International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 09 Issue: 03 | March - 2025 SJIF Rating: 8.586 ISSN: 2582-3930

Literature Review on Combating Cyber Threats

Deepu C P
Department of Computer Science and Engineering (Cyber Security)
Vimal Jyothi Engineering College
Chemperi, Kannur
Email:deepu3dra5@gmail.com

Swathi Ravi M
Department of Computer Science and Engineering (Cyber Security)
Vimal Jyothi Engineering College
Chemperi, Kannur
Email:raviswathi931@gmail.com

Lajin C P
Department of Computer Science and Engineering (Cyber Security)
Vimal Jyothi Engineering College
Chemperi, Kannur
Email:lajincp1011@gmail.com

Faheema Hassan
Department of Computer Science and Engineering (Cyber Security)
Vimal Jyothi Engineering College
Chemperi, Kannur
Email:faheemah703@gmail.com

Mr.Rasheed Ahamed Azad V
Assistant Professor
Department of Computer Science and Engineering (Cyber Security)
Vimal Jyothi Engineering College
Chemperi, Kannur
Email:rasheedklpm@vjec.ac.in

***Abstract*—Technological advancement is accelerating, but this may also endanger people to cyberattacks. RSA and all the other traditional encryption techniques were once thought to be unforgivable, but were soon broken with the emergence of quantum computing, which removed them for the Quantum Resistant Algorithm. This traditional method is thought to be robust with regard to the current available technologies. However, this would change because, with each technological advancement, a system thought to be perfectly secure today will find its weakness tomorrow. Threats extend much beyond problems with encryption. Software flaws, weak passwords, phishing schemes, social engineering techniques more complex threats like artificial intelligence tools, such as hacking automated toolkits and deepfake-based identity fraud, are all utilised by cybercriminals to obtain confidential information without authorisation. In the digital age, cybersecurity is a constant struggle due to the growing likelihood of data breaches, ransomware attacks even major system failures are caused by the growth in digital infrastructure.**

***Index Terms*—Cybersecurity, Hybrid Security Systems, Physical-Digital Integration, AI/ML Security, Proactive Cyber Defense, Fake Data Generation.**

I. INTRODUCTION

The current world scenario shows that digital systems are becoming vulnerable to cyber breaches in data privacy and the critical infrastructure. With the increase of interdependencies in technologies and advanced sophistication in cyberattacks, the capabilities of conventional security solutions quickly fall into the quagmire of being mostly reactive and failing to keep pace with changing threats. These high-profile data breaches and ransomware attacks highlighted how vulnerable traditional defenses really were, since they were majorly software-based. Since the attacker has now been widely seen to exploit the most sophisticated methods of AI-driven threats and zero-day exploits, the urgency for a novel hybrid security system that combines digital and physical defenses became pressing. It will be a multi-layered defense of both cyber and hardware threats, integrating AI/ML for real-time threat detection with physical security measures such as secure hardware activation keys and biometric authentication. This hybrid approach will be proactive and continuous in monitoring digital environments and physical infrastructures, thereby reducing attack surfaces and successfully preventing unauthorized access. In the view of the evolving sophisticated Cyber threats and the increasing dependence on digital systems for critical operations across industries, not only robust but more importantly scalable and adaptable solutions are needed to cope with different environments. With continuous evolution in cyberattacks, conventional one-dimensional defense mechanisms cannot be sustained.To effectively secure sensitive data and infrastructure, the systems need to envision and mitigate risks in the future and deliver reliable protection from continually evolving complex, persistent cyber threats. To secure critical assets within a dynamic and interconnected environment, there is therefore a necessity to develop and embrace a robust hybrid security system.

II. LITERATURE SURVEY

Hari Mohan Rai et al. propose [1] a in-depth study on the incorporation of blockchain technology and the IoT to enhance security, integrity and confidentiality, particularly in nuclear energy applications. The study considers several phases of privacy, security and data integrity as well as possible applications for these technologies. Nuclear energy sector developments is an application of the blockchain technology that was able to solve flow chart security related issues. It recognizes some of the limitations of the report as including the need for practical verification, challenges of IoT configurations with constrained resources and the increasing threat of cyberattacks. The future studies should, therefore, concentrate on post-quantum cryptography, scalable blockchain solutions, standardization, privacy laws and

TABLE I
COMPARISON TABLE

Reference	Description	Advantages	Disadvantages
[1]	Blockchain and IoT integration enhances data security, privacy and integrity in energy applications, particularly in the nuclear sector.	• Provides tamper-proof data storage through blockchain's immutability. • Ensures accurate data verification for critical applications.	• Blockchain struggles with scalability for large IoT data. • Requires constant updates to address evolving cyberthreats.
[2]	The HDE model uses ChCoA for key optimization and EDHA for decryption, improving data security and performance.	• Faster encryption and decryption with reduced processing time. • Secure key optimization enhances data protection.	• Computationally intensive for key optimization. • Limited real-time application adaptability.
[3]	The study combines traditional data security methods with blockchain to enhance data integrity, privacy and security.	• Provides tamper-proof and traceable data. • Supports secure applications in various fields.	• Privacy risks due to blockchain's openness. • High computational costs for implementation.
[4]	A two-stage model uses nine CIA indicators and expert scoring to classify and secure data accurately.	• Enhances data protection with detailed CIA indicators. • Scalable for various industries.	• Risk of bias in expert scoring. • Time-intensive implementation.
[5]	A machine-learning algorithm enhances security by detecting threats, analyzing sensitive data and integrating data from multiple sources.	• Automates sensitive data identification and behavior tracking. • Enhances data integrity, privacy and disaster recovery.	• High resource consumption for large datasets. • Limited efficiency for real-time security needs.
[6]	An improved KPCA algorithm enhances network intrusion detection, improving classification accuracy, reducing false alarms and optimizing performance in the big data era.	• Higher classification accuracy. • Lower false alarm and missing alarm rates.	• Relies on the quality of the dataset. • May require significant computational resources.
[7]	A hybrid deep learning model combining Adaptive TensorFlow DNN and Improved Particle Swarm Optimization (IPSO) for detecting malware and software piracy in IoT environments.	• Accurate and effective malware detection. • Real-time threat identification.	• Requires large, high-quality datasets. • Computationally expensive for resource-constrained devices.
[8]	Securing computers with cybersecurity measures and green computing strategies ensures protection from viruses, minimizes energy consumption and promotes sustainability in digital environments.	• Prevents data breaches and system disruptions. • Optimizes energy usage, supporting environmental sustainability.	• Implementation can be costly and complex. • Requires ongoing updates to address evolving threats.
[9]	This study examines how security tools and user activities impact malware protection, highlighting that risky behavior increases infections while security activities reduce them.	• Provides insights into how user actions influence malware protection. • Combines survey data with real-world scans for robust findings.	• Focuses only on personal computers, excluding mobile devices. • Data is outdated (2014), limiting relevance to current threats.
[10]	This study explores the challenges and solutions related to cyber-attacks, emphasizing the evolving role of cyberspace in global security.	• Discusses the need for cooperation between governments and private sectors to tackle cyber threats.	• Traditional security methods are insufficient to address the complexity of modern cyber threats.
[11]	This paper discusses the global state of data security governance, highlighting challenges and proposing solutions to modernize systems for protecting big data.	• Provides a comprehensive overview of legislative efforts in data protection worldwide.	• Complex regulations may create difficulties in balancing data sharing and security.
[12]	This article explores the effectiveness of Nature-inspired Cyber Security (NICS) in securing web data and applications against evolving cyber threats.	• It provides high-level security through bio-inspired techniques like deception and camouflage.	• Full implementation of NICS as a comprehensive security solution is still in progress.

real-world testbeds to enhance and validate this integration.

Prasad Vangapandu et al. propose a novel approach [2] to encryption and decryption by using the Hybridized Data Encoding (HDE) model to enhance the safeguarding of data.The main goal of the paper is to enhance the cryptographic operations effectiveness, while rectifying the issues in the use of algorithms that demand vast memory usage and power consumption. In this approach, the ChCoA (Chaotic Coati Optimization Algorithm) will optimize the process of encryption while the EDHA decrypts the data. Thus, the security for exchanging data and against vulnerability is provided in the model suggested. It evaluates its model performance by using the Matlab platform, giving a processing time of 0.55 seconds and throughput of 249.1093 kb/s. This efficient method results in improved performance in cryptographic systems and further strengthens data security.

Yuqing Xu et al. discuss the growing role of blockchain [3] as a distributed infrastructure and its use in various applications. All of these, namely intelligent contracts, cryptographic techniques, distributed node consensus algorithms and blockchain's unique chain data format, support safe transfer, data restoration and data verification. However, data security remains a huge challenge since data has become a necessary part of the blockchain. Data security technologies that include K-Anonymity, ring signatures, trusted execution environments, homomorphic encryption, secure multi-party computing, zero-knowledge proof, and many more are highlighted in the study. These technologies are analyzed in the context of blockchain in an attempt to resolve conventional data security concerns and ensure the ecological security and protection of blockchain data. The study compares several approaches to improve overall security in blockchain systems.

Xingde Zhou et al. propose a two-phase [4] classification system for data. The nine CIA (Confidentiality, Integrity, Availability) indicators serve as the foundation for this hybrid strategy. The technique uses a specialized scoring mechanism for exact filtering and statistical analysis and data screening. This method is also applied to G Securities Company, where their data is classified into 76 sections. There is a second grading step that is performed on the scores of each indices for the various sections. It illustrates outcome which shows that such a way of improving data protection accuracy and robustness enhances data sharing and its circulation value; essentially, it primarily depends on the CIA (Confidentiality, Integrity, Availability).

Ruchun Jia et al. propose a security defense algorithm which is based on the Machine Learning [5] that utilizes metadata association features to address the increasing cybersecurity threats in the era of big data. This specific algorithm focuses on the privacy, integrity and availability, and also controls unauthorized access. It establishes a user model that maps to metadata from data sources to decompose user queries into queries for heterogeneous data sources, enabling data integration based on metadata association. The system analyses the user data and builds an behavior audit platform. With the volume of 5×10^3 bits in data volume, the experiment result shows that the proposed method attains 92 percentage of data storage integrity, 98 percentage of data accuracy and a relatively low data intrusion success rate of 2.6. The proposed method has proven its strong resistance against data intrusion, good data accuracy and robust performance for disaster recovery. It will maximize the security defense strength for the big data users.

Junjun Guo et al. propose an improved Kernel Principle Component Analysis (KPCA) algorithm [6] to address the challenges in analyzing and protecting internet information security. The proposed algorithm enhances the performance of traditional KPCA feature extraction, which in turn improves its subsequent classification capability. The experiment employed the KDDCUP99 security audit dataset, simulating network intrusions. Here, 7 weeks of data of size 5 million records were used in training the data and 2 weeks of data of size 2 million records for validation. The experimental results prove that the advanced algorithm is better than the traditional KPCA in efficiency, convenience and speed. Meanwhile, the improved accuracy, false alarm rate and missing alarm rate of the new algorithm are of significant improvement. This algorithm is thus a more efficient tool for big data network intrusion classification.

S. Markkandeyan et al. propose a hybrid Deep Learning (DL) strategy [7] to enhance cybersecurity in the Internet of Things (IoT) by detecting malware-infected programs and files. The research works on identifying the illegal content. This is done via SC duplication that is based upon the TensorFlow deep neural network accompanied by particle swarm optimization. In this mixed approach, DL has been combined with optimization methods that provide more accurate and effective threat detection, especially in real-time scenarios. The method applies tokenization, weighting features for noisy data filtration and further applies DL in order to identify SC duplication. Google Code Jam(GCJ) is referred for the dataset and for the identification of suspicious actions, E-LSTM is used. For testing malware samples, the Maling dataset is utilized. The proposed method outperforms traditional approaches in classifying and evaluating cybersecurity threats within the IoT environment.

Imtiaz Ahmad et al. inspect the changing characteristics of an altered computer virus framework [8] to better understand how its parameters interlink with attributes of the network. Banach's and Schaefer's fixed-point theorems are used for its application and this helps in examining the availability and variety of remedies for the framework proposed here. Adequate circumstances for Ulam–Hyers stability are also derived in the computer virus model. Numerical analysis

is made with an efficient numerical technique, evaluating the impact of various input elements on the dynamics of computer viruses and analyzing solution trajectories. This research helps design networks with a minimal chance of virus outbursts based on different segmentation constraints and extends an awareness towards the connection between model parameters. This study integrates robust cybersecurity and green computing strategies, providing security as well as energy efficiency in network environments.

Á lvaro Arenas et al. investigate [9] the effectiveness of two methods for defending home computers against security risks: security exercises and security tools. A model, in collaboration with more than 1900 people based on data coming from Spain and with a combined actual and self-reported data online survey and user-computer information, has explained the security impact that users have for protection of malware infection using their personal computers as part of the routine activity theory. Multidimensional, the logit, and probit regressions are used in the study to show that while using security software is positively correlated with greater danger actions and infections, using security measures also lowers malware infections. These results highlight the fact that security education and awareness programs are essential as security tools themselves are not good enough to ensure protection for users.

Yuchong Li's study provides [10] thorough analysis of the present state of cyber security today, highlighting the difficulties and developments in defending against cyberattacks in a society that is largely dependent on electronic technology. It focuses on the various cyber threats that face organizations, including PCs viruses, attack vectors, including DDS (Data Distribution Service), might serve strategic, military, or financial objectives. A review of standard and emerging prevention methods against the damage cyber-attacks may cause with both operational and research phase solutions is also included. The paper also reviews early-generation cyber security frames work and emerging trends and the latest results in the field. It hopes to be useful to IT and cyber security researchers with information on strengths, weaknesses and challenges within the cyber security solution.

Liyuan Sun et al. [11] analyze global big data security governance, focusing on challenges brought by faster technological advances in fields such as distributed computing and machine learning. As big data is turning out to be the strategic resource in this age of complexity, modern governance frameworks require adaptation to safeguard it against incessant cyber attacks. This requires a strong regulatory compliance framework so that the governance models adapt toward protecting sensitive information without compromising the scalability factor. Solutions like maintaining privacy, different encryption techniques, real-time anomalies and a blockchain-based network ensure integrity to data. It indicates the need for global standards and collaborative cybersecurity strategies to ensure that big data security governance is more resilient.

Shishir Kumar Shandilya [12] explores digital data security issues, with a focus on the dangers presented by the ever-evolving cyber attacks. His focus areas in research are on advanced methodologies of detecting data breaches and ensuring safe information flow within complex digital ecosystems. One key area he is talking about here is Data Provenance-aware techniques, where data lineage tracing and tracking their movement and transformations across systems could detect anomalies and prevent data leaks, thereby guaranteeing accountability. By maintaining the data lineage details, these methods improve breach detection and strengthen the security policies. Shandilya also introduces Nature-Inspired Cyber Security (NICS) systems. The NICS systems are adaptive, self-evolving security frameworks modeled after the biological processes of immune responses, swarm intelligence and natural adaptation. The natural alterations have dynamic adaptation mechanisms to emerging cyber threats, making these highly effective countermeasures in counteracting sophisticated attacks. By integrating provenance tracking with bio-inspired security approaches, his research is focused toward developing a stronger digital security framework that can be proactive against the eternal shifting cyber threat.

CONCLUSION

This survey indicates the growing demand for sophisticated and adaptive computer security solutions to be developed against ever-increasing threats from hackers over the internet. Though technologies such as encryption, machine learning blockchain seem to offer a lot of promise as defenses, the implementation in resource-constrained environments is quite challenging. Therefore, it demands a holistic approach towards ensuring protection with real-time threat detection, multi-layered defenses safeguarding software and hardware systems. This interconnection requires dealing with vulnerability aspects in connection with unauthorized access, malware attacks systems' integrity. Therefore, this kind of interconnectivity has brought out a great necessity to design and adopt scalable, flexible responsive security architectures toward developing greater cyber-resilient infrastructure and maintaining critical data and system security as long-lasting entities in this realm. In addition, the increasing sophistication and number of cyberattacks mean that innovative solutions need to be identified that will not only cover present security gaps but also provide insights into what will happen in the future. As the digital landscape continues to evolve, it therefore needs to be solutions agile enough to scale with the complexities of an interconnected system and maintain their integrity under new, unforeseen threats. Needed critically now are comprehensive and dynamic security frameworks to protect not just data but also, more importantly, the core trust in our global digital infrastructure. Unless these next-generation solutions come along, the vulnerabilities in systems continue to scale up even further, increasing the role of these actors. There has

never been a more pressing need to implement next-generation security policies.

REFERENCES

[1] H. M. Rai, K. K. Shukla, L. Tightiz, and S. Padmanaban, "Enhancing data security and privacy in energy applications: Integrating iot and blockchain technologies," *Heliyon*, vol. 10, no. 19, 2024.
[2] P. Vangapandu, T. Surendra, C. Ramineni, M. R. Madhavi, and R. H. Kishore, "Hybridized data encoding based encryption and diffie hellman decryption for security enhancement," *Knowledge-Based Systems*, vol. 306, p. 112653, 2024.
[3] Y. Xu, G. Xu, Y. Liu, Y. Liu, and M. Shen, "A survey of the fusion of traditional data security technology and blockchain," *Expert Systems with Applications*, p. 124151, 2024.
[4] X. Zhou, Z. Deng, J. Li, and J. Hao, "A two-stage data security classification model: Taking securities firm for example," *Procedia Computer Science*, vol. 242, pp. 249–255, 2024.
[5] R. Jia, J. Zhang, and Y. Lin, "Machine learning security defense algorithms based on metadata correlation features." *Computers, Materials & Continua*, vol. 78, no. 2, 2024.
[6] J. Guo and L. Wang, "Learning to upgrade internet information security and protection strategy in big data era," *Computer communications*, vol. 160, pp. 150–157, 2020.
[7] S. Markkandeyan, A. D. Ananth, M. Rajakumaran, R. Gokila, R. Venkatesan, and B. Lakshmi, "Novel hybrid deep learning based cyber security threat detection model with optimization algorithm," *Cyber Security and Applications*, vol. 3, p. 100075, 2025.
[8] I. Ahmad, A. A. Bakar, R. Jan, and S. Yussof, "Dynamic behaviors of a modified computer virus model: Insights into parameters and network attributes," *Alexandria Engineering Journal*, vol. 103, pp. 266–277, 2024.
[9] A´ . Arenas, G. Ray, A. Hidalgo, and A. Uruen˜a, "How to keep your information secure? toward a better understanding of users security behavior," *Technological Forecasting and Social Change*, vol. 198, p. 123028, 2024.
[10] Y. Li and Q. Liu, "A comprehensive review study of cyber-attacks and cyber security; emerging trends and recent developments," *Energy Reports*, vol. 7, pp. 8176–8186, 2021.
[11] L. Sun, H. Zhang, and C. Fang, "Data security governance in the era of big data: status, challenges, and prospects," *Data Science and Management*, vol. 2, pp. 41–44, 2021.
[12] S. K. Shandilya, "Paradigm shift in adaptive cyber defense for securing the web data: The future ahead," *Journal of Web Engineering*, vol. 21, no. 4, pp. 1371–1376, 2022.