Journal of Frontiers in Multidisciplinary Research

Privacy-Preserving AI for Cybersecurity: Homomorphic Encryption in Threat Intelligence Sharing

Abdullahi Olalekan Abdulkareem [1], Jamiu Olamilekan Akande [2*], Olufunbi Babalola [3], Adeladan Samson [4], Steve Folorunso [5]

[1] Lamar University, College of Business Beaumont, Texas, USA
[2] School of Computing and Digital Technology Birmingham City University, Birmingham, UK
[3] Carnegie Mellon University, 5000 Forbes Avenue Pittsburgh, PA 15213, USA
[4] Centre of Excellence for Excellence for Artificial Intelligence and Data Modelling University of Hull Cottingham Rd Hull, HU6 7RX United Kingdom
[5] University of Liverpool, United Kingdom

* Corresponding Author: **Jamiu Olamilekan Akande**

Article Info

E-ISSN: 3050-9726
P-ISSN: 3050-9718
Volume: 04
Issue: 02
July – December 2023
Received: 27-10-2023
Accepted: 26-11-2023
Published: 24-12-2023
Page No: 202-212

Abstract

The growing reliance on artificial intelligence (AI) for cybersecurity applications, particularly in threat intelligence sharing, presents both significant opportunities and complex challenges. As cyber threats become more sophisticated and widespread, organizations increasingly depend on collaborative efforts to detect, analyze, and mitigate attacks. Sharing threat intelligence across sectors enhances situational awareness and strengthens collective defense mechanisms. However, this collaborative approach raises serious privacy concerns, as the data involved often contains sensitive, proprietary, or personally identifiable information (PII). Ensuring data confidentiality while enabling meaningful AI-driven analysis necessitates robust privacy-preserving techniques. Homomorphic encryption (HE) has emerged as a promising solution that allows computations to be performed directly on encrypted data, preserving privacy without compromising analytical utility. This capability enables organizations to share encrypted threat intelligence and perform AI-based anomaly detection, malware classification, and pattern recognition without revealing raw data. In this context, HE facilitates secure multi-organizational collaboration, allowing encrypted inputs to be processed by machine learning models without exposing underlying information. This explores the integration of homomorphic encryption with AI in cybersecurity, emphasizing its application in privacy-preserving threat intelligence sharing. We review the various types of homomorphic encryption partial, somewhat, and fully homomorphic encryption and evaluate their suitability for real-world cybersecurity use cases. System architectures that support encrypted AI model inference, encrypted feature extraction, and secure aggregation of threat data are examined. Additionally, we discuss trade-offs between encryption strength, model performance, latency, and computational overhead. Case studies from sectors such as finance and healthcare illustrate the practical feasibility of HE-enhanced cybersecurity frameworks. Ultimately, this highlights homomorphic encryption as a key enabler of privacy-preserving AI for cybersecurity. It underscores the importance of continued research and optimization to make HE-based threat intelligence systems scalable, efficient, and widely adoptable in the evolving landscape of cyber defense.

DOI: https://doi.org/10.54660/.JFMR.2023.4.2.202-212

Keywords: Privacy-Preserving, AI, Cybersecurity, Homomorphic Encryption, Threat Intelligence Sharing

1. Introduction

Artificial Intelligence (AI) has become a cornerstone in modern cybersecurity, offering advanced capabilities in threat detection, vulnerability assessment, behavioral analysis, and response automation (Jimmy, 2021; Manda, 2021). In particular, AI enhances

threat intelligence, a strategic component of cybersecurity that involves the collection, processing, and analysis of data related to potential or ongoing threats. By leveraging machine learning (ML) models trained on large-scale datasets, AI systems can uncover hidden attack patterns, predict emerging threats, and provide actionable insights in real time (Sundaramurthy *et al*., 2022; Tadi, 2022). As cyberattacks grow increasingly complex and frequent, AI-driven threat intelligence offers the scalability and speed necessary to protect critical infrastructure, enterprises, and governments against evolving adversaries (Reddy, 2021; Guembe *et al*., 2022).

Effective threat intelligence, however, relies heavily on data sharing between organizations, sectors, and jurisdictions. The collaborative exchange of Indicators of Compromise (IoCs), attack signatures, tactics, techniques, and procedures (TTPs) enhances collective situational awareness and facilitates a coordinated defense strategy (Steingartner *et al*., 2021; Gupta *et al*., 2021). In many cases, attacks targeting one entity may also affect others within the same ecosystem, making shared intelligence critical to preventing widespread compromise. Data sharing enables security operations centers (SOCs) and national cybersecurity agencies to detect trends, reduce detection latency, and formulate faster response actions (Repetto *et al*., 2021; Shahjee and Ware, 2022). The more comprehensive and diverse the datasets available to AI models, the more accurate and effective they become.

