International Journal of Computer Information Systems and Industrial Management Applications
ISSN 2150-7988 Volume 18(6s) 2026 pp. 88-100
https://doi.org/10.70917/ijcisim-2026-2870
Article

A Systematic Literature Review on IoT Cyber-Attacks During the COVID-19 Era: Taxonomy, Trends, and Mitigation Techniques

Ackmez Allamammaly

IT Analyst, Department of Information Technology, Mauritius Institute of Education (MIE), Reduit
Mauritius
Email Id: a.ackmez@mie.ac.mu
ORCID ID 0009-0004-8230-8603

Abstract: The COVID-19 outbreak has caused people to adopt IoT devices more than ever before, which has resulted in increased cyber attacks that target these devices throughout the world. The literature review studies academic research which evaluates the COVID-19 effects on IoT criminal activities during the period from 2018 to 2023. The research shows that cybercriminals attack IoT devices using specific methods and tools which they employ to launch their cyber attacks. The researchers applied the PRISMA approach to select academic papers which discussed how criminals used IoT technology to carry out COVID-19 related offenses. The research established a method to classify cybercriminals who execute disgraceful acts against IoT devices through their cyber operations. The COVID-19 period saw an upswing in ransomware attacks which involved phishers and botnets targeting both IoT and healthcare systems because too many IoT devices were deployed without proper security measures. The study results presented new methods which could help prevent IoT related crimes that resulted from the attack. The research team suggested using artificial intelligence to detect intrusions, blockchain technology for authentication, and edge computing as the most effective security solution for IoT devices. The research will help researchers and practitioners and policy makers to understand different cyber attack types which target IoT systems while they work to strengthen IoT device security.
Keywords: Cyber-Attacks; Systematic Literature Review; IoT Security; COVID-19

1. INTRODUCTION

Background of the Study

Over the last 10 years, there has been an enormous increase in the number of applications developed for the Internet of The Internet of Things (IoT) operates through interconnected devices that use the Internet to connect with each other. The quantity of devices that connect to the Internet reached 10 billion devices in 2021 which shows that Internet-connected devices experienced massive growth. The number of IoT applications will keep increasing because existing applications require development and technology continues to advance. The implementation of cloud computing and edge computing together with their corresponding technologies enables organizations to collect and analyze extensive data about ongoing activities at particular sites through AI-powered big data analytic tools which help organizations to achieve higher operational efficiency and make better business decisions (Gerodimos et al., 2023).

The COVID-19 pandemic brought about changes in how people used the Internet of Things (IoT).

The statement from this publication states that all advantages of IoT technology became apparent during the COVID 19 pandemic which occurred in the year 2020. Organizations need to develop agile response capabilities because COVID has shown how they must adapt to new operational situations that demand different customer interaction methods which result in different customer expectation patterns. Physical meetings and other in-person activities have decreased because people now conduct business through virtual methods which include video conferencing. All companies will prioritize employee health and safety as their main operational focus throughout their future business activities. The IoT enables businesses to achieve operational flexibility while sustaining their essential functions during emergency situations like the COVID 19 pandemic.

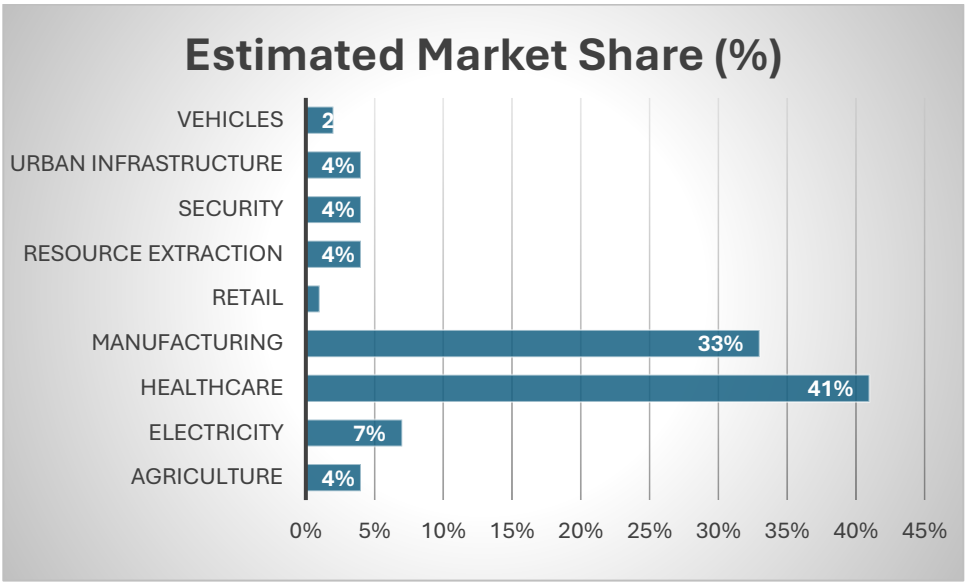

Figure 1. Market share estimated for the main application areas of IoT by 2025 (Gupta and Quamara, 2020).

The graph shows the projected market share for major IoT application sectors which will start operating in 2025. The healthcare sector will maintain its position as the leading market segment according to predictions which show that it will dominate most of the market share until 2025. The number of IoT devices that connect to the Internet has grown significantly together with the vast amounts of data that these devices generate since COVID-19 started (Saqib and Moon, 2023). The figure shows the global internet connections for IoT devices which will reach 2030 through its current total of billions.

