A Systematic Review Of Research Papers On Cybersecurity With Modern And Ancient Approaches

Prithvi P Shenoy, Dr. Niharika P Kumar
Dept. of ISE, RVITM
Bangalore, India

Abstract - There are various turbulences in our VUCA era, and cybercrime is one of the most significant contributors to turbulence. According to Cybersecurity Ventures, the cost of damages caused by cybercrime worldwide will increase by 15% annually over the next five years, reaching USD 10.5 trillion annually by 2025 versus USD 3 trillion in 2015. Hence there is a need for deep, structured research to bring awareness, make policies, implement an integrated control framework, monitor them closely and report periodically. This paper attempts a systematic review of research articles post-2018, covering a variety of cybersecurity-related subjects, such as network security, data privacy, threat intelligence, incident response, and risk management, among others. Initial results suggest that numerous hypothetical institutional models have been developed to address the dangerous problems. Even though there continues to be research on the methods, relatively few studies have shed light on the actual efficacy of these measurements. In conclusion, an interdisciplinary research approach is required to address cybersecurity's multifaceted nature systematically. This approach should incorporate cybersecurity's scientific, technical, organisational, human, and political components. As a result, an effort has been made to identify the principles from the Indian Knowledge System that are still relevant in modern science. Cybersecurity researchers and organisations will benefit from this systematic review in the quest to understand, measure, and manage cyber risks.

Index Terms - cybersecurity, emerging technologies, cyber-attacks, defence mechanisms, cyber-physical system (CPS)

I. INTRODUCTION

According to a recent analysis of cybercrime statistics, a breach with a life cycle of more than 200 days typically costs $4.87 million. With the teeming chaos created by cyber-attacks, companies and individuals need to explore effective cyber security services in light of the rise in cyberattacks to shield their information from data breaches. Malware hackers employ creative techniques to remain undetected. This can entail renaming legitimate files and employing a malicious payload contained in a file that mimics an error log. Phishing emails continue to be the most prevalent type of cyberattack in the world, there is no doubt about that. Additionally, it becomes riskier every day. A fraudulent link may be clicked by 1 in 5 email recipients, according to the Phishing Benchmark Global Report. In addition, 3 billion phishing emails are sent daily in an effort to hack sensitive data.

Have you ever considered the harm a virus could cause to your computer? This can be understood with an illustration. MyDoom, which has cost $38 billion in financial losses, is the most costly computer virus ever created in the entire history of cyber security. On the other hand, all defence tactics are built on situational awareness. Therefore, there has been a need for increased diversity and inclusion in cybersecurity research to ensure a broader representation of perspectives and expertise for more comprehensive and effective solutions has resulted in the development of this paper. This survey draws on a systematic review of relevant research papers from reputable journals, conferences, and other academic sources. By analysing and synthesising the findings of existing research papers, this review aims to shed light on the key themes, methodologies, and findings in the field of cybersecurity, as well as identify areas that require further investigation.

II. LITERATURE SURVEY

As a part of understanding the current landscape of cybersecurity threats and defence strategies, an approach of a systematic review of research papers was employed. From the tools and frameworks used to detect the major threats to analysing the attacks and devising defence strategies, a range of papers were selected from established sources. In order to align the study with the recent trends, about 20 articles post 2018 were shortlisted and summarised.

The study of diverse cyber security approaches around the world has revealed the disruption due to malignant attacks and emphasises the exigency of designing effective frameworks for integrated security of systems. Sufficient research is unavailable to analyse the legislation and methods that have been implemented to prevent cyber attacks. Thus, a study of security concerns in various sectors across the globe has provided useful insights by highlighting the challenges for the optimal management of cyber security systems.

III. RESEARCH METHODOLOGY

This qualitative research analyses the data on cyber security threats and prevention of attacks based on the grounded theory approach. Due to lack of sufficient empirical data, a systematic review of the literature was carried out in accordance with the principles of narrative analysis. This led to the review of the trends and gaps in the literature with special focus on the tools employed to mitigate the cyber attacks. To get a wider perspective, the study was extended to include the security techniques in various sectors like healthcare and learning.

IV. ANALYSIS

Table 01. Analysis of articles

Sl.	Title of paper	Aim of paper	Findings	Gaps
1	Internet of Things: A Comprehensive Study of Security Issues and Defense Mechanisms [1]	To enlist security challenges and analyse defence mechanisms against those attacks	Major threats include 1. Flooding networks 2. Spoofing 3. Altered integrity and credibility of data 4. Authenticity repudiation Top attacks 1. Sinkhole attack 2. Wormhole attack 3. Selective forwarding 4. Sybil attack 5. Denial of Service (DoS) Attack 6. Hello Flood Attack	Steps for leveraging loopholes to escape hackers and attackers especially with advancements in technology
2	Cyber Security Situational Awareness among Parents [2]	A quantitative data analysis to examine the level of parental awareness about cybersecurity laws in Malaysia	The level of awareness among parents is moderate 1. Only 65.6% of respondents acknowledged the activities of their children in the cyberspace 2. A smaller fraction recognised the exposure to threats 3. 75.7% were aware of the role played by parents in monitoring the usage of mobiles.	Emphasis to be laid on organisation-specialised programs, effective awareness and information sharing sessions specially designed for parents and teachers.
3	A Scoring System to efficiently measure Security in Cyber-Physical Systems [3]	To determine a security score of a CPS based on a) Potential of an attack b) Harm of attack	Vulnerability of CPS Resulting damages 1. Data loss 2. Damage to critical components 3. Harm to end users 4. Evaluation of impact on assets	Refinement of mitigation concepts with practical implementation and proof of concept
4	Cyber security threats, challenges and defense mechanisms in cloud computing [4]	To scrutinise security threats associated with cloud computing	Presentation of benefits of cloud computing for businesses Inferential analysis of threats like 1. SQL injections 2. Cross site scripting 3. Man in the middle attacks 4. Sniffer attacks 5. Captcha breaking 6. Google hacking	Anomalies due to insecure APIs
5	Social Cybersecurity : An emerging science [5]	To define the new science of social cybersecurity	Distinction between social cybersecurity, cybersecurity and cognitive cybersecurity Building tools using social network analysis and AI	Little knowledge about the field
6	Implementation of Cyber-Physical	To implement a protocol that helps in	Scalable and flexible protocol with Modbus/TCP communication over the	Elucidates only the behaviour of CPS under

	Systems with Modbus Communication for Security Studies [6]	studying behaviour of CPS under different conditions	traditional Modbus approach supported by most devices	attack Complex industrial processes require sophisticated detection and prevention measures
7	Smart Cyber-Physical Systems: Beyond Usable Security to Security Ergonomics by Design [7]	To reiterate the need of security ergonomics with emphasis on security breach	Existing frameworks 1. Swiss cheese 2. Human factors analysis and classification system Proposes foundational design principles for security ergonomics along with the importance of human factors to be considered in CPS	Mitigating human errors while moving towards smart CPS is a huge challenge
8	A comprehensive review of cyber-attacks and defense mechanisms for improving security in smart grid energy systems: Past, present and future [8]	To study and discuss different cyber-attack models	Key ideas on smart grids (SG) 1. Usage of modern technology questions the security and stability of energy systems 2. System malfunctions may even cost lives 3. Attacks include - false data driven, data injection attack 4. Detection mechanisms based on federated learning methods	
9	The Current State of Cyber Security in Ireland [9]	A comparative analysis of different cybersecurity strategies	Roles, responsibilities and interactions 1) Stakeholders of the network 2) Governmental cyber security centre 3) Sector CERTs	Insufficient awareness amongst people and policymakers
10	An Innovative Modular Approach of Teaching Cyber Security across Computing Curricula [10]	To present the current status of modules developed for teaching cybersecurity	Topics included 1. Risk management 2. Software reverse engineering 3. Cryptography Modules comprise 1. Caesar Cipher - software lab activity 2. Client server communication 3. Sniffing Methodology - powerpoint slides, lab exercises	Interactive tools for experiential learning of various attacks and defence solutions
11	The Construction Method of Computer Network Security Defense System Based on Multisource Big Data [11]	To propose a computer network security defence system based on big data	Main functions include 1. Data source selection 2. Unified view establishment 3. Unified view update Usage of rule-based algorithm for optimization	
12	Ethics in Cybersecurity Research and Practice [12]	To rethink the ethical flank while considering security	Key issues addressed 1. privacy 2. transparency 3. accountability 4. fairness respect for autonomy	Need of identifying a balance between security and freedom to an individual
13	Framework Of Malay Intelligent Autonomous Helper (Min@H): Text, Speech And Knowledge Dimension	To determine elements that shape the future of military education	Technology transforms modern day methods of learning and teaching Proposed system is a virtual helper to a trainee by a) Detecting behaviours b) Reasoning and responding to those behaviours	Cyber threats not considered in developing the computational model

	Towards Artificial Wisdom For Future Military Training System [13]		Generating appropriate social responses	
14	Cybersecurity in healthcare [14]	To analyse threats to medical devices and critical infrastructure	Two primary drivers that expose the sector to threats 1. Advancing technology 2. Evolving federal policy Striking facts 1. Cyber attacks which target medical information is increasing 22 percent a year 2. A single attack costs organisations around 3.7 million dollars	Defence strategies specific to healthcare sector need to be proposed
15	Cybersecurity Data Science: An overview from machine learning perspective [15]	To discuss intrusion detection approaches in detail	Highlights different attack types with cybersecurity datasets Unique defence strategies identified 1. Signature based IDS 2. Anomaly based IDS 3. Hybrid approach 4. Stateful protocol analysis approach	Integration of data science and machine learning methods to build effective defence mechanisms
16	Does the NIS implementation strategy effectively address cyber security risks in the UK? [16]	To implement cyber risk management with Networks and Information Security (NIS)	Implementation approach sector wise 1. Health 2. Transport 3. Finance 4. Water 5. Energy 6. Digital infrastructure Discussion includes security culture and strategic goals	1. Recommendations have been provided on the identified gaps - need to be implemented
17	Design principles for national cyber security sensor networks: Lessons learned from small-scale demonstrators [17]	To identify a framework for cyber security sensor network (CSSN)	Level based indicators of threats 1. Atomic indicators 2. Computed indicators 3. Behavioural indicators Blueprint of the architecture highlights the sensor network node along with sensing tools and servers	Distribution of roles and responsibilities for the introduced architecture 2. Addressing the governance, operational and implementation issues
18	Global cybersecurity: New directions in theory and methods [18]	To illuminate the various methods of examining cybersecurity in democratic contexts	Investigates sociological sites of cybersecurity Emphasises disciplinary epistemology and establishes the potential of ethnographic study	3. Theoretical frameworks have been devised as an assemblage of sociotechnical practices and politics separately
19	Framework for Improving Critical Infrastructure Cybersecurity [19]	To provide a common organising structure to cybersecurity by assembling standards, guidelines and practices	Primary focus on 1) Information Technology 2) Industrial control systems 3) Cyber physical systems 4) Connected devices 5) Internet of Things Cyber supply chain relationships	4. Self assessing Cybersecurity risk not on par with evolving metrics
20	Machine learning and deep learning methods for cybersecurity [20]	To identify various network attacks	Zero-day attacks cannot be detected using misused technologies Classification of attacks based on datasets ML and DL Algorithms used 1. Support vector machine 2. K-nearest neighbour 3. Decision tree	5. Benchmark datasets and few 6. Evaluation metrics are not uniform

			4. Deep belief network 5. Recurrent neural networks 6. Convolutional neural networks	

V. RESULTS AND FINDINGS

The preliminary results point to an increase in the usage of AI and ML in cybersecurity for automated response, threat detection, and anomaly detection. The growing recognition of the importance of human factors in cybersecurity, including user behaviour, human-centric security designs, and awareness training highlights the altering perspectives of finding solutions. The forthcoming problems and research trends in securing IoT devices and networks include issues related to privacy, authentication, and data integrity. The evolving landscape of cloud computing and the need for robust security measures to protect data and applications stored in the cloud is observed. The requirement of timely and accurate threat intelligence, as well as effective information sharing and collaboration among stakeholders for proactive cybersecurity measures is highlighted in the articles discussing the frameworks.

These results focus on solving issues related to the following themes:

1. Innovative Solutions: The need for innovative and adaptive cybersecurity solutions that can effectively combat emerging threats and evolving attack vectors.
2. Policy and Legal Frameworks: The importance of developing robust policy and legal frameworks that address the challenges of cybersecurity, including regulations, standards, and guidelines.
3. International Cooperation: The increasing need for international cooperation and collaboration among countries, organisations, and stakeholders to address global cybersecurity challenges that transcend national boundaries.
4. Privacy and Data Protection: The growing focus on privacy and data protection in cybersecurity research, including the development of privacy-preserving technologies and practices.
5. Education and Awareness: The importance of continuous education and awareness programs to foster a cybersecurity-aware culture, including cybersecurity training for users, practitioners, and policymakers.

Many organisational models have been designed hypothetically to counter the menacing issues. Although there is research available on the approaches, very few studies have thrown light on the actual effectiveness of these measures. However, some inferences on cyber security have been mentioned in the ancient Indian sciences which are discussed in the next section.

VI. POINTS OF DISCUSSION

Table 02. Ancient Science parallels

Sl. no	Source	Ancient Indian concepts	Modern day relevance
1.	Subhashita समयोचितपद्य मालिका	चिन्तनीया हि विपदाम् आदावेव प्रतिक्रिया । न कूपखननं युक्तं प्रदीप्ते वह्निना गृहे ॥ Meaning: We should have the solutions ready even before some problem comes to us, unlike digging a well when the house is on fire	Cyber risk management includes 1. Having predefined solutions to possible threats 2. Designing risk response strategies prior to the attacks
2.	Panchatantra	उत्थायोत्थाय बोद्धव्यं महद्भयमुपस्थितम् Meaning: Get up and realise that a great fear has come upon you	Cyber paranoia 1. The fear factor surrounding cyber security is greater than ever, especially after the pandemic. 2. Requirement of every day, every moment monitoring to avoid potential attacks
3.	Ramayana	तं वञ्चयानो राजेन्द्रमापतन्तं निरीक्ष्यवै। बभूवान्तर्हितस्त्रासात्पुनस्सन्दर्शनेऽभवत्।।च3.44.3।। On seeing Rama approaching him, the deer disappeared due to fear and again came within sight. With his sword and the bow, Rama chased wherever the deer ran.	Maricha : The hacker, attacker and deceiver Study the behaviours and activities of hackers The distraction attack 1. Attacks happen through DoS, Website defacements 2. Defending against the attack by using leveraged Domain Name System (DNS)

		स प्राप्तकालमाज्ञाय चकार च तत स्वनम्। सदृशं राघवस्येह हा सीते लक्ष्मणेति च।।3.44.19।। Then Maricha realised that the appropriate time had come. In a voice similar to Rama's, he shouted loudly 'Alas Sita, Alas Lakshmana '	
	Ramayana	उपतस्थे च वै देहीं भिक्षुरूपेण रावणः। Disguised as a mendicant he stepped toward where Sita was. सद्यस्सौम्यं परित्यज्य भिक्षुरूपं स रावणः। स्वं रूपं कालरूपाभं भेजे वैश्रवणानुजः।।3.49.6।। Ravana shed the gentle figure of a mendicant and assumed a ferocious form	Ravana : Impacts of social engineering 1) Attackers manipulate, influence and deceive the victim to gain control 2) Baiting, phishing, tailgating are a few examples 3) Used to carry out further attacks
	Ramayana	युद्ध्यस्व यदि शूरोऽसि मुहूर्तं तिष्ठ रावण।।3.50.22।। O Ravana, if you are brave, fight with me. (- says Jatayu on seeing Sita being kidnapped) हृता सा राक्षसेन्द्रेण रावणेन विहायसा। मायामास्थाय विपुलां वातदुर्दिनसङ्कुलाम्।।3.68.9।। Jatayu informs Rama about the abduction	Jatayu : Perimeter device logs 1) Effective Intrusion detection systems, Virtual private networks 2) Deployment of perimeter devices - Routers, firewalls etc 3) Understanding external threats and countermeasures
4.	Vedas and Puranas	Establishing organisational security culture is akin to performing a yagna 1. the *yajaman* (e.g., a CXO) making offerings (e.g., investments, capital) 2. "*svaha*" – "this of me I offer" (investments, goods, services, business ideas, different types of capital), 3. "*tathastu*"— so it shall be	Increased cyberattacks (Eg: AIIMS cyber-attack, SBI cyber-attack, NotPetya, Colonial Pipeline) Action terms for IT/IoT driven organisations 1. Entice C-suites to promote security culture 2. Culture of compliance to improve enterprise security posture 3. Plain awareness without action is of no use

VII. CONCLUSION

The empirical studies that validate the effectiveness of cybersecurity solutions and provide evidence-based insights into their real-world impact are limited. Another drawback is the lack of standardised evaluation criteria and benchmarks for cybersecurity solutions, hindering meaningful comparisons and assessments of their effectiveness. Since there has been little collaboration between academia and industry it has led to a gap between theoretical research and practical implementation of cybersecurity solutions. Hence, there is a need for an interdisciplinary research approach that integrates scientific, technical, organisational, human and political aspects of cybersecurity to address its complex nature systematically. As a result, an attempt has been made to draw the present-day scientific relevance of concepts from the Indian Knowledge System. In conclusion, this paper provides a valuable overview of the current state of cybersecurity research, identifies areas that require further attention, and presents future directions for the field. By addressing these trends, gaps, and future directions, cybersecurity empiricists and practitioners can accord to the development of effective and robust cybersecurity solutions, policies, and practices to safeguard critical systems, data, and privacy in the digital era.

VIII. REFERENCES

[1] Ahanger, T. A., & Aljumah, A. (2019). Internet of things: A comprehensive study of security issues and defense mechanisms. IEEE Access, 7, 11020-11028. doi:10.1109/access.2018.2876939

[2] Ahmad, N., Mokhtar, U. A., Fariza Paizi Fauzi, W., Othman, Z. A., Hakim Yeop, Y., & Huda Sheikh Abdullah, S. N. (2018). Cyber security situational awareness among parents. 2018 Cyber Resilience Conference (CRC). doi:10.1109/cr.2018.8626830

[3] Aigner, A., & Khelil, A. (2020). A scoring system to efficiently measure security in cyber-physical systems. 2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom). doi:10.1109/trustcom50675.2020.00151

[4] Aljumah, A., & Ahanger, T. A. (2020). Cyber security threats, challenges and defense mechanisms in cloud computing. IET Communications, 14(7), 1185-1191. doi:10.1049/iet-com.2019.0040

[5] Carley, K. M. (2020). Social Cybersecurity: An emerging science. Computational and Mathematical Organization Theory, 26(4), 365-381. doi:10.1007/s10588-020-09322-9

[6] Chattha, H. A., Rehman, M. M., Mustafa, G., Khan, A. Q., Abid, M., & Haq, E. U. (2021). Implementation of cyber-physical systems with Modbus Communication for Security Studies. 2021 International Conference on Cyber Warfare and Security (ICCWS). doi:10.1109/iccws53234.2021.9702959

[7] Craggs, B., & Rashid, A. (2017). Smart cyber-physical systems: Beyond Usable Security to security ergonomics by Design. 2017 IEEE/ACM 3rd International Workshop on Software Engineering for Smart Cyber-Physical Systems (SEsCPS). doi:10.1109/sescps.2017.5

[8] Ghiasi, M., Niknam, T., Wang, Z., Mehrandezh, M., Dehghani, M., & Ghadimi, N. (2023). A comprehensive review of cyber-attacks and defense mechanisms for improving security in smart grid energy systems: Past, present and future. Electric Power Systems Research, 215, 108975. doi:10.1016/j.epsr.2022.108975

[9] Lang, M., Dowling, S., & Lennon, R. G. (2022). The current state of Cyber Security in Ireland. 2022 Cyber Research Conference - Ireland (Cyber-RCI). doi:10.1109/cyber-rci55324.2022.10032682

[10] Lodgher, A., Yang, J., & Bulut, U. (2018). An innovative modular approach of teaching cyber security across computing curricula. 2018 IEEE Frontiers in Education Conference (FIE). doi:10.1109/fie.2018.8659040

[11] Ma, J., & Li, S. (2022). The construction method of computer network security defense system based on Multisource Big Data. Scientific Programming, 2022, 1-13. doi:10.1155/2022/7300977

[12] Macnish, K., & Van der Ham, J. (2020). Ethics in Cybersecurity Research and Practice. Technology in Society, 63, 101382. doi:10.1016/j.techsoc.2020.101382

[13] Marzukhi, S., Zainol, Z., Muhamed, H., Awang, N. F., Sembok, T. M., & Juhary, J. B. (2019). Framework of Malay Intelligent Autonomous Helper (min@h): Text, speech and knowledge dimension towards artificial wisdom for future military training system. 2019 1st International Conference on Artificial Intelligence and Data Sciences (AiDAS). doi:10.1109/aidas47888.2019.8970881

[14] Rai, B. K., & Solanki, T. (2021). Access control mechanism in Health Care Information System. Cybersecurity, 149-160. doi:10.1201/9781003145042-10

[15] Sarker, I. H., Kayes, A. S., Badsha, S., Alqahtani, H., Watters, P., & Ng, A. (2020). Cybersecurity Data Science: An overview from machine learning perspective. Journal of Big Data, 7(1). doi:10.1186/s40537-020-00318-5

[16] Shukla, M., Johnson, S. D., & Jones, P. (2019). Does the NIS implementation strategy effectively address cyber security risks in the UK? 2019 International Conference on Cyber Security and Protection of Digital Services (Cyber Security). doi:10.1109/cybersecpods.2019.8884963

[17] Skopik, F., & Filip, S. (2019). Design principles for national cyber security sensor networks: Lessons learned from small-scale demonstrators. 2019 International Conference on Cyber Security and Protection of Digital Services (Cyber Security). doi:10.1109/cybersecpods.2019.8885134

[18] Stevens, T. (2018). Global cybersecurity: New directions in theory and methods. Politics and Governance, 6(2), 1-4. doi:10.17645/pag.v6i2.1569

[19] Stine, K. (2014). Framework for improving critical infrastructure cybersecurity, version 1.0 . doi:10.6028/nist.cswp.1

[20] Xin, Y., Kong, L., Liu, Z., Chen, Y., Li, Y., Zhu, H., . . . Wang, C. (2018). Machine learning and deep learning methods for cybersecurity. IEEE Access, 6, 35365-35381. doi:10.1109/access.2018.2836950