Despite its benefits, cybersecurity data exchange is fraught with privacy concerns. Shared threat intelligence may include sensitive internal logs, user behavior records, network traffic data, and proprietary system configurations. Disclosure of such information can expose organizations to competitive risks, legal liabilities, and regulatory violations especially under data protection laws such as the General Data Protection Regulation (GDPR) and the Health Insurance Portability and Accountability Act (HIPAA). These concerns often hinder organizations from participating in data sharing initiatives, weakening the overall effectiveness of collaborative threat intelligence.

To overcome these barriers, privacy-preserving techniques have emerged as vital enablers of secure and trustworthy AI applications in cybersecurity. Among these, homomorphic encryption (HE) stands out as a powerful tool that allows computations to be performed directly on encrypted data. Unlike conventional encryption schemes that require data decryption for analysis thereby exposing sensitive content HE supports encrypted model inference and computation, maintaining data confidentiality throughout the process (Sana *et al*., 2021; Hamza *et al*., 2022). This makes it possible for organizations to contribute encrypted threat intelligence to a shared analysis platform without compromising their internal privacy. AI models can be trained or applied on encrypted datasets, enabling detection of cyber threats without revealing the underlying raw data.

Homomorphic encryption is particularly promising in multi-party or cross-organizational scenarios, where stakeholders do not fully trust one another or require strict data protection guarantees. With HE, collaborative AI systems can function across these boundaries, aggregating and analyzing data while preserving confidentiality and compliance. However, practical deployment of HE in real-time cybersecurity remains challenging due to its computational intensity and integration complexity (Asghar *et al*., 2019; Perumallaplli, 2019). As research and computational methods improve, HE is expected to become more viable and scalable for real-world applications.

The intersection of AI, cybersecurity, and data privacy demands robust mechanisms for secure data sharing. Homomorphic encryption offers a groundbreaking approach to enabling privacy-preserving AI-driven threat intelligence, allowing organizations to reap the benefits of collaborative cybersecurity while safeguarding sensitive data. This sets the stage for a future in which trust, privacy, and intelligence coexist in the global fight against cyber threats.

2. Methodology

The PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) methodology was employed to systematically identify, screen, and synthesize scholarly literature on the application of privacy-preserving artificial intelligence, with a specific focus on homomorphic encryption in the context of cybersecurity and threat intelligence sharing. A structured and comprehensive literature search was conducted across five major electronic databases: IEEE Xplore, SpringerLink, ScienceDirect, ACM Digital Library, and Scopus. The search included publications from 2015 to 2025 and utilized combinations of keywords such as “privacy-preserving AI,” “homomorphic encryption,” “cybersecurity,” “threat intelligence,” “encrypted machine learning,” “federated learning,” and “secure data sharing.”

All peer-reviewed journal articles, conference papers, and technical reports that discussed the integration of AI and cryptographic techniques, particularly homomorphic encryption, in cybersecurity or threat intelligence were considered. Studies that focused solely on traditional encryption, cloud computing without AI elements, or theoretical discussions without application to threat detection were excluded. After removing 87 duplicates from an initial set of 392 search results, 305 unique records were screened based on title and abstract. Of these, 186 were excluded for lacking relevance to both homomorphic encryption and AI-based cybersecurity. The full texts of the remaining 119 articles were evaluated in detail, and 56 studies that met the inclusion criteria were selected for the final qualitative synthesis.

From each selected study, key data were extracted, including the type of AI model used (e.g., logistic regression, neural networks), form of homomorphic encryption (partially, somewhat, or fully homomorphic), threat detection task, system architecture, and performance metrics such as accuracy, computational overhead, and latency. The synthesis of findings allowed for a comparative assessment of current methodologies, challenges, and potential advancements in applying homomorphic encryption to privacy-preserving AI systems for collaborative cybersecurity efforts.

2.1 Fundamentals of Threat Intelligence Sharing

Threat intelligence sharing is a cornerstone of modern cybersecurity, enabling organizations to detect, mitigate, and respond to cyber threats more effectively through collective knowledge and situational awareness. At its core, threat intelligence involves the gathering, analysis, and dissemination of information about malicious actors, their tactics, and the vulnerabilities they exploit (Tounsi, 2019; Seker, 2019). By converting raw data into actionable insights, threat intelligence empowers security teams to anticipate and

defend against potential attacks before significant damage occurs.

Threat intelligence can be broadly categorized into several types, each offering unique insights into adversary behavior. The most commonly exchanged form is Indicators of Compromise (IoCs) observable data such as IP addresses, domain names, file hashes, and URLs that signal malicious activity within a network or system. These indicators help organizations detect and respond to known threats. Another critical type is Tactics, Techniques, and Procedures (TTPs), which provide deeper contextual understanding of how adversaries operate. TTPs include information on attack methods (e.g., phishing, ransomware), tools used, and behavioral patterns, offering predictive capabilities and facilitating proactive defense strategies. Strategic threat intelligence includes high-level information about threat actors' motivations, affiliations, and geopolitical context, while operational intelligence focuses on near-term events and campaigns targeting specific sectors (Hicks *et al*., 2019; Cruickshank and Rassler, 2020).