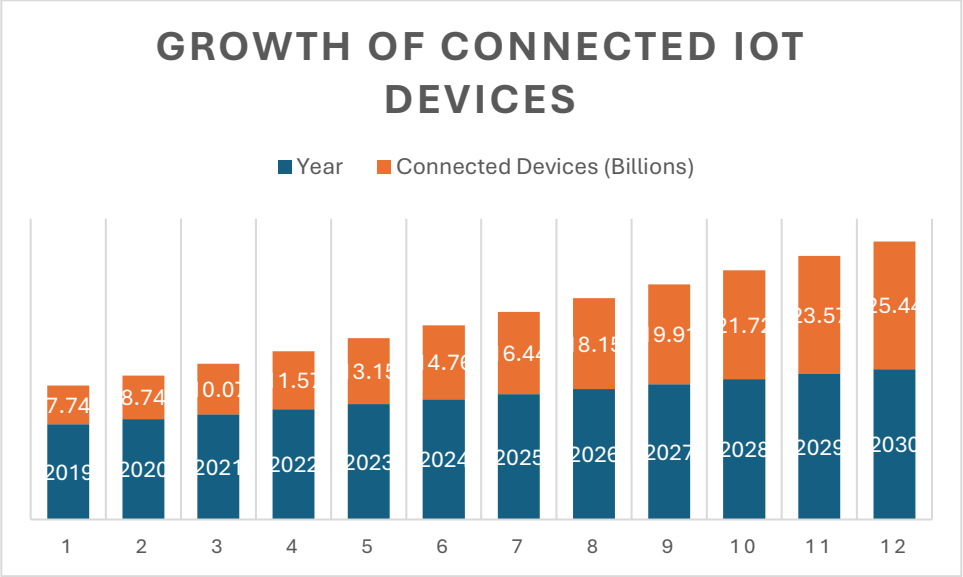

Figure 2. Global number of IoT connections to Internet are from 2019 to 2030. (Sulich et al., 2021).

People began using remote work and internet access during the COVID-19 pandemic because they wanted to stay home due to their stress and fear and their mistrust of others. The general public does not understand cybersecurity protection according to Ghadeer 2018. Cybercriminals have increased their operations by a significant degree according to Ahmed and Tushar 2020 and Sulich et al. 2021. The process of training people about cybersecurity needs to begin because it represents the most critical requirement for creating cybersecurity awareness according to Saleous et al. 2023.

The process of detecting and stopping cyber attacks gets improved through cybersecurity awareness programs. The program enhances how employees handle security matters. The security of systems and infrastructures receives stronger protection according to Corallo et al. 2022.

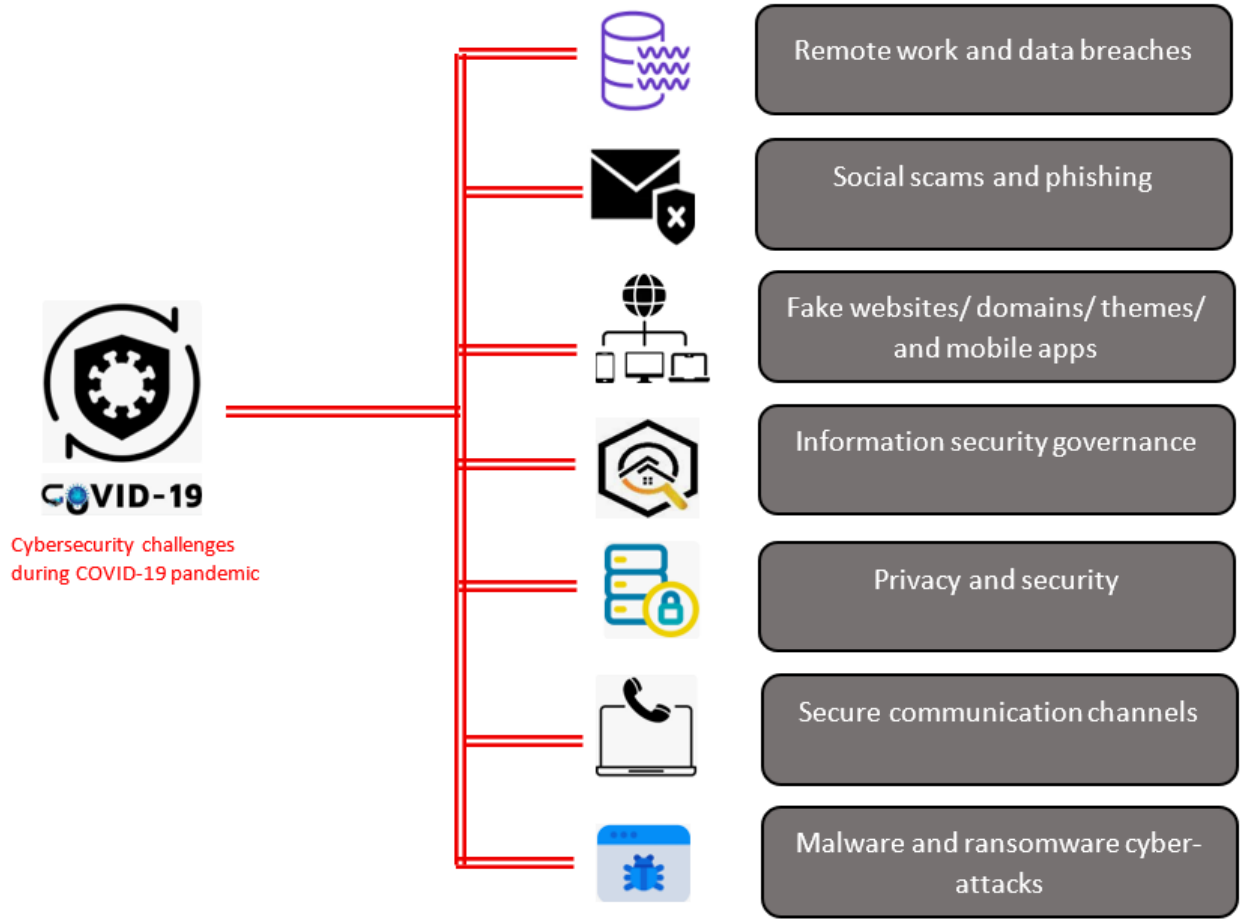

Figure 3. Global number of IoT connections to Internet are from 2019 to 2030. (Hijji and Alam, 2021).

The contests of cybersecurity have increased through two main factors which include the development of new attacks and protection methods and the effects of the COVID-19 pandemic (Saleous et al., 2023). The different cybersecurity challenges which arose during COVID-19 are shown in Figure 3. The main security problems which needed attention were social engineering attacks and data security and cyber-attacks according to the research conducted by Chen et al. in 2018. The number of cyber-attacks increased because people worked from their homes. The number of phishing attacks which use fake websites and mobile applications to steal user information has increased to dangerous levels.

Problem Statement

The current situation regarding IoT security problems creates serious threats because people now use IoT devices more than ever subsequently the outbreak of the COVID-19 pandemic (Khanam et al. 2020). The COVID-19 pandemic caused a twofold upsurge in IoT cyber-attacks because people began working from home and adopting video conferencing tools and online shopping and internet usage and wireless technology and digital entertainment and surveillance systems and e-learning and automation and touchless payment systems and social distancing and unemployment and cybersecurity ignorance and telemedicine and new human behavior patterns and remote data collection. Researchers have previously examined IoT cyber-attacks together with their defense methods but they did not carry out in-depth research about these topics during the COVID-19 pandemic. The need to study IoT cyber-attacks together with mitigation strategies which operate during COVID-19 period creates essential requirements for research. The researchers developed an IoT cyber-attack classification system with corresponding COVID-19 mitigation solutions as their primary research outcome.

Aim of the Review

This paper will identify, organise and evaluate all published research on both IoT-based Cyberattacks in relation to COVID-19 and create a clear classification of all the different Cyberattacks types associated with IoT during this period as well as identify trends that were observed and develop an understanding of what is being done to reduce or eliminate these types of attacks in a timely and comprehensive manner. The article presents research about how the Pandemic affected IoT systems and how this led to changes in Cybersecurity strategies.

Research Questions

RQ1: What methodologies are adopted for conducting SLRs in IoT cybersecurity?

RQ2: What general IoT cyber-attacks and mitigation techniques are documented?

RQ3: What IoT cyber-attacks occurred specifically during COVID-19?

RQ4: What mitigation strategies were proposed or adopted during COVID-19?

RQ5: How can these attacks and mitigation techniques be taxonomized?

2. LITERATURE REVIEW

The researchers presented information about different types of cyber threats and phishing attacks which occurred during the COVID-19 pandemic. The educational and healthcare and financial sectors which experienced the highest cyber threats during the COVID-19 pandemic received description. The researchers conducted discussions about cyber attack protection methods which included malware Distributed DoS hacking phishing and ransomware

The researchers of Alamoodi et al. 2020 studied COVID-19 which became a worldwide emergency during December 2019 when the new coronavirus SARS-CoV-2 first emerged in China. WHO announced that COVID-19 has resulted in millions of confirmed cases and hundreds of thousands of confirmed deaths throughout the world. Social media platforms have distributed multiple types of COVID-19 information which has created a vast collection of content that shows different viewpoints and emotions about various COVID-related incidents. The increasing amount of social media content and big data about COVID-19 allows computer scientists and researchers to study how people perceive social issues and current events which include the COVID pandemic. The analysis of that data will provide essential insights for our study.

Shammari et al. (2021) established through their research that during the COVID-19 pandemic most common cyber-attacks fell into three main categories. The researchers presented the top ten most common cybersecurity threats which existed at that time. According to Buzzio-Garcia (2021) multiple cyber threats showed increased activity. The researchers presented their control solutions after they had examined different types of cyber threats which had been mentioned before.

The research conducted by Lallie and his colleagues in 2021 demonstrated that cyber attacks impacted various countries according to their specific regional distribution. The study provided a list of forty-three cyber-attack instances along with their respective percentage distribution but it did not include a formal taxonomy of cyber-attack types or mitigation techniques or a comprehensive systematic literature review (SLR) with countermeasure methods. The research presentation lacks details about the attackers' operational methods which they employed for executing their assaults. The study by Hijji and Alam 2021 examined social engineering techniques which hackers used to attack organizations during the COVID-19 outbreak because it documented all research about the organizations which faced social engineering cyber-attacks. The study presented a complete list of all malicious software types that cybercriminals used to execute social engineering operations during the COVID-19 pandemic. The study proposes multiple solutions which include artificial intelligence and blockchain technology and cybersecurity training and Internet of Things (IoT) awareness programs and cyber resilience measures and big data analytics implementation. The research conducted by Saleous and his colleagues in 2023 created a cyber-attack taxonomy which categorized different cyber-attack types according to their targeted systems and operational platforms and available security defenses during the COVID-19 pandemic. The study provided details about the cyber-attacks which targeted various systems during the time of the COVID-19 pandemic. The study presented an overview of all cyber threats which occurred during COVID-19 together with the corresponding protective measures.

Faramarzi et al. (2024) conducted research which required researchers to search through three databases, PubMed, Scopus, and IEEE, from January 2020 until February 2023 while following PRISMA standards for systematic reviews and meta-analysis. The study selected 57 articles from a pool of 1576 articles which had received identification. The research examined 30% of the articles which used IoT technology for detection while 22% of the articles studied patient monitoring. The evaluation measured six different parameters which included Vital Signs and Diagnostic Imaging and History of Physical Complaint(s) and Laboratory Tests and Air Quality and Medical History. The Authors Bhattacharya & Singh (2025) examined a number of different dimensions of the public's experience with COVID-19. The COVID-19 pandemic created both a public health emergency and an infodemic which resulted in massive information overload through social media and other channels which spread dangerous and incorrect information.

The global infodemic created multiple public confusion which resulted in people losing trust for medical professionals who provided assistance and it disrupted all International public health operations. Researchers will discover better emergency management methods through their study of infodemic origin research which will help them control false information during future incidents. The systematic review followed PRISMA 2020 guidelines to conduct its research which used systematic database searches from PubMedScopusWeb of Science and Google Scholar until December 2024 to identify studies that met the selection criteria of COVID-19 disinformation which included its Causes and Dissemination and Impact and Countermeasures. The authors used thematic analysis to

retrieve, categorize, and synthesize data from 76 studies. The researchers used AMSTAR 2 Tool to assess study quality. Digital Media and Social Media together with psychological elements showed the highest level of false information about the topic. The results led to three main effects which included reduced public health rule adherence and increased vaccine refusal rates and decreased people trust in medical institutions. The results showed that fact-checking and digital literacy programs and AI-based moderation systems and reliable messengers had variable success rates because different cultural and situational factors affected their performance. The assessment determined that multiple techniques needed to be applied together to effectively handle misinformation problems. The effective solution required multiple methods which included both reactive and proactive and structural elements to be implemented. The review showed that scientific collaboration between different fields together with specialized social study methods showed essential value for conducting research work.

3. METHODOLOGY

SLR Design

The research uses a SLR framework which implements PRISMA as its preferred method for systematic review and meta-analysis reporting. PRISMA enables a transparent and replicable process for identifying relevant literature, screening studies, and reporting inclusion/exclusion decisions. The three-phase review process establishes this method for structural research paper evaluation which includes assessment of relevance and quality and thematic suitability.

Search Strategy

The research team implemented an all-embracing search method to obtain scholarly articles which they located in fundamental scientific databases that specialize in Internet of Things and cybersecurity and advanced technological studies. The following databases were selected: "IEEE Xplore ACM Digital Library SpringerLink Elsevier ScienceDirect MDPI". The researchers employed multiple keyword combinations with Boolean operators to achieve their maximum operational reach. The research team used core search terms which included IoT cyber-attacks Internet of Things security COVID-19 cybersecurity pandemic cyber-attacks IoT susceptibilities during COVID-19 IoT mitigation techniques and IoT pandemic threats. The research team established rules about what to include and what to exclude from their research work. The selection of papers for this SLR adhered to a systematic multi-phase screening approach to guarantee the inclusion of only high-quality, pertinent, and current research. The criteria were formulated according to the review objectives and corresponded with the screening methodology utilized in the study.

Inclusion Criteria

The study investigates IoT cyber-attacks and their associated vulnerabilities and intrusion detection systems and their methods for attack mitigation. The research examines IoT cyber-attacks that occurred during COVID-19 together with those which developed because of increased IoT use during the pandemic for remote work and healthcare IoT and smart surveillance and other applications. The study selected research articles which were published from 2018 until 2023 to examine current security practices that developed during the COVID-19 period. The research uses peer-reviewed sources which include journal articles and conference papers and systematic reviews and book chapters from established academic publishers like IEEE and ACM and Springer and Elsevier and MDPI. The study requires complete access to the English text because it needs full text for evaluation purposes.

Minimum Scientific Contribution: Studies presenting original findings, technical analysis, frameworks, datasets, or conceptual models relevant to IoT cybersecurity.

Exclusion Criteria

The research papers that study non-IoT fields and different attack methods and general networking security without IoT focus do not connect to IoT cybersecurity research. The studies that investigate IoT security problems during the pandemic period but do not establish any link to COVID-19. The category of non-peer-reviewed or informal publications includes magazines and news articles and blog posts and white papers and opinion essays and unpublished manuscripts. The study maintained COVID-19 contextual relevance by excluding all publications that existed between 2018 and 2023. The research excluded short papers that had less than 4 pages and studies that did not explain their methods and incomplete studies and papers that did not present data for analysis. The research found that the same study had been conducted multiple times through different versions and overlapping extended abstracts.

Three-Phase Screening Flow

The researchers used PRISMA guidelines to conduct their study selection process through three phases of screening which allowed them to find relevant studies in an unbiased manner. The first phase of the study determined which studies to include based on their relevance and quality and their compliance with the review criteria.

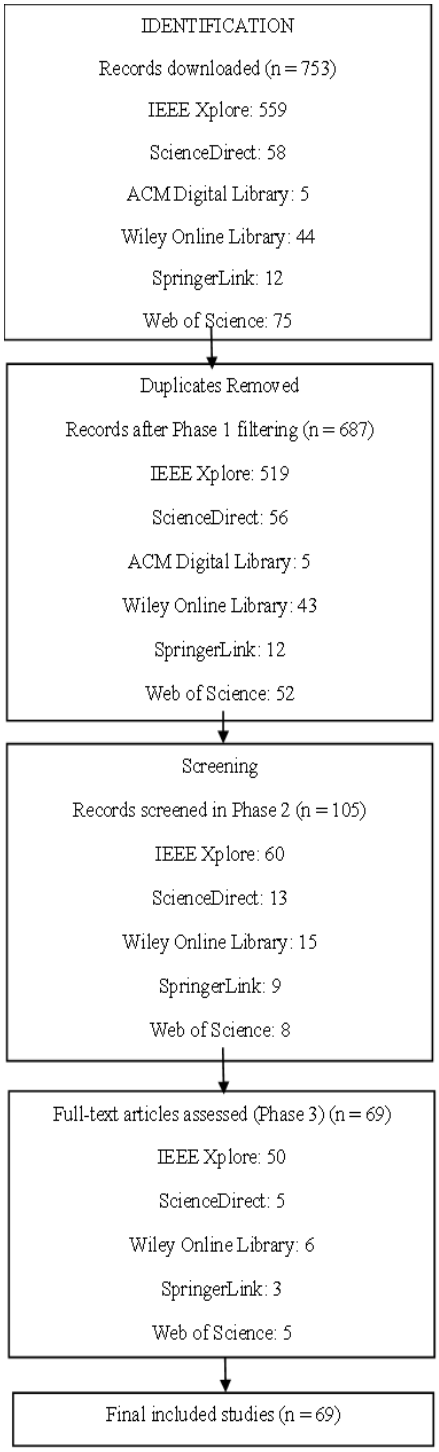

Figure 4. PRISMA Flowchart.

Phase 1: Identification

The researchers conducted an extensive database search which included IEEE Xplore ACM Digital Library SpringerLink Elsevier ScienceDirect and MDPI during their initial research period. The search applied Boolean operators together with keyword combinations which focused on IoT cyber-attacks and COVID-19 and IoT security.

The research process produced a vast number of academic studies which researchers used to create two different sets of criteria for their research. The system automatically identified duplicate records which it proceeded to delete from the database. The team excluded all non-research materials which included news articles blogs and editorials from the study.

Phase 2: Screening

The second phase entailed a comprehensive evaluation of titles and abstracts to ascertain if the research fulfilled the established inclusion criteria. Each record was scrutinized for:

Relevance to IoT security or cyber-attacks

Indications of COVID-19 context or pandemic-era digital transformation

Publication date within the 2018–2023 timeframe

Suitability for contributing to taxonomy development or trend analysis

Phase 3: Eligibility

In the final phase, the full text of each remaining study was thoroughly analysed. Evaluation criteria included:

Depth of IoT cyber-attack analysis

Clear methodological description and technical grounding

Inclusion of mitigation strategies or defensive frameworks

Explicit or indirect relevance to pandemic-induced IoT challenges

Overall academic rigor, clarity, and completeness

Quality Assessment

The research study used four essential criteria to assess research quality which proved both methodological strength and academic value. The first step of the study required researchers to measure clarity through their assessment of research objectives and problem statements and research methods which enabled them to interpret outcomes. The researchers assessed uniqueness to measure how much the study contributed fresh knowledge about IoT security, which included new attack methods and developing threat patterns and new COVID-19 pandemic security response strategies. The researchers assessed empirical grounding through their evaluation of evidence strength which included datasets and experiments and simulations and testbeds and real-world case studies that supported the proposed methodology and security assessments. The researchers assessed relevance through their examination of direct study connections to IoT cyber-attacks which occurred during the COVID-19 pandemic through study links to pandemic-related security vulnerabilities and the rise of IoT usage and the resulting changes in cyber threats. The research study established criteria which required only high-quality research that had major effects and relevant context to serve as the basis for the systematic review process.

Data Extraction

The study implemented an organized data extraction template which enabled researchers to collect and organize relevant data from their selected research studies. The publication required researchers to document essential information which included the specific IoT cyber-attack type that was studied and the IoT layer which was affected through different attack paths and methodologies. The extraction process also identified the pandemic relevance of each study, determining if attacks were linked to COVID-themed phishing operations, heightened remote access vulnerabilities, or the exploitation of healthcare IoT systems that proliferated during the pandemic. The documented mitigation strategies featured AI/ML-based intrusion detection systems, blockchain-enabled authentication, lightweight encryption methods, and policy frameworks which provided organizations with additional security solutions. The researchers compiled study results together with study limitations to create an in-depth analysis which demonstrated research contributions and methodological strengths and potential research weaknesses. The extraction process established uniformity between studies which allowed researchers to conduct meaningful comparisons between their results.

4. SYNTHESIS METHOD

The data which researchers collected from the investigation underwent processing through multiple analysis levels which worked to identify both patterns and trends together with the relationships between different components found in the academic sources. The research team used Internet of Things architecture levels to create three research categories which divided threats and mitigation methods into three groups according to perception, network, middleware, and application layer security. The secondary synthesis stage entailed thematic coding, which grouped cyber-attacks into classifications that included malware, ransomware, phishing, DDoS, spoofing, and other significant threat types identified during the COVID-19 period. The study compared attacker patterns from both pre-COVID-19 and COVID-19 periods to describe how attacker behavior changed together with the IoT threat landscape changes that occurred because of worldwide digital transformation. All information obtained from the research created an organized taxonomy which mapped specific attack types to their corresponding IoT layers together with main attack routes and necessary defense methods. The researchers used systematic data synthesis to construct a complete knowledge framework about IoT cyber-attacks during COVID-19 and all defensive methods which appeared in figure. 5.

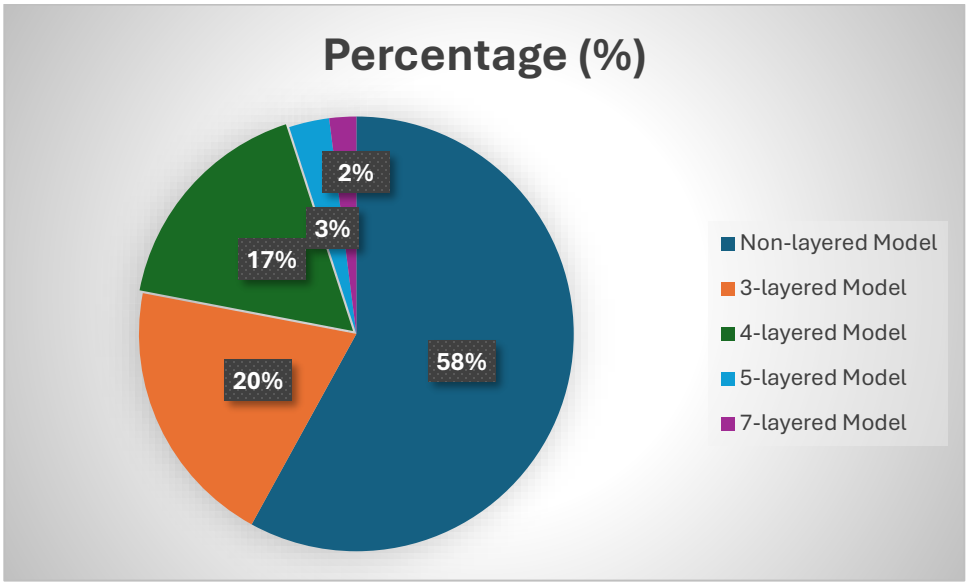

Figure 5. Percentage of IoT Architecture model retained research papers over the total papers in phase 3.

5. RESULT ANALYSIS

Overview of Selected Studies

The chosen research demonstrated a varied distribution across publishing years, geographical locations, and academic sources, highlighting the global significance of IoT cybersecurity throughout the COVID-19 era. The majority of publications emerged between 2020 and 2022, aligning with the zenith of the pandemic and the increase in IoT integration within healthcare, remote work, and intelligent infrastructure. Research contributions were predominantly centered in Asia, Europe, and North America, underscoring the extensive acknowledgment of IoT-related cyber dangers in technologically advanced and interconnected settings. The majority of the research featured were sourced from peer-reviewed publications and conferences published by IEEE, Springer, Elsevier, ACM, and MDPI, demonstrating significant academic involvement and methodological rigor. The distribution patterns correspond with the trends illustrated in Figures 6.

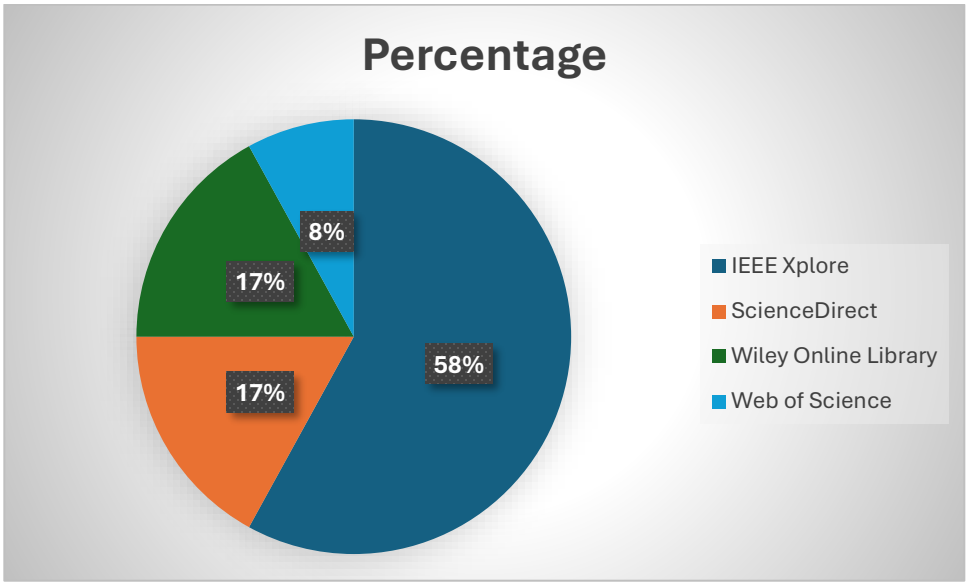

Figure 6. The research papers which belong to COVID-19 studies after phase three total twelve and the research papers which belong to this collection constitute a specific research paper percentage.

IoT Cyber-Attacks

The researchers in the study discovered IoT cyber-attacks which they classified through multiple architectural models to demonstrate the intricate structure of IoT systems. Previous research has categorized many forms of cyber assault according to their overarching category or description: malware, DoS, spoofing and brute-force attacks were categorized as they targeted devices without regard to the architectural segmentation of the device. The Three-Layer Model for Internet of Things (IoT) demonstrates how attacks on a particular layer lead to three cyber attack types

which target the perception layer and network layer & application layer. The perception layer contains attacks which include sensor manipulation through tampering and device capture through physical node capture and signal jamming. The network layer contains vulnerabilities which enable attackers to manipulate routing information and execute denial of service attacks through DDoS floods and conduct data flow attacks through man-in-the-middle techniques. The application layer suffers from the most significant numbers of cyber assault types which include ransomware attacks with encrypted payloads and malicious payloads which contain malware and hackers who restrict access to unauthorized areas and exploit application programming interfaces. The Four-Layer Model of Internet of Things (IoT) establishes processing and middleware as two additional operational components which introduce new potential security weaknesses. The Five-Layer Model of IoT business layer showed new threats that included Deception attack type which stole or hijacked account information and data breaches that compromised analytics through data integrity loss and unregulated data flows which violated privacy rights. A Seven-Layer Model of Internet of Things (IoT) provided deeper views of the attacks against device to device connectivity, aggregation of data, abstraction, application and cooperation layers. The more detailed attack classification system shows how multi-layer attacks operate because IoT systems function across various physical locations and multiple business processes which include device operations and network activities and cloud functions.

IoT Cyber-Attacks During COVID-19

The COVID-19 pandemic carried major variations to the IoT cyber-threat landscape according to the selected research and supporting evidence. The pandemic led to direct attacks which included COVID-themed phishing schemes that targeted IoT-connected networks and healthcare IoT systems which suffered ransomware attacks because of operational challenges. Perpetrators exploited public fear and false information together with rapid technological changes to access unprotected systems and steal medical records. People launched attacks through indirect connections after organizations began using IoT systems for their remote work requirements and their smart home systems and their systems designed to handle pandemic emergencies. The rapid growth of IoT devices has expanded attack possibilities which have led to more brute-force attacks and remote-access intrusions and botnet propagation and security issues from badly built or rapidly implemented IoT products. The results demonstrate that the pandemic caused dual effects because it directly enabled COVID-19 focused attacks while it created unsafe conditions through fast IoT deployment in important industries which is shown in figure 7.

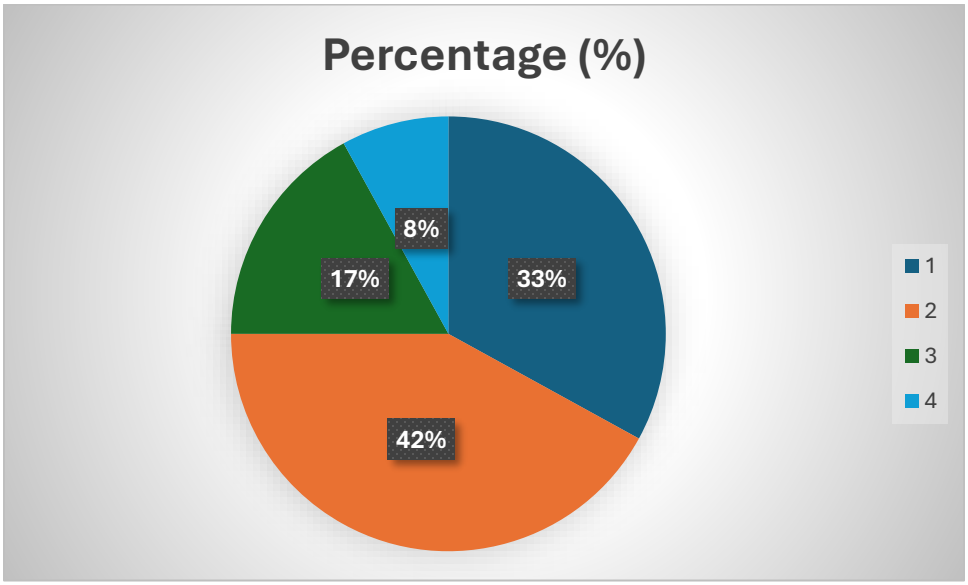

Figure 7. Percentage of research papers directly related to COVID-19 by year.

IoT Mitigation Strategies

The examined research papers proposed various methods of risk reduction which included advanced machine learning techniques, standard cybersecurity solutions, and new distributed system frameworks. Artificial Intelligence techniques have been successfully used to implement Deep Neural Networks (DNN) and Support Vector Machines (SVM) which analyze network traffic patterns and detect malware signatures and identify behavioral anomalies through their analysis. AI-powered systems develop new capabilities which enable them to handle emerging threats and increased traffic during worldwide pandemics. The system protects against all potential threats through its ability to discover system flaws and apply necessary updates while operating with standard Firewall and Access Control and Encryption and Secure Firmware installations and Machine Learning Techniques. Enterprises acquire additional advantages through their use of Blockchain technology which enables Decentralized Authentication beyond Internet requirements and delivers customers Immutable/Cryptographically Secure Data while Software-Defined Networking (SDN) enables real-time network management and local threat containment through Fog/Edge technology that

maintains extremely fast response times for local threat evaluations. All of these techniques and methods form a Cooperative Defense Layering method that will significantly reduce the overall threat of both Generic IoT Vulnerabilities, and the effects of Cybersecurity Risks associated with the Corona Virus Pandemics...

Taxonomy of IoT Cyber-Attacks and Mitigation During COVID-19

The review establishes a classification system for Cyber-Attack types which targeted IoT systems during the COVID-19 Pandemic according to figure 8. This helps researchers and practitioners understand the growing Cyber Threat Landscape because it functions as a valuable resource. The Taxonomy used additional data which the SLR study gathered to establish a system that enables Cyber-Attack classification through five criteria which include Attack type, IoT Layer attacked, Attack vector, Mitigation methodology used, and whether or not they are related specifically to COVID-19. The taxonomy groups cybersecurity incidents into two categories which include Direct Cyber-Attacks that target COVID-19 and Indirect Cyber-Attacks that occurred because of people using IoT devices while working from home. The Taxonomy categorizes the Cyber Criminals used to breach IoT devices during the pandemic which shows the best methods to minimize risks from these attacks and thus contributes to knowledge advancement in IoT security research.

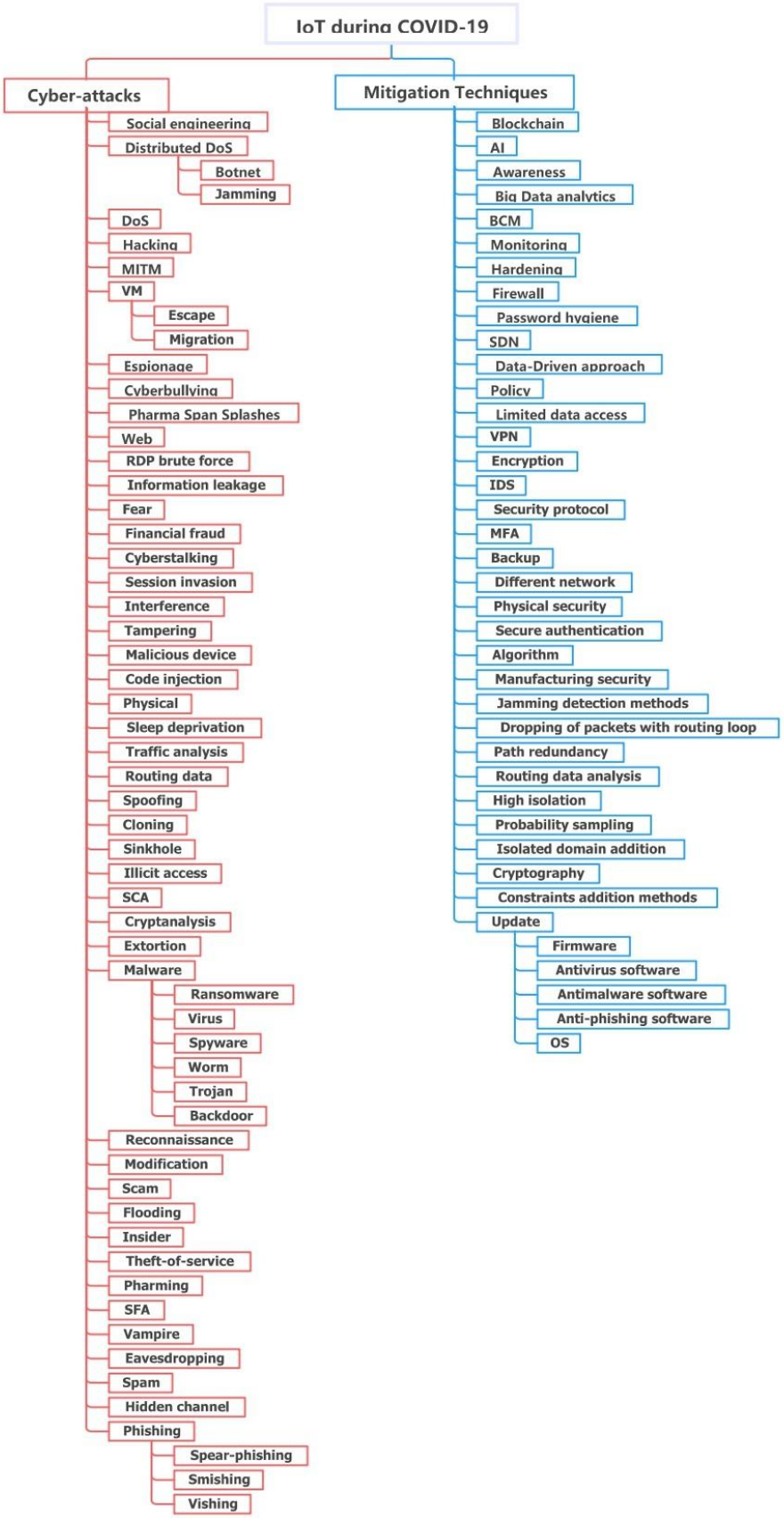

Figure 8. Taxonomy of IoT cyber-attacks during COVID-19 and mitigation techniques.

6. DISCUSSION

The document demonstrates how COVID-19 has impacted IoT Cyber Security because the pandemic created an environment which enabled cybercriminals to concentrate their attacks on healthcare organizations. Cyber Criminals now have more ways to attack healthcare IoT systems because Telehealth Remote Patient Monitoring and Integrated Health Networks have become more common. Cyber Criminals used the COVID-19 Cyber Attacks to create public anxiety and uncertainty which resulted in increased Phishing and Ransomware attacks that enabled them to breach IoT-connected home networks and other IoT devices. Cyber Attackers gained access to employee work and personal life through remote work because employees used weak passwords and unsecured home networks and unpatched IoT devices.

The Review establishes its main value through its capacity to unify multiple separate research projects about IoT security which researchers conducted during the COVID-19 pandemic to create a complete evaluation of how the pandemic transformed IoT security threats. Cyber Security Professionals will gain improved ability to detect and handle upcoming threats connected to IoT through the development of a new taxonomy which classifies IoT Cyber Attacks based on their attack Type Layer Vector Method of Mitigation and Relevance to COVID-19. The implications of this research extend to three distinct groups because researchers obtain specific guidance for their upcoming research efforts while practitioners obtain concrete recommendations to strengthen IoT system security and policymakers receive a reminder about the critical need for cybersecurity systems that can handle emergencies. The combined knowledge from these studies enables organizations to enhance their IoT protection systems against security threats which emerge during times of worldwide instability.

7. CONCLUSION

As evident from IoT security issues throughout the covid19 pandemic, Internet of Things vulnerabilities rose because of new technological developments which made IoT systems more susceptible to cyberattacks. The covid19 pandemic introduced different security threats which originated from hospital environments and worldwide workforce operations because people worked under pressure to complete tasks while hospitals experienced increased digital system changes that would have normally occurred six to twelve months later.

The developing threat patterns required a taxonomy that IOT Cyber Security uses to predict future cyber threats which IOT technologies will create. The organization needs to choose its proper protective measures which include traditional encryption and AI-based defence systems and blockchain-based trust systems. IOT solutions need to deliver flexible and intelligent protection systems which can detect and stop attacks because IOT usage will continue to grow after the pandemic. Organizations need to protect their IoT systems because this process ensures secure digital operations during future emergencies.

References

1. Abdelhaq, M. (2022) Internet of Things Fundamentals, Architectures, Challenges and Solutions: A Survey.
2. Gerodimos, A., Maglaras, L., Ferrag, M.A., Ayres, N. and Kantzavelou, I. (2023) 'IoT: Communication protocols and security threats', Internet of Things and Cyber-Physical Systems, 3, pp. 1-13 Available at: 10.1016/j.iotcps.2022.12.003.
3. Ghadeer, H. (Oct 2018) Cybersecurity Issues in Internet of Things and Countermeasures. IEEE, pp. 195.
4. Chen, C., Hasan, M. and Mohan, S. (2018) 'Securing Real-Time Internet-of-Things', Sensors, 18(12), pp. 4356 Available at: 10.3390/s18124356.
5. Gomathi, R.M., Krishna, G.H.S., Brumancia, E. and Dhas, Y.M. (Feb 2018) A Survey on IoT Technologies, Evolution and Architecture. IEEE, pp. 1.
6. Gupta, B.B. and Quamara, M. (2020) 'An overview of Internet of Things (IoT): Architectural aspects, challenges, and protocols', Concurrency and computation, 32(21), pp. n/a Available at: 10.1002/cpe.4946.
7. Saqib, M. and Moon, A.H. (2023) 'A Systematic Security Assessment and Review of Internet of Things in the Context of Authentication', Computers & security, 125, pp. 103053 Available at: 10.1016/j.cose.2022.103053.
8. Sulich, A., Rutkowska, M., Krawczyk-Jezierska, A., Jezierski, J. and Zema, T. (2021) 'Cybersecurity and Sustainable Development', Procedia Computer Science, 192, pp. 20-28 Available at: 10.1016/j.procs.2021.08.003.
9. Ahmed, J. and Tushar, Q. (Dec 16, 2020) Covid-19 Pandemic: A New Era Of Cyber Security Threat And Holistic Approach To Overcome. IEEE, pp. 1.
10. Saleous, H., Ismail, M., AlDaajeh, S.H., Madathil, N., Alrabaee, S., Choo, K.R. and Al-Qirim, N. (2023) 'COVID-19 pandemic and the cyberthreat landscape: Research challenges and opportunities', Digital Communications and Networks, 9(1), pp. 211-222 Available at: 10.1016/j.dcan.2022.06.005.
11. Corallo, A., Lazoi, M., Lezzi, M. and Luperto, A. (2022) 'Cybersecurity awareness in the context of the Industrial Internet of Things: A systematic literature review', Computers in industry, 137, pp. 103614 Available at: 10.1016/j.compind.2022.103614.
12. Hijji, M. and Alam, G. (2021) 'A Multivocal Literature Review on Growing Social Engineering Based Cyber-Attacks/Threats During the COVID-19 Pandemic: Challenges and Prospective Solutions', IEEE access, 9, pp. 7152-7169 Available at: 10.1109/ACCESS.2020.3048839.
13. Khanam, S., Ahmedy, I.B., Idna Idris, M.Y., Jaward, M.H. and Bin Md Sabri, A.Q. (2020) 'A Survey of Security Challenges, Attacks Taxonomy and Advanced Countermeasures in the Internet of Things', IEEE access, 8, pp. 219709-219743 Available at: 10.1109/ACCESS.2020.3037359.
14. Vargo, D., Zhu, L., Benwell, B. and Yan, Z. (2021) 'Digital technology use during COVID-19 pandemic: A rapid review', Human Behavior and Emerging Technologies, 3(1), pp. 13-24 Available at: 10.1002/hbe2.242.

15. Shammari, A.A., Maiti, R.R. and Hammer, B. (Mar 10, 2021) Organizational Security Policy and Management during Covid-19. IEEE, pp. 1.
16. Buzzio-Garcia, J., Salazar-Vilchez, V., Moreno-Torres, J. and Leon-Estofanero, O. (Oct 12, 2021) Review of Cybersecurity in LatinAmerica during the Covid-19 Pandemic. A brief Overview. Piscataway: IEEE, pp. 1.
17. Lallie, H.S., Shepherd, L.A., Nurse, J.R.C., Erola, A., Epiphaniou, G., Maple, C. and Bellekens, X. (2021) 'Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic', Computers & security, 105, pp. 102248 Available at: 10.1016/j.cose.2021.102248.
18. Alamoodi, A., Zaidan, B., Zaidan, A., Albahri, O., Mohammed, K., Malik, R., Almahdi, E., Chyad, M., Tareq, Z., Albahri, A., Hameed, H., & Alaa, M. (2020). Sentiment analysis and its applications in fighting COVID-19 and infectious diseases: A systematic review. Expert Systems with Applications, 167, 114155 - 114155.
19. Faramarzi, S., Abbasi, S., Faramarzi, S., Kiani, S., & Yazdani, A. (2024). Investigating the role of machine learning techniques in internet of things during the COVID-19 pandemic: A systematic review. Informatics in Medicine Unlocked.
20. Bhattacharya, S., & Singh, A. (2025). Unravelling the infodemic: a systematic review of misinformation dynamics during the COVID-19 pandemic. Frontiers in Communication.