer vulnerabilities identified in the SLR.

In this scenario, multiple compromised devices (e.g., PCs, mobile devices, servers) were coordinated to send spoofed and malicious requests to overwhelm an IoT web server at the application layer.

Vol. 10, No. 06; 2025

ISSN: 2456-3676

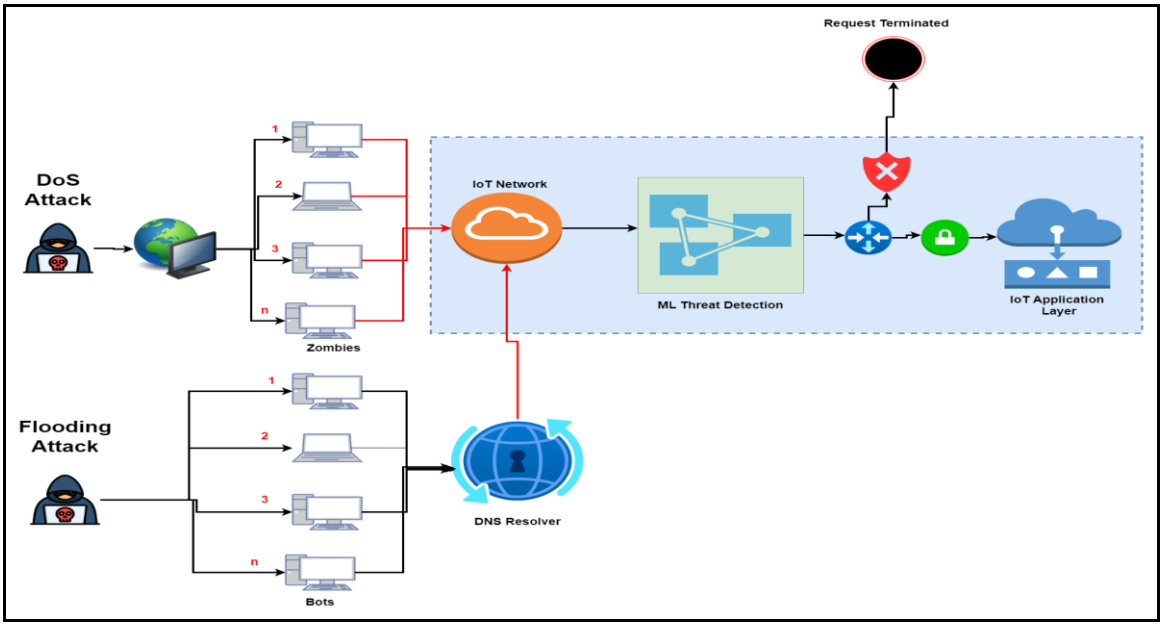


Figure 4.1. DoS and flooding attack simulations (Source: Author).

This simulation reflects an authentic threat commonly faced in IoT networks, where attackers leverage multiple compromised nodes to flood servers with requests, thereby causing service interruption or total system downtime.

4.1.2 Framework Activity and Response

The behaviour of the framework during the simulated attack scenario is summarised below:

1. Detection

The Attack Detection Model identified an abnormal and sudden increase in incoming traffic across multiple devices. The traffic analysis module flagged this as an anomaly indicative of a potential DDoS attack.

2. Classification

The Classification Model analysed the flagged traffic patterns using real-time and historical data. The model correctly identified the traffic as a DDoS attack, distinguishing it from normal traffic spikes that occur during legitimate usage.

3. Mitigation

The Response Policy component triggered automated defence actions by:

- instructing the Network Layer firewall to block traffic from identified malicious sources, and
- activating the Notification System to alert administrators in real time.

This ensured rapid containment of malicious traffic without requiring manual intervention.

Vol. 10, No. 06; 2025

ISSN: 2456-3676

4. Assessment

The evaluation demonstrated that:

- Machine learning significantly improved detection speed, enabling early awareness of suspicious behaviour.
- Automated classification reduced response latency, helping isolate compromised devices immediately.
- Firewall-based mitigation quickly suppressed harmful traffic before it impacted IoT services.
- The framework successfully reduced downtime and minimised damage, showing that automated ML-driven IoT protection is both effective and efficient.

4.2 Comparative Framework Analysis: NIST Cybersecurity Framework (NIST CSF)

The NIST CSF is a globally recognised cybersecurity framework used to guide organisations in managing and reducing cybersecurity risk. Although not originally designed for IoT, its principles apply across many digital environments and serve as a benchmark for evaluating new security frameworks.

Figure 4.2**.** NIST Cybersecurity Framework (NIST, 2024).

NIST CSF comprises five core functions:

1. **Identify** – Understand cybersecurity risks, assets, and vulnerabilities.
2. **Protect** – Deploy safeguards to ensure critical service delivery.
3. **Detect** – Implement mechanisms to identify cybersecurity incidents.
4. **Respond** – Take appropriate action to address detected incidents.
5. **Recover** – Restore systems or services impacted by a cybersecurity event.

Vol. 10, No. 06; 2025

ISSN: 2456-3676

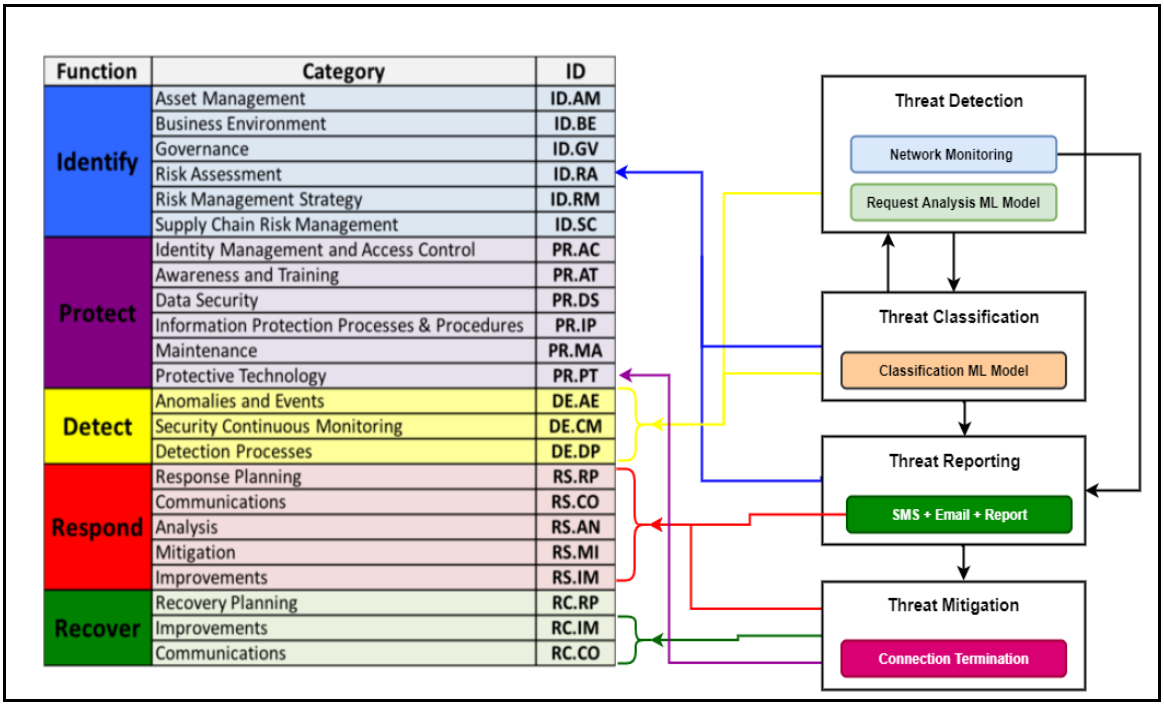


Figure 4.3. Comparison between NIST CSF and the Developed IoT Framework (Source: Author).

Although the NIST CSF is general-purpose, the comparison reveals strong conceptual alignment with the developed IoT-focused framework.

4.2.1 Comparative Analysis

1. Risk Management Focus

Both frameworks emphasise the identification and management of cybersecurity risks.

- The NIST CSF provides a structured organisational-level approach.
- The developed framework applies these principles specifically to IoT application-layer environments.

2. Incident Detection and Response

- The developed framework uses machine learning for real-time detection and classification of threats.
- The NIST CSF outlines high-level processes for detection and response.
- Both approaches aim to minimise the impact of cybersecurity incidents.

3. Continuous Improvement

- The developed framework adapts to new threats using ML-driven learning.
- NIST CSF encourages periodic reviews and updates of security practices.

Vol. 10, No. 06; 2025

ISSN: 2456-3676

- Both recognise that cybersecurity must evolve continuously.

4. Structured Approach
- NIST CSF is organised around five broad cybersecurity functions.
- The developed framework follows a structured process flow covering detection, classification, mitigation, and reporting.

Both emphasise systematic and repeatable procedures.

5. User Engagement and Communication

Both frameworks recognise the need for effective communication:
- The developed framework includes real-time alerts and actionable notifications.
- NIST CSF integrates communication within incident response and recovery phases.

4.2.2 Strengths of the Developed Framework

(i) IoT-Specific Focus

Unlike the general-purpose NIST CSF, the developed framework is tailored specifically to IoT ecosystems, addressing the unique vulnerabilities and protocol weaknesses of IoT application-layer communications.

(ii) Real-Time Processing

The framework's use of machine learning supports:
- real-time detection,
- high-speed data processing, and
- immediate threat response.

This is a major advantage over NIST CSF's conceptual guidance model.

(iii) Adaptability

The framework continuously improves by learning from newly observed threats and incorporating updated attack patterns within the Knowledge Base, enabling:
- adaptability to evolving IoT threats,
- compatibility with multiple application-layer protocols (e.g., MQTT, CoAP, mDNS).

NIST CSF, by contrast, requires manual updates.

(iv) User-Centric Notifications

The system provides instant alerts to administrators, fostering quick awareness and action.

NIST CSF recommends communication but does not specify real-time implementation mechanisms.

(v) Localised Edge Processing

By enabling local threat detection and mitigation at the edge, the framework:
- reduces latency,
- minimises bandwidth usage,

Vol. 10, No. 06; 2025

ISSN: 2456-3676

- improves responsiveness in IoT environments.

The NIST framework does not explicitly describe or mandate edge computing.

4.3 Summary and Implications

The developed IoT Vulnerability Assessment Framework demonstrates clear advantages over general-purpose cybersecurity models such as NIST CSF:

- Designed for IoT-specific vulnerabilities
- Strong ML-driven real-time detection and response
- Adaptable and scalable across IoT protocols and environments
- Provides fine-grained analysis of software, hardware, and application-layer threats
- Integrates monitoring, classification, knowledge management, and mitigation

However, the NIST CSF remains advantageous due to its:

- industry-wide adoption,
- regulatory recognition,
- and emphasis on governance and compliance.

The findings suggest that integrating elements of NIST CSF, such as implementation tiers and regulatory mapping-would strengthen future iterations of the proposed IoT framework.

4.4 Overall Discussion

The goal of this research was to examine IoT application-layer protocols and develop a comprehensive methodology capable of identifying and mitigating vulnerabilities, with a particular focus on agricultural IoT environments. Building on the findings of the systematic literature review (SLR), a machine-learning-based framework was designed, implemented, and evaluated. The outcomes of the study reveal key strengths and limitations of the framework and provide insights into its relevance for future IoT security practice.

4.4.1 Summary of Findings

The SLR revealed that IoT application-layer protocols suffer from multiple recurring vulnerabilities, including:

- Denial of Service (DoS)
- Distributed Denial of Service (DDoS)
- Man-in-the-Middle (MitM) attacks
- Malware, worms, and malicious script injections

The review further showed a lack of unified IoT security approaches, as most existing solutions were fragmented or protocol-specific.

These insights motivated the development of a real-time machine-learning-driven IoT security framework that can detect, classify, and mitigate IoT application-layer threats. The evaluation confirmed that the designed system successfully addresses common IoT attack types.

Vol. 10, No. 06; 2025

ISSN: 2456-3676

4.4.2 Framework Evaluation

The framework was evaluated using simulated IoT attack scenarios, including DoS, DDoS, and spoofing behaviour. The results showed the model's strong capability to:

- detect abnormal traffic patterns,
- classify threats accurately, and
- trigger immediate mitigation responses.

Strengths Identified

1. Real-Time Processing
2. The framework continuously analyses network traffic, identifying anomalies as they occur, which is vital given how quickly IoT attacks can propagate.
3. Adaptability
4. The machine learning models enable the system to learn from new threats, ensuring continued effectiveness as IoT security challenges evolve.
5. IoT-Specific Design
6. Unlike general cybersecurity tools such as the NIST CSF, the developed framework was designed specifically for IoT environments and application-layer vulnerabilities.

These strengths indicate that the framework provides a robust and future-oriented approach to IoT security.

4.4.3 Challenges and Areas for Improvement

Although the framework performed strongly, the evaluation revealed several challenges that must be addressed to enhance its usefulness:

1. Integration with Legacy IoT Systems

Older or low-resource IoT devices may not support the protocol features required for full deployment of the framework. This limits adoption in sectors such as agriculture, where legacy devices remain widespread.

2. Dependence on Large Datasets

The framework's performance relies heavily on the availability of large, high-quality datasets for training the machine learning models. In environments where data is scarce, performance may degrade, leading to false positives or missed threats.

3. Response Complexity

Although automated response is a strength, highly sensitive IoT environments may require context-sensitive or multi-step mitigation strategies rather than uniform blocking actions.

Vol. 10, No. 06; 2025

ISSN: 2456-3676

4. Continuous Knowledge Base Updating

IoT threat landscapes evolve quickly. The framework requires continuous updates to its knowledge base, an activity that can be resource-intensive and may require ongoing partnerships or automated threat intelligence pipelines.

Addressing these limitations is essential for ensuring the framework remains effective in real-world IoT settings.

Additionally, many existing agricultural IoT deployments use standard protocols such as MQTT, HTTP, and CoAP rather than agriculture-specific protocols. Therefore, this study focuses on widely adopted protocols first, with future work extending the framework to technologies such as LoRaWAN, SIGFOX, and sensor-specific payloads for soil telemetry.

4.5 Future Directions

Several opportunities exist for enhancing the framework:

1. Enhanced Integration with Legacy Systems
   Future versions of the framework should include lightweight or modular components compatible with older IoT devices.
2. Reducing Dataset Requirements
   Research into data-efficient ML models, semi-supervised learning, or transfer learning could reduce reliance on large labelled datasets.
3. Improving Automated Response Intelligence
   Next-generation versions should include context-aware responses that differentiate between attack severity, system type, and operational environment.
4. Automating Knowledge Base Updates
   Developing automated update pipelines or integrating external cybersecurity threat feeds will ensure the system remains aligned with emerging attack vectors.
5. Extensive Real-World Testing
   Pilot deployments in real agricultural IoT settings, industrial IoT networks, and smart city infrastructures will help validate performance and uncover additional areas for refinement.

These future directions will increase the system's robustness, adaptability, and suitability for broad IoT adoption.

References

Abbasi, M., Plaza, M. and Martín, Y. (2023). Security of IoT Application Layer: Requirements, Threats, and Solutions. pp.86–100. doi:https://doi.org/10.1007/9783031223563_9.

Abbasi, M., Plaza-Hernández, M. and Mezquita, Y. (2023). Security of IoT Application Layer: Requirements, Threats, and Solutions. *Lecture notes in networks and systems*, pp.86–100. doi:https://doi.org/10.1007/978-3-031-22356-3_9.

Ade-Ojo, G.O., Markowski, M., Essex, R., Stiell, M. and Jameson, J. (2022). A systematic scoping review and textual narrative synthesis of physical and mixed-reality simulation in

pre-service teacher training. *Journal of Computer Assisted Learning*. Doi:https://doi.org/10.1111/jcal.12653.

Afonso, J., Ramírez-Campillo, R., Filipe Manuel Clemente, Fionn Büttner and Andrade, R. (2023). The Perils of Misinterpreting and Misusing 'Publication Bias' in Meta-analyses: An Education Review on Funnel Plot-Based Methods. *Sports Medicine*. Doi:https://doi.org/10.1007/s40279-023-01927-9.

Ahmed, S. and Khan, M. (2023). Securing the Internet of Things (IoT): A Comprehensive Study on the Intersection of Cybersecurity, Privacy, and Connectivity in the IoT Ecosystem. *AI, IoT and the Fourth Industrial Revolution Review*, [online] 13(9), pp.1–17. Available at: https://scicadence.com/index.php/AI-IoT-REVIEW/article/view/13.

Ali, A., Mateen, A., Hanan, A. and Amin, F. (2022). Advanced Security Framework for Internet of Things (IoT). *Technologies*, 10(3), p.60. doi:https://doi.org/10.3390/technologies10030060.

Alkhafajee, A.R., Al-Muqarm, A.M.A., Alwan, A.H. and Mohammed, Z.R. (2021). *Security and Performance Analysis of MQTT Protocol with TLS in IoT Networks*. [online] IEEE Xplore. Doi:https://doi.org/10.1109/IICETA51758.2021.9717495.

Altulaihan, E., Almaiah, M.A. and Aljughaiman, A. (2022). Cybersecurity Threats, Countermeasures and Mitigation Techniques on the IoT: Future Research Directions. *Electronics*, [online] 11(20). doi:https://doi.org/10.3390/electronics11203330.

Anand, N. and Singh, K.J. (2023). A Comprehensive Study of DDoS Attacks on Internet of Things Networks. *Lecture notes in electrical engineering*, pp.573–586. doi:https://doi.org/10.1007/978-981-99-4713-3_56.

Anand, P., Singh, Y., Selwal, A., Alazab, M., Tanwar, S. and Kumar, N. (2020). IoT Vulnerability Assessment for Sustainable Computing: Threats, Current Solutions, and Open Challenges. *IEEE Access*, pp.1–1. doi:https://doi.org/10.1109/access.2020.3022842.

Aqeel, M., Ali, F., Iqbal, M.W., Rana, T.A., Arif, M. and Auwul, Md.R. (2022). A Review of Security and Privacy Concerns in the Internet of Things (IoT). *Journal of Sensors*, 2022, pp.1–20. doi:https://doi.org/10.1155/2022/5724168.

Arvind, S. and Narayanan, V.A. (2019). *An Overview of Security in CoAP: Attack and Analysis*. [online] IEEE Xplore. Doi:https://doi.org/10.1109/ICACCS.2019.8728533.

Aslan, Ö., Aktuğ, S.S., Ozkan-Okay, M., Yilmaz, A.A. and Akin, E. (2023). A Comprehensive Review of Cyber Security Vulnerabilities, Threats, Attacks, and Solutions. *Electronics*, [online] 12(6), pp.1–42. doi:https://doi.org/10.3390/electronics12061333.

Aufner, P. (2019). The IoT security gap: a look down into the valley between threat models and their implementation. *International Journal of Information Security*, 19(1), pp.3–14. doi:https://doi.org/10.1007/s10207-019-00445-y.

Bharati, S. and Podder, P. (2022). Machine and Deep Learning for IoT Security and Privacy: Applications, Challenges, and Future Directions. *Security and Communication Networks*, 2022, pp.1–41. doi:https://doi.org/10.1155/2022/8951961.

Bibi, N., Iqbal, F., Akhtar, S., Anwar, R. and Bibi, S. (2021). A Survey of Application Layer Protocols of Internet of Things. *IJCSNS International Journal of Computer Science and Network Security*, [online] 21(11). doi:https://doi.org/10.22937/IJCSNS.2021.21.11.41.

Bodeau, D., McCollum, C. and Fox, D. (2018). *Prepared for: Department of Homeland Security Cyber Threat Modeling: Survey, Assessment, and Representative Framework Authors*. [online] Available at: https://www.mitre.org/sites/default/files/2021-11/prs-18-1174-ngci-cyber-threat-modeling.pdf.

Carrera-Rivera, A., Ochoa, W., Larrinaga, F. and Lasa, G. (2022). How to Conduct a Systematic Literature review: a Quick Guide for Computer Science Research. *MethodsX*, [online] 9(1), p.101895. Available at: https://www.sciencedirect.com/science/article/pii/S2215016122002746.

Chae, C.-J., Kim, K.-B. and Cho, H.-J. (2017). A study on secure user authentication and authorization in OAuth protocol. *Cluster Computing*, 22(S1), pp.1991–1999. doi:https://doi.org/10.1007/s10586-017-1119-6.

Coiduras-Sanagustín, A., Manchado-Pérez, E. and César García-Hernández (2024). Understanding perspectives on personal data privacy in Internet of Things (IoT): A Systematic Literature Review (SLR). *Heliyon*, pp.e30357–e30357. Doi:https://doi.org/10.1016/j.heliyon.2024.e30357.

Dachyar, M., Zagloel, T.Y.M. and Saragih, L.R. (2019). Knowledge growth and development: internet of Things (IoT) research, 2006–2018. *Heliyon*, [online] 5(8), p.e02264. doi:https://doi.org/10.1016/j.heliyon.2019.e02264.

Demestichas, K., Peppes, N. and Alexakis, T. (2020). Survey on Security Threats in Agricultural IoT and Smart Farming. *Sensors*, 20(22), p.6458. doi:https://doi.org/10.3390/s20226458.

Dickson, K. and Yeung, C.A. (2022). PRISMA 2020 updated guideline. *British Dental Journal*, 232(11), pp.760–761. doi:https://doi.org/10.1038/s41415-022-4359-7.

Digvijaysinh, P. (2019). *CYBER SECURITY TECHNIQUES FOR INTERNET OF THINGS IN AGRICULTURE*. [online] Available at: https://www.researchgate.net/profile/Manoharsinh-Zala-2/publication/341868495_Impact_of_farm_technology_training_centre_on_knowledge_of_cucurbitaceous_growers/links/5ed76ed945851529452a70d7/Impact-of-farm-technology-training-centre-on-knowledge-of-cucurbitaceous-growers.pdf#page=97.

Dinculeană, D. and Cheng, X. (2019). Vulnerabilities and Limitations of MQTT Protocol Used between IoT Devices. *Applied Sciences*, 9(5), p.848. doi:https://doi.org/10.3390/app9050848.

Dorairaju, G. (2021). *Cyber Security in Modern Agriculture Case Study: IoT-based Insect Pest Trap System Technology Master's Degree Programme in Cyber Security*. [online] Available at: https://www.theseus.fi/bitstream/handle/10024/497436/Thesis_Dorairaju_Ganeas.pdf?sequence=2&isAllowed=y.

Elder-Vass, D. (2022). Pragmatism, critical realism and the study of value. *Journal of Critical Realism*, [online] 21(3), pp.1–27. doi:https://doi.org/10.1080/14767430.2022.2049088.

Vol. 10, No. 06; 2025

ISSN: 2456-3676

Fan, D., Breslin, D., Callahan, J.L. and Iszatt-White, M. (2022). Advancing literature review methodology through rigour, generativity, scope and transparency. *International Journal of Management Reviews*, 24(2). doi:https://doi.org/10.1111/ijmr.12291.

Farooq, M.S., Riaz, S., Abid, A., Abid, K. and Naeem, M.A. (2019a). A Survey on the Role of IoT in Agriculture for the Implementation of Smart Farming. *IEEE Access*, [online] 7, pp.156237–156271. doi:https://doi.org/10.1109/ACCESS.2019.2949703.

Farooq, M.S., Riaz, S., Abid, A., Abid, K. and Naeem, M.A. (2019b). A Survey on the Role of IoT in Agriculture for the Implementation of Smart Farming. *IEEE Access*, [online] 7, pp.156237–156271. doi:https://doi.org/10.1109/ACCESS.2019.2949703.

Farooq, M.S., Riaz, S., Abid, A., Umer, T. and Zikria, Y.B. (2020). Role of IoT Technology in Agriculture: a Systematic Literature Review. *Electronics*, [online] 9(2), p.319. doi:https://doi.org/10.3390/electronics9020319.

Ferdows, J., Mehedi, SK.T., Hossain, A.S.M.D., Mamun Shamim, A.A. and Islam Rasiq, G.M.R. (2020). A Comprehensive Study of IoT Application Layer Security Management. In: *2020 IEEE International Conference for Innovation in Technology (INOCON)*. Doi:https://doi.org/10.1109/inocon50539.2020.9298245.

Ferrag, M.A., Shu, L., Yang, X., Derhab, A. and Maglaras, L. (2020). Security and Privacy for Green IoT-based Agriculture: Review, Blockchain solutions, and Challenges. *IEEE Access*, pp.1–1. doi:https://doi.org/10.1109/access.2020.2973178.

Fikri, M.A., Putra, F.A., Suryanto, Y. and Ramli, K. (2019). Risk Assessment Using NIST SP 800-30 Revision 1 and ISO 27005 Combination Technique in Profit-Based Organization: Case Study of ZZZ Information System Application in ABC Agency. *Procedia Computer Science*, 161, pp.1206–1215. doi:https://doi.org/10.1016/j.procs.2019.11.234.

Gusenbauer, M. (2022). Search where you will find most: Comparing the disciplinary coverage of 56 bibliographic databases. *Scientometrics*, 127. doi:https://doi.org/10.1007/s11192-022-04289-7.

Harth, G., Hamid, Z. and Alisa, T. (n.d.). *Survey on IoT application layer protocols*. [online] Available at: https://www.researchgate.net/profile/Harth-Alneamy/publication/349716921_Survey_on_IoT_application_layer_protocols/links/603e4a59299bf1e0784f9d49/Survey-on-IoT-application-layer-protocols.pdf [Accessed Mar. 2021].

Ibrahim, H., Mostafa, N., Halawa, H., Elsalamouny, M., Daoud, R., Amer, H., Adel, Y., Shaarawi, A., Khattab, A. and ElSayed, H. (2019). A layered IoT architecture for greenhouse monitoring and remote control. *SN Applied Sciences*, 1(3). doi:https://doi.org/10.1007/s42452-019-0227-8.

Iqbal, W., Abbas, H., Daneshmand, M., Rauf, B. and Abbas, Y. (2020). An In-Depth Analysis of IoT Security Requirements, Challenges and their Countermeasures via Software Defined Security. *IEEE Internet of Things Journal*, 7(10), pp.1–1. doi:https://doi.org/10.1109/jiot.2020.2997651.

Isaac, J.O. (2021). *IOT - LIVESTOCK MONITORING AND MANAGEMENT SYSTEM*. [online] ijeast. Available at: https://ijeast.com/papers/254-257,Tesma509,IJEAST.pdf.

Vol. 10, No. 06; 2025

ISSN: 2456-3676

Jungell-Michelsson, J. and Heikkurinen, P. (2022). Sufficiency: A systematic literature review. *Ecological Economics*, 195, p.107380. doi:https://doi.org/10.1016/j.ecolecon.2022.107380.

Kambourakis, G., Kolias, C., Geneiatakis, D., Karopoulos, G., Makrakis, G.M. and Kounelis, I. (2020). A State-of-the-Art Review on the Security of Mainstream IoT Wireless PAN Protocol Stacks. *Symmetry*, 12(4), p.579. doi:https://doi.org/10.3390/sym12040579.

Kaur, K., Kaur, A., Yonis Gulzar and Gandhi, V. (2024). Unveiling the core of IoT: comprehensive review on data security challenges and mitigation strategies. *Frontiers in computer science*, 6. doi:https://doi.org/10.3389/fcomp.2024.1420680.

Kerzner, H. (2022). *Innovation Project Management: Methods, Case Studies, and Tools for Managing Innovation Projects*. *Google Books*. John Wiley & Sons.

Khan, A.A., Badshah, S., Liang, P., Waseem, M., Khan, B., Ahmad, A., Fahmideh, M., Niazi, M. and Akbar, M.A. (2022). Ethics of AI: A Systematic Literature Review of Principles and Challenges. *The International Conference on Evaluation and Assessment in Software Engineering 2022*. doi:https://doi.org/10.1145/3530019.3531329.

Khan, K.S. and Zamora, J. (2022). *Systematic Reviews to Support Evidence-Based Medicine*. Boca Raton: CRC Press. Doi:https://doi.org/10.1201/9781003220039.

Kim, J. and Park, J. (2023). Enhancing Security of Web-Based IoT Services via XSS Vulnerability Detection. *Sensors*, 23(23), pp.9407–9407. doi:https://doi.org/10.3390/s23239407.

Kristen, E., Kloibhofer, R., Díaz, V.H. and Castillejo, P. (2021). Security Assessment of Agriculture IoT (AIoT) Applications. *Applied Sciences*, 11(13), p.5841. doi:https://doi.org/10.3390/app11135841.

Kumar, L., Ahlawat, P., Rajput, P., Navsare, R.I. and Singh, P., Kumar (2021). *INTERNET OF THINGS (IOT) FOR SMART PRECISION FARMING AND AGRICULTURAL SYSTEMS PRODUCTIVITY: A REVIEW*. [online] IJEAST. Available at: https://www.ijeast.com/papers/141-146,Tesma509,IJEAST.pdf.

Lakshminarayana, S., Praseed, A. and Thilagam, P.S. (2024). Securing the IoT Application Layer from an MQTT Protocol Perspective: Challenges and Research Prospects. *IEEE Communications surveys and tutorials/IEEE communications surveys and tutorials*, pp.1–1. doi:https://doi.org/10.1109/comst.2024.3372630.

Lalit, M., Chawla, S.K., Rana, A.K., Nisar, K., Soomro, T.R. and Khan, M.A. (2022). IoT Networks: Security Vulnerabilities of Application Layer Protocols. In: *2022 14th International Conference on Mathematics, Actuarial Science, Computer Science and Statistics (MACS)*. IEEE Xplore, pp.1–5. doi:https://doi.org/10.1109/MACS56771.2022.10022971.

Liao, B., Ali, Y., Nazir, S., He, L. and Khan, H.U. (2020). Security Analysis of IoT Devices by Using Mobile Computing: A Systematic Literature Review. *IEEE Access*, 8, pp.120331–120350. doi:https://doi.org/10.1109/access.2020.3006358.

Maraveas, C., Piromalis, D., Arvanitis, K.G., Bartzanas, T. and Loukatos, D. (2022). Applications of IoT for optimized greenhouse environment and resources management.

Vol. 10, No. 06; 2025

ISSN: 2456-3676

Computers and Electronics in Agriculture, 198, p.106993. doi:https://doi.org/10.1016/j.compag.2022.106993.

McIntosh, T., Susnjak, T. and Liu, T. (2024). *From COBIT to ISO 42001: Evaluating cybersecurity frameworks for opportunities, risks, and regulatory compliance in commercializing large language models*. [online] Available at: https://www.sciencedirect.com/science/article/pii/S0167404824002694.

Mishra, S. R., Shanmugam, B., Yeo, K. C., & Thennadil, S. (2025). SDN-Enabled IoT Security Frameworks—A Review of Existing Challenges. Technologies, 13(3), 121. https://doi.org/10.3390/technologies13030121

Möller, D.P.F. (2023). NIST Cybersecurity Framework and MITRE Cybersecurity Criteria. *Advances in Information Security*, pp.231–271. doi:https://doi.org/10.1007/978-3-031-26845-8_5.

Morchid, A. (2023). Applications of internet of things (IoT) and sensor technology to increase food security and agricultural Sustainability: Benefits and challenges. *Ain Shams Engineering Journal*, [online] 15(3), p.102509. doi:https://doi.org/10.1016/j.asej.2023.102509.

Mouha, R.A. (2021). Internet of Things (IoT). *Journal of Data Analysis and Information Processing*, [online] 9(2), pp.77–101. doi:https://doi.org/10.4236/jdaip.2021.92006.

Mrabet, H., Belguith, S., Alhomoud, A. and Jemai, A. (2020). A Survey of IoT Security Based on a Layered Architecture of Sensing and Data Analysis. *Sensors*, 20(13), p.3625. doi:https://doi.org/10.3390/s20133625.

Mrutyunjay, P., Debapam, S., Raushan, K., Laxmi, N.S. and Avinash, K. (2024). *Enhancing precision agriculture: A comprehensive review of machine learning and AI vision applications in all-terrain vehicle for farm automation*. [online] Available at: https://doi.org/10.1016/j.atech.2024.100483.

Naeem, M., Ozuem, W., Howell, K.E. and Ranfagni, S. (2023). A step-by-step process of thematic analysis to develop a conceptual model in qualitative research. *International Journal of Qualitative Methods*, [online] 22(1), pp.1–18. doi:https://doi.org/10.1177/16094069231205789.

Narayanaswamy, S. and Kumar, A.V. (2019). Application Layer Security Authentication Protocols for the Internet of Things: A Survey. *Advances in Science, Technology and Engineering Systems Journal*, 4(1). doi:https://doi.org/10.25046/aj040131.

Nebbione, G. and Calzarossa, M.C. (2020). Security of IoT Application Layer Protocols: Challenges and Findings. *Future Internet*, 12(3), p.55. doi:https://doi.org/10.3390/fi12030055.

Nebbione, G. and Calzarossa, M.C. (2020a). Security of IoT Application Layer Protocols: Challenges and Findings. *Future Internet*, 12(3), p.55. doi:https://doi.org/10.3390/fi12030055.

Nebbione, G. and Calzarossa, M.C. (2020b). Security of IoT Application Layer Protocols: Challenges and Findings. *Future Internet*, 12(3), p.55. doi:https://doi.org/10.3390/fi12030055.

Vol. 10, No. 06; 2025

ISSN: 2456-3676

Olubiyi, O.A., Thomas, K.Y. and Kehinde, L.O. (2019). *Development of an MQTT-based IoT Architecture for Energy-Efficient and Low-Cost Applications*. [online] International Journal of Internet of Things. Available at: https://www.researchgate.net/profile/Olubiyi-Akintade/publication/333973074_Development_of_an_MQTT-based_IoT_Architecture_for_Energy-Efficient_and_Low-Cost_Applications/links/5d108f52a6fdcc2462a03a42/Development-of-an-MQTT-based-IoT-Architecture-for-Energy-Efficient-and-Low-Cost-Applications.pdf.

Omolara, A.E., Alabdulatif, A., Abiodun, O.I., Alawida, M., Alabdulatif, A., Alshoura, W.H. and Arshad, H. (2022). The internet of things security: A survey encompassing unexplored areas and new insights. *Computers & Security*, [online] 112, p.102494. doi:https://doi.org/10.1016/j.cose.2021.102494.

Ozalp, A.N., Albayrak, Z., Cakmak, M. and Ozdogan, E. (2022). Layer-based examination of cyber-attacks in IoT. In: *2022 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA)*. Doi:https://doi.org/10.1109/hora55278.2022.9800047.

Pakmehr, A., Aßmuth, A., Taheri, N. and Ghaffari, A. (2024). DDoS attack detection techniques in IoT networks: a survey. *Cluster Computing*. Doi:https://doi.org/10.1007/s10586-024-04662-6.

Patel, A., Patel, D., Kakkar, R., Oza, P., Agrawal, S., Tanwar, S., Sharma, R. and Nagendar Yamsani (2023). Safeguarding the IoT: Taxonomy, security solutions, and future research opportunities. *Security and Privacy*, 7(2). doi:https://doi.org/10.1002/spy2.354.

Paul, J. and Barari, M. (2022). Meta-analysis and Traditional Systematic Literature reviews-What, why, when, where, and how? *Psychology & Marketing*, 39(6), pp.1099–1115.

Paulus, T.M. (2022). Using Qualitative Data Analysis Software to Support Digital Research Workflows. *Human Resource Development Review*, 22(1), p.153448432211383. doi:https://doi.org/10.1177/15344843221138381.

Pendleton, A., Operations, G., Dill, R. and Pettit, D. (2019). *Surveying the Incorporation of IoT Devices into Cybersecurity Risk Management Frameworks*. [online] Available at: https://personales.upv.es/thinkmind/dl/conferences/securware/securware_2019/securware_2019_7_20_30043.pdf.

Pollock, D., Peters, M.D.J., Khalil, H., McInerney, P., Alexander, L., Tricco, A.C., Evans, C., de Moraes, É.B., Godfrey, C.M., Pieper, D., Saran, A., Stern, C. and Munn, Z. (2023). Recommendations for the extraction, analysis, and presentation of results in scoping reviews. *JBI Evidence Synthesis*, Publish Ahead of Print(3). doi:https://doi.org/10.11124/jbies-22-00123.

Quy, V.K., Hau, N.V., Anh, D.V., Quy, N.M., Ban, N.T., Lanza, S., Randazzo, G. and Muzirafuti, A. (2022). IoT-Enabled Smart Agriculture: Architecture, Applications, and Challenges. *Applied Sciences*, 12(7), p.3396. doi:https://doi.org/10.3390/app12073396.

Rädiker, S. and Gizzi, M.C. (2024). *The Practice of Qualitative Data Analysis: Research Examples Using MAXQDA, Volume 2*. *Google Books*. BoD – Books on Demand.

Vol. 10, No. 06; 2025

ISSN: 2456-3676

Rethlefsen, M.L. and Page, M.J. (2022). PRISMA 2020 and PRISMA-S: common questions on tracking records and the flow diagram. *Journal of the Medical Library Association*, [online] 110(2). doi:https://doi.org/10.5195/jmla.2022.1449.

Samer Mheissen, Spineli, L.M., Baraa Daraqel and Ahmad Saleem Alsafadi (2024). Language bias in orthodontic systematic reviews: A meta-epidemiological study. *PloS one*, 19(4), pp.e0300881–e0300881. doi:https://doi.org/10.1371/journal.pone.0300881.

Sauer, P.C. and Seuring, S. (2023). How to conduct systematic literature reviews in management research: a guide in 6 steps and 14 decisions. *How to conduct systematic literature reviews in management research: a guide in 6 steps and 14 decisions*, 17. doi:https://doi.org/10.1007/s11846-023-00668-3.

Schoonenboom, J. (2023). The Fundamental Difference Between Qualitative and Quantitative Data in Mixed Methods Research. *Forum Qualitative Sozialforschung / Forum: Qualitative Social Research*, [online] 24(1). doi:https://doi.org/10.17169/fqs-24.1.3986.

Sen, S. and Yildirim, I. (2022). A Tutorial on How to Conduct Meta-Analysis with IBM SPSS Statistics. *Psych*, [online] 4(4), pp.640–667. doi:https://doi.org/10.3390/psych4040049.

Senneseth, M., Pollak, C., Urheim, R., Logan, C. and Palmstierna, T. (2022). Personal recovery and its challenges in forensic mental health: systematic review and thematic synthesis of the qualitative literature. *BJPsych Open*, [online] 8(1). doi:https://doi.org/10.1192/bjo.2021.1068.

Shafi, U., Mumtaz, R., García-Nieto, J., Hassan, S.A., Zaidi, S.A.R. and Iqbal, N. (2019). Precision Agriculture Techniques and Practices: From Considerations to Applications. *Sensors (Basel, Switzerland)*, [online] 19(17), p.3796. doi:https://doi.org/10.3390/s19173796.

Shaheen, N., Shaheen, A., Ramadan, A., Hefnawy, M.T., Ramadan, A., Ibrahim, I., Hassanein, M., Ashour, M.E. and Flouty, O. (2023). Appraising Systematic reviews: a Comprehensive Guide to Ensuring Validity and Reliability. *Frontiers in Research Metrics and Analytics*, 8(8). doi:https://doi.org/10.3389/frma.2023.1268045.

Sharma, A. and Bhushan, K. (2024). A hybrid approach based on PUF and ML to protect an MQTT-based IoT system from DDoS attacks. *Cluster Computing*. Doi:https://doi.org/10.1007/s10586-024-04638-6.

Siwakoti, Y.R., Bhurtel, M., Rawat, D.B., Oest, A. and Johnson, R. (2023). Advances in IoT Security: Vulnerabilities, Enabled Criminal Services, Attacks and Countermeasures. *IEEE Internet of Things Journal*, [online] pp.1–1. doi:https://doi.org/10.1109/JIOT.2023.3252594.

Skinner, R.J., Nelson, R.R. and Chin, W. (2022). Synthesising Qualitative Evidence: A Roadmap for Information Systems Research. *Journal of the Association for Information Systems*, 23(3), pp.639–677. doi:https://doi.org/10.17705/1jais.00741.

Squires, V. (2023). Thematic Analysis. *Springer Texts in Education*, pp.463–468. doi:https://doi.org/10.1007/978-3-031-04394-9_72.

Sredhar, A., Khan, A., Gilal, A.R., Alsughayyir, A., Alshanqiti, A. and Talpur, B.A. (2024). Assessing and Mitigating Network Vulnerabilities in Philips Hue and Nest Protect Smart

Vol. 10, No. 06; 2025

ISSN: 2456-3676

Home Devices. *International Journal of Advanced Computer Science and Applications*, 15(2). doi:https://doi.org/10.14569/ijacsa.2024.0150202.

Srivastava, A., Gupta, S., Quamara, M., Chaudhary, P. and Aski, V.J. (2020). Future IoT-enabled threats and vulnerabilities: State of the art, challenges, and future prospects. *International Journal of Communication Systems*, 33(12), p.e4443. Doi:https://doi.org/10.1002/dac.4443.

Sudha, K.S. and Jeyanthi, N. (2021). A Review on Privacy Requirements and Application Layer Security in Internet of Things (IoT). *Cybernetics and Information Technologies*, 21(3), pp.50–72. doi:https://doi.org/10.2478/cait-2021-0029.

Syed, M. and McLean, K.C. (2023). Master narrative methodology: A primer for conducting structural-psychological research. *Cultural Diversity and Ethnic Minority Psychology*, 29(1). doi:https://doi.org/10.1037/cdp0000470.

Taherdoost, H. (2023). Security and Internet of Things: Benefits, Challenges, and Future Perspectives. *Electronics*, 12(8), p.1901. doi:https://doi.org/10.3390/electronics12081901.

Taquette, S.R. and Souza, L.M.B. da M. (2022). Ethical Dilemmas in Qualitative research: a Critical Literature Review. *International Journal of Qualitative Methods*, 21(21), pp.1–15. doi:https://doi.org/10.1177/16094069221078731.

Tournier, J., Lesueur, F., Mouël, F.L., Guyon, L. and Ben-Hassine, H. (2020). A survey of IoT protocols and their security issues through the lens of a generic IoT stack. *Internet of Things*, p.100264. doi:https://doi.org/10.1016/j.iot.2020.100264.

Uttley, L., Quintana, D.S., Montgomery, P., Carroll, C., Page, M.J., Falzon, L., Sutton, A. and Moher, D. (2023). The problems with systematic reviews: a living systematic review. *Journal of Clinical Epidemiology*, 156(5), pp.30–41. doi:https://doi.org/10.1016/j.jclinepi.2023.01.011.

Varsha, P.S., Chakraborty, A. and Kar, A.K. (2024). How to Undertake an Impactful Literature

Zhao, X., Peng, H., Li, X., Li, Y., Xue, J., Liang, Y. and Pei, M. (2020). Defending Application Layer DDoS Attacks via Multidimensional Parallelotope. *Security and Communication Networks*, 2020, pp.1–11. doi:https://doi.org/10.1155/2020/6679304.