The need for real-time, collaborative threat intelligence sharing is increasingly urgent as cyberattacks become more sophisticated, frequent, and cross-sectoral. Isolated defense measures are often insufficient to counter distributed threats such as zero-day exploits, advanced persistent threats (APTs), and large-scale ransomware campaigns. Sharing threat intelligence across organizations and sectors allows defenders to learn from each other's experiences and rapidly adapt to new threats (Tounsi and Rais, 2018; Van Haastrecht *et al*., 2021). For example, if a financial institution detects a new phishing domain, sharing this indicator with healthcare or energy sector entities can preempt similar attacks. go resilience and response capabilities across industries.

However, despite its critical role, the full potential of threat intelligence sharing is constrained by significant limitations tied to data sensitivity and privacy laws (Chadwick *et al*., 2020; Rantos *et al*., 2020). Threat intelligence often contains sensitive operational details, such as system configurations, incident response protocols, and user activity logs. Sharing such data can inadvertently expose vulnerabilities, intellectual property, or personal information. This creates reluctance among organizations, especially in highly regulated sectors such as healthcare and finance, to participate in open data sharing. Regulations such as the General Data Protection Regulation (GDPR) in the European Union and the Health Insurance Portability and Accountability Act (HIPAA) in the United States impose strict requirements on how personal and health data must be protected. Any disclosure of personal identifiable information (PII) or protected health information (PHI) must be minimized or authorized, and any breach can lead to severe penalties.

Additionally, the risk of reputational damage, competitive disadvantage, or legal liability further disincentivizes sharing. Organizations fear that disclosing a breach even in anonymized form could erode stakeholder trust or attract regulatory scrutiny. Technical barriers, such as the lack of standard data formats and secure communication protocols, also complicate seamless information exchange (Costin and Eastman, 2019; Spanakis *et al*., 2021). These limitations have led to fragmented threat intelligence ecosystems, where crucial insights remain siloed and underutilized.

To overcome these challenges, privacy-preserving technologies such as homomorphic encryption, secure multiparty computation, and federated learning are gaining traction. These tools enable organizations to share and analyze encrypted threat data without revealing sensitive content, thus aligning cybersecurity objectives with legal and privacy obligations. Integrating such technologies into AI-driven threat intelligence systems could revolutionize collaborative cyber defense, making it both effective and compliant (Tanikonda *et al*., 2022; Fakhar and Haile, 2022).

Threat intelligence sharing is fundamental to collective cybersecurity resilience. While its benefits are clear particularly in enabling real-time, cross-organizational detection and mitigation of cyber threats current privacy, legal, and operational constraints limit its widespread adoption (Riebe *et al*., 2021; Marapu, 2022). Addressing these challenges through technological innovation and regulatory harmonization is critical to unlocking the full value of shared threat intelligence in the digital age.

2.2 Privacy Challenges in Cybersecurity Data Sharing

As cyber threats grow in sophistication and frequency, sharing cybersecurity-related data across organizations has become increasingly vital to building collective defenses as shown in figure 1. Through collaborative threat intelligence sharing, entities can identify common vulnerabilities, detect emerging attack patterns, and respond more swiftly to incidents (Wagner *et al*., 2019; Schlette *et al*., 2021). However, despite these benefits, organizations face serious privacy challenges that complicate the widespread adoption of open data sharing models. These challenges are rooted in the risks of exposing sensitive or proprietary data, the potential for data misuse or leakage, and stringent regulatory requirements. Balancing the need for transparency with the imperative of confidentiality remains one of the most pressing dilemmas in modern cybersecurity.

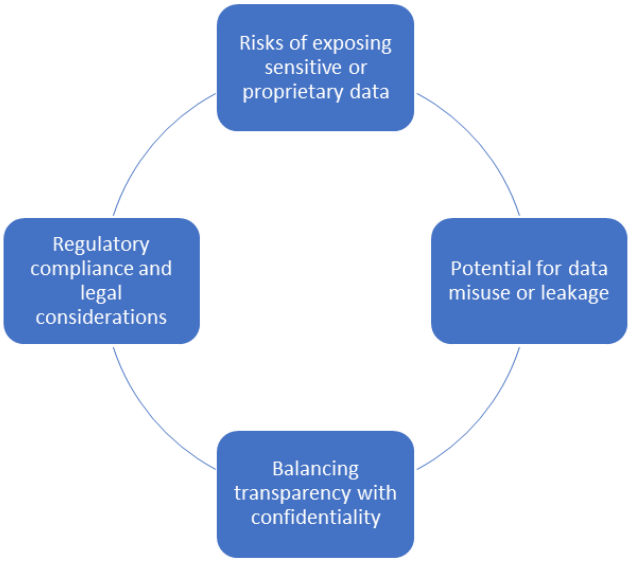

Fig 1: Privacy Challenges in Cybersecurity Data Sharing

One of the primary concerns is the risk of exposing sensitive or proprietary data. Cybersecurity logs and incident reports often contain not only indicators of compromise (IoCs) but also detailed information about internal infrastructure, user behavior, access controls, and system vulnerabilities. Sharing such data without proper safeguards could inadvertently reveal proprietary technologies, business operations, or weak security configurations. Competitors or malicious actors

could exploit this information, potentially leading to intellectual property theft, reputational damage, or further compromise (Basuchoudhary and Searle, 2019; Carnovale *et al*., 2022). Organizations must therefore carefully weigh the value of collaborative threat sharing against the potential cost of data exposure.

In addition to exposure risks, there is a significant potential for data misuse or leakage once information has been shared. Shared threat data, especially when transferred to third parties or cloud platforms, becomes vulnerable to unauthorized access, interception, or exploitation. Even within trusted sharing communities, inadequate access controls or poor data sanitization practices can lead to the unintended disclosure of confidential information (Wong *et al*., 2019; Rajkumar *et al*., 2022). Furthermore, data that is anonymized or pseudonymized may still be susceptible to re-identification through correlation with other datasets. This risk is particularly concerning when shared data includes personally identifiable information (PII) or sensitive behavioral data from users.

Compounding these technical risks are complex regulatory compliance and legal considerations. Data protection laws such as the General Data Protection Regulation (GDPR) in the European Union, the California Consumer Privacy Act (CCPA), and the Health Insurance Portability and Accountability Act (HIPAA) in the United States impose strict guidelines on how sensitive data must be collected, processed, shared, and stored. Non-compliance can result in severe financial penalties and legal liability. For example, GDPR mandates data minimization, user consent for data processing, and the right to be forgotten all of which can limit the scope and duration of cybersecurity data sharing initiatives. These regulatory frameworks are designed to protect user privacy but can inadvertently inhibit timely and effective threat response when organizations are unsure about the legal boundaries of data exchange (Srinivas *et al*., 2019; Olukoya, 2022).

These challenges highlight the necessity of balancing transparency with confidentiality in cybersecurity collaboration. On one hand, openness and timely disclosure of threat information are essential for the rapid dissemination of countermeasures and collective situational awareness. On the other hand, excessive transparency without privacy safeguards can compromise organizational integrity and user trust (Kaufhold *et al*., 2021; Alavizadeh *et al*., 2021). To navigate this tension, organizations must adopt privacy-aware sharing strategies, such as anonymization, access-controlled data lakes, and secure data exchange protocols. However, these methods often reduce data granularity, which may weaken the effectiveness of shared intelligence.

Emerging privacy-preserving technologies, such as homomorphic encryption, secure multiparty computation, and federated learning, offer promising solutions to these challenges. These techniques enable data to be analyzed and processed without exposing its contents, thereby allowing organizations to collaborate on threat detection without compromising privacy or regulatory compliance. By leveraging these innovations, it is possible to create a cybersecurity ecosystem that supports robust information sharing while safeguarding the confidentiality and integrity of sensitive data (Kolluru *et al*., 2019; Loonam *et al*., 2020).

Privacy challenges remain a critical barrier to effective cybersecurity data sharing. Addressing risks related to data exposure, misuse, and legal compliance is essential for building trust and enabling sustainable collaboration. As cyber threats continue to evolve, so too must the technologies and policies that underpin secure and privacy-preserving information sharing.

2.3 Overview of Privacy-Preserving AI Techniques

The growing integration of artificial intelligence (AI) into cybersecurity and data analytics has led to significant advancements in threat detection and decision-making (Raza, 2021; Lekkala *et al*., 2022). However, the increasing reliance on data-intensive AI models also raises pressing concerns about privacy, particularly when sensitive personal or organizational information is involved. This has led to the development and adoption of privacy-preserving AI techniques computational approaches that enable the training and use of machine learning models without compromising the confidentiality of underlying data as shown in figure 2. Among the most prominent of these techniques are differential privacy, secure multiparty computation (SMPC), federated learning, and homomorphic encryption.

Differential privacy is a mathematical framework that provides quantifiable guarantees about the privacy of individuals within a dataset. It ensures that the output of a computation (such as a trained model) does not reveal whether any particular individual's data was included in the input. This is typically achieved by injecting random noise into data queries or model updates. In AI, differential privacy can be applied during both training and inference phases, limiting the ability of adversaries to reverse-engineer or extract sensitive data from model outputs. The main advantage of differential privacy is its formal privacy guarantees, which are particularly useful in regulated sectors like healthcare and finance (Hassan *et al*., 2019; Janghyun *et al*., 2022). However, the trade-off is often a reduction in model accuracy, especially when dealing with small or sparse datasets.

Secure multiparty computation (SMPC) is a cryptographic approach that allows multiple parties to jointly compute a function over their inputs without revealing those inputs to each other. This is particularly useful in collaborative cybersecurity or threat intelligence scenarios where organizations are unwilling to share raw data due to privacy or regulatory concerns. In the SMPC paradigm, data is split into encrypted shares and distributed among participants. Each party performs part of the computation on their share, and the results are combined to produce the final output. The benefit of SMPC lies in its strong security guarantees it can ensure that no single party learns anything beyond the intended result (Zhong *et al*., 2020; Brightwood *et al*., 2022). However, the computational overhead and communication costs can be substantial, making it challenging to apply to complex models or real-time use cases without optimization.

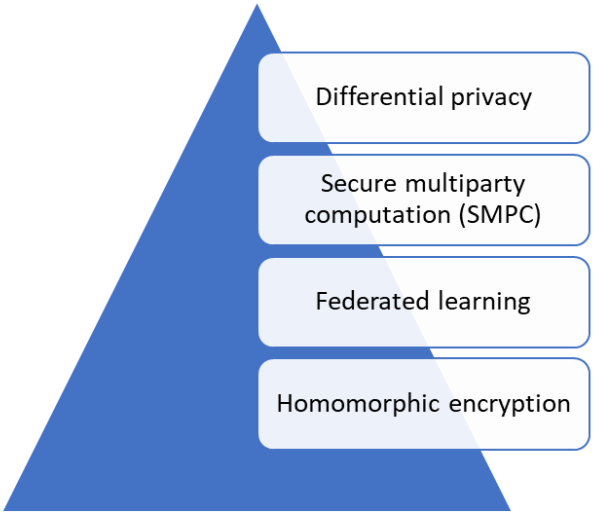

Fig 2: Privacy-Preserving AI Techniques

Federated learning is another widely adopted privacy-preserving technique that allows machine learning models to be trained collaboratively across decentralized devices or servers holding local data samples, without exchanging the raw data itself. Instead, each participating device computes a model update based on its local data and sends only the model parameters (e.g., weight gradients) to a central server, which aggregates them to update a global model. This approach is highly relevant in edge computing and mobile environments, where data resides on numerous distributed devices. Federated learning preserves data locality, reducing privacy risks and bandwidth consumption. Nevertheless, it faces challenges related to model convergence, data heterogeneity, and security threats such as gradient inversion or model poisoning.

Homomorphic encryption (HE) represents a groundbreaking advancement in privacy-preserving computation. HE is a form of encryption that allows computations to be performed directly on encrypted data without requiring decryption. The results, once decrypted, match the outcome of operations performed on plaintext data. This makes it possible to perform machine learning tasks such as inference or even training on encrypted datasets. Homomorphic encryption can be categorized as partially, somewhat, or fully homomorphic depending on the types and complexity of supported operations (Alloghani *et al*., 2019; Marcolla *et al*., 2022). The key advantage of HE is that it enables secure, outsourced computation in untrusted environments, such as cloud platforms or shared threat intelligence hubs, while preserving complete data confidentiality. However, HE is currently constrained by high computational overhead and slow processing speeds, which limit its practical deployment in real-time or large-scale systems.

Privacy-preserving AI techniques offer essential solutions to the growing tension between the utility of data-driven intelligence and the need to protect sensitive information. Differential privacy, SMPC, federated learning, and homomorphic encryption each offer unique advantages and limitations, making them suitable for different applications and deployment scenarios. Continued research and innovation in these techniques will be critical for developing AI systems that are not only intelligent and effective but also ethical, compliant, and trustworthy in the age of ubiquitous data (Shneiderman, 2020; Kaur *et al*., 2022).

2.4 Homomorphic Encryption in Cybersecurity Applications

Homomorphic encryption (HE) is a cryptographic innovation that enables computation on encrypted data without the need for decryption. In the context of cybersecurity, where confidentiality and data integrity are paramount, HE represents a transformative approach to securing sensitive operations, such as threat intelligence sharing, malware detection, and user behavior analysis. As AI and machine learning become increasingly integral to cybersecurity strategies, homomorphic encryption provides a viable mechanism to ensure that data privacy is preserved even during collaborative and outsourced computations (Khurana and Kaul, 2019; Palle and Punitha, 2021).

Homomorphic encryption comes in three primary forms: partially, somewhat, and fully homomorphic encryption (FHE). Partially homomorphic encryption supports only one type of mathematical operation (either addition or multiplication) an unlimited number of times. For example, RSA supports multiplicative operations, while the Paillier scheme supports additive ones. These are efficient and widely used for basic secure data aggregation tasks. Somewhat homomorphic encryption (SHE) enables a limited number of both addition and multiplication operations, making it suitable for certain machine learning algorithms with shallow computation graphs. However, it lacks the flexibility needed for more complex AI tasks. Fully homomorphic encryption (FHE), the most powerful form, supports arbitrary computation on ciphertexts, allowing any combination and depth of operations (Chillotti *et al*., 2020; Mittal and Ramkumar, 2021). This capability makes FHE ideal for enabling encrypted machine learning model inference and training, but it comes at a cost of significant computational overhead and latency.

One of the most promising uses of HE in cybersecurity is in secure computation for threat pattern recognition. Organizations often need to analyze sensitive telemetry data such as login attempts, network flows, or system logs to detect anomalies or malicious behavior. HE allows this data to remain encrypted throughout the analysis process. For instance, a centralized AI model hosted on a third-party platform can process encrypted log entries from different organizations and identify encrypted patterns indicative of coordinated attacks, without ever accessing the raw data. This

capability is particularly valuable for detecting threats that span multiple entities or sectors, such as advanced persistent threats (APTs) and distributed denial-of-service (DDoS) attacks (Bahrami *et al*., 2019; Ren *et al*., 2022).

HE also supports encrypted model inference, where a user can submit encrypted data to an AI model and receive an encrypted result. In this paradigm, neither the data owner nor the model host gains visibility into each other's assets. This is especially useful for managed security services or cloud-based cybersecurity platforms, where organizations prefer not to expose internal datasets, and providers want to protect their proprietary models. Furthermore, homomorphic encryption facilitates encrypted input/output (I/O) operations, ensuring that the entire computational pipeline from input to inference to output remains confidential. This full-stack protection can be crucial for sectors like finance, defense, and healthcare, where data sensitivity is extremely high.

HE's most compelling advantage lies in its suitability for collaborative environments with untrusted participants. In multi-organizational cybersecurity collaborations, such as information sharing and analysis centers (ISACs) or cross-border cyber defense alliances, stakeholders may be hesitant to share raw threat intelligence due to concerns about trust, compliance, or competition. Homomorphic encryption allows these organizations to contribute encrypted threat data to a shared analytical model or repository, where meaningful computation can be performed without exposing the underlying inputs. The results still encrypted can then be returned and decrypted locally, enabling each party to benefit from collective analysis while maintaining strict privacy controls.

Despite its potential, the practical adoption of homomorphic encryption in cybersecurity is currently limited by performance challenges. FHE operations are computationally intensive and require significant processing time and memory resources. However, ongoing advancements in cryptographic schemes, hardware acceleration, and algorithm optimization are steadily improving feasibility. Libraries such as Microsoft SEAL, IBM HELib, and Google's TFHE offer practical implementations, and several research initiatives are exploring hybrid approaches that combine HE with other privacy-preserving methods to balance efficiency and security (Breeding, 2019; Iqbal *et al*., 2022).

Homomorphic encryption is a powerful enabler of privacy-preserving AI in cybersecurity. Its ability to perform secure computations on encrypted data unlocks new possibilities for threat detection, secure inference, and multi-party collaboration. While current performance limitations remain a barrier to widespread deployment, rapid progress in this field signals a future where homomorphic encryption will become a standard component of secure, intelligent cybersecurity infrastructures.

2.5 System Architecture for Privacy-Preserving Threat Intelligence Sharing

The advancement of privacy-preserving techniques has enabled a new generation of cybersecurity architectures that allow for collaborative threat intelligence sharing without compromising data confidentiality. Central to these architectures is the integration of homomorphic encryption (HE) and secure AI frameworks, which together support the secure exchange and analysis of sensitive threat data across multiple organizations (Shrestha and Kim, 2019; Murugesan *et al*., 2021). A privacy-preserving system architecture designed for threat intelligence sharing typically comprises four key stages; data collection and encryption at the source, encrypted model training or inference, application of AI models on encrypted inputs, and secure aggregation and collaborative analysis.

The first component of this architecture is data collection and encryption at the source. In a distributed cybersecurity ecosystem, individual organizations generate telemetry data from various endpoints, including firewalls, intrusion detection systems (IDS), and network traffic logs. These datasets may include sensitive indicators of compromise (IoCs), user behavior analytics, and system anomalies. Before sharing this data with any central authority or collaborative platform, it must be encrypted using homomorphic encryption schemes. Encryption at the source ensures that raw data never leaves the organizational boundary in a readable form, significantly reducing the risk of leakage, misuse, or regulatory non-compliance. This approach aligns with data protection mandates such as GDPR and HIPAA, making the system legally robust.

Once encrypted, the data can be used in model training or inference operations without decryption. Depending on the design, organizations may contribute their encrypted data to a centralized secure enclave, or leverage decentralized federated learning approaches enhanced with homomorphic encryption. In the centralized model, the encrypted data is used to train AI models within a secure computation environment. Alternatively, if models are already trained, encrypted inference can be performed, where incoming encrypted threat data is processed to predict malicious activity, anomalies, or other security threats. Homomorphic encryption allows these computations to occur without ever revealing the plaintext, preserving end-to-end privacy.

The next architectural layer involves the application of AI models on encrypted inputs, particularly for core cybersecurity tasks such as anomaly detection, malware classification, and intrusion identification. These AI models typically based on convolutional neural networks (CNNs), recurrent neural networks (RNNs), or ensemble methods can be tailored to operate on features derived from encrypted threat logs (Abiodun *et al*., 2019; Khan *et al*., 2020). For example, an AI model trained to detect behavioral anomalies in login patterns can evaluate encrypted sequences of login timestamps, IP addresses, and device IDs. Likewise, a malware classification system can process encrypted binary features extracted from suspicious files to determine potential threats. The critical innovation here is the ability to run inference directly on encrypted inputs, which ensures that no party involved in the model computation process gains access to raw data.

The final and perhaps most complex element of the system architecture is the secure aggregation and collaborative analysis of encrypted threat data. This phase is especially important in multi-party environments, such as sector-specific ISACs or international cyber alliances, where organizations contribute data to a shared repository. Aggregated encrypted data can be analyzed collectively to uncover macro-level trends, coordinated attacks, or shared vulnerabilities. Secure multi-party computation (SMPC) protocols or homomorphically encrypted aggregation functions can be used to compute statistical summaries, correlation metrics, or pattern similarities across datasets, all without decrypting individual contributions. Insights derived

from such aggregated analytics can then be shared back with participants in encrypted form, or selectively decrypted based on predefined access policies.

To support this system architecture, secure key management, encrypted communication protocols, and trusted execution environments (TEEs) may also be integrated to provide additional layers of security. These components ensure that encryption keys are not compromised and that computations are conducted in tamper-proof settings.

In conclusion, a robust system architecture for privacy-preserving threat intelligence sharing must enable secure data handling from collection to analysis. By encrypting data at the source and enabling encrypted AI computation and aggregation, such architectures empower organizations to collaborate effectively while maintaining strict privacy, compliance, and trust (Wu, 2020; Deebak *et al*., 2022). This paradigm represents a significant advancement in cybersecurity, offering a scalable and secure foundation for collective defense in the digital age.

2.6 Performance Evaluation

The implementation of privacy-preserving AI using homomorphic encryption (HE) in threat intelligence sharing has begun to move from theoretical exploration to real-world application across sectors such as finance, healthcare, and critical infrastructure. These domains demand both high security and strong data privacy, making them ideal for evaluating the practical viability of homomorphic encryption in cybersecurity (Compagnucci *et al*., 2019; Hamza *et al*., 2022). Through case studies and performance evaluations, researchers and practitioners assess key metrics such as accuracy, latency, computational overhead, and system scalability essential for gauging the trade-offs between privacy, efficiency, and threat detection performance.

In the financial sector, institutions face continuous threats including phishing, fraud, and ransomware. A consortium of banks in Europe piloted a privacy-preserving collaborative threat detection system using fully homomorphic encryption to share encrypted fraud patterns and behavioral transaction logs. The AI models, specifically trained for fraud detection using federated learning combined with HE, could identify cross-institutional anomalies without revealing customer transaction data. Accuracy remained within 2–3% of traditional models (achieving over 90%), but latency increased significantly up to fivefold primarily due to encryption and decryption operations. While computational overhead remained manageable through the use of hardware acceleration (e.g., GPUs and specialized HE libraries like Microsoft SEAL), real-time applicability was limited to batch processing rather than live streaming analytics.

In the healthcare domain, where privacy laws such as HIPAA strictly govern the handling of patient data, researchers deployed HE-based models for detecting cyber threats in hospital networks, such as unauthorized access to electronic health records (EHRs). By encrypting access logs and applying LSTM-based anomaly detection models trained on encrypted data, the system detected over 85% of anomalies while maintaining full data confidentiality. Compared to unencrypted baselines, inference latency increased by approximately 300%, though this was acceptable in the context of periodic compliance auditing rather than urgent real-time response. Importantly, this approach enabled hospitals to share encrypted incident data with central health authorities for threat correlation, without violating patient privacy.

In critical infrastructure sectors such as energy and transportation, where systems are often targeted by state-sponsored actors, secure and private monitoring is vital. A case study in a national energy grid involved homomorphically encrypting SCADA (Supervisory Control and Data Acquisition) logs and feeding them into a centralized AI-driven threat monitoring platform. The platform could perform secure model inference to identify anomalies such as unusual voltage fluctuations or unauthorized device communication (Ahmed *et al*., 2019; Fang *et al*., 2020). Although detection accuracy was comparable to plaintext models (with only a marginal decrease of about 1.5%), the system faced significant limitations in scalability and response time, with inference taking several seconds per instance due to the computationally heavy nature of FHE.

Performance benchmarks across these deployments illustrate the current boundaries of HE-based AI systems. While accuracy can be preserved close to unencrypted counterparts, latency and computational overhead are significantly higher. In most cases, latency ranged from 2x to 10x longer, depending on the complexity of the AI model and the size of encrypted input. Memory usage and energy consumption were also higher, impacting feasibility for edge deployment.

Comparisons with unencrypted systems clearly demonstrate the trade-offs involved. Unencrypted AI offers faster processing and lower resource consumption but sacrifices data privacy and may violate legal standards when data is shared across organizational boundaries. Homomorphic encryption, in contrast, enables compliant and secure collaboration, but at the cost of reduced performance.

These case studies highlight a fundamental trade-off between privacy, efficiency, and detection performance. In environments where privacy is paramount, such as healthcare, the trade-off is acceptable. However, in latency-sensitive contexts like live intrusion detection in critical infrastructure, the performance penalties may hinder adoption unless optimized further. Hybrid approaches—combining HE with trusted execution environments (TEEs) or differential privacy—may offer a path forward, balancing privacy and performance more effectively.

In conclusion, real-world deployments of HE in cybersecurity demonstrate its promise and limitations. While homomorphic encryption offers unmatched privacy guarantees, further research is needed to reduce computational burdens and improve scalability. As hardware and cryptographic techniques evolve, HE-based AI systems are likely to become more practical, enabling widespread, privacy-preserving threat intelligence sharing across diverse sectors (Xu *et al*., 2021; Podschwadt *et al*., 2022).

2.7 Challenges and Future Research Directions

Homomorphic encryption (HE) has emerged as a powerful tool in enabling privacy-preserving AI for cybersecurity, particularly in scenarios involving threat intelligence sharing across organizational boundaries. By allowing computations to be performed directly on encrypted data, HE ensures the confidentiality of sensitive information throughout the analysis process. However, despite its theoretical appeal and growing real-world applicability, several critical challenges must be addressed to unlock its full potential in cybersecurity operations. These challenges span computational cost and scalability, model compatibility with encrypted data,

robustness to adversarial threats, and the need for standardization and interoperability as shown in figure 3.

One of the most prominent limitations of homomorphic encryption is its computational cost and scalability. Fully homomorphic encryption (FHE), in particular, requires significantly more computational resources than traditional plaintext operations. The processing time for even simple arithmetic operations can be orders of magnitude higher when performed on ciphertexts. This computational burden leads to increased latency and energy consumption, making real-time deployment in high-speed cybersecurity environments such as intrusion detection systems or endpoint protection challenging. Additionally, the overhead grows substantially with the complexity of the AI models and the size of input data. Research into more efficient encryption schemes, hardware acceleration (e.g., GPUs, FPGAs), and parallel processing is essential to enhance scalability and improve the practicality of HE for large-scale deployments.

Fig 3: Challenges and Future Research Directions

Another significant challenge involves model compatibility and training over encrypted data. While inference on encrypted inputs is feasible with current HE schemes, training machine learning models directly on encrypted data remains a largely unresolved problem due to the limitations in supporting non-linear operations such as activation functions. Most current implementations rely on training in plaintext and deploying the model for encrypted inference, which introduces trust issues during the training phase. Future research must focus on developing HE-friendly model architectures and training algorithms that can operate efficiently on encrypted datasets. Techniques such as approximating non-linear functions and using low-degree polynomials have shown promise, but they often compromise model expressiveness and accuracy (Denuit *et al*., 2019; Cramer *et al*., 2020).

In the context of cybersecurity, enhancing robustness against adversarial threats in encrypted environments is another pressing concern. As machine learning models become increasingly targeted by adversarial attacks such as data poisoning, evasion, or model inversion it is imperative to ensure that privacy-preserving models are not only secure in terms of data confidentiality but also resilient to adversarial manipulation. The encryption layer may mask inputs from the model host, but it does not inherently prevent attacks that exploit model vulnerabilities or input-output behavior. Designing encrypted models with built-in adversarial defenses, such as robust training or anomaly detection mechanisms, is a key direction for future research. Moreover, hybrid security frameworks that integrate HE with secure enclaves or differential privacy may offer layered protection against both data leakage and model attacks.

Another crucial area of development lies in standardization and interoperability for cross-organizational threat sharing. Current implementations of homomorphic encryption and privacy-preserving AI often lack consistent standards, making it difficult for different organizations or sectors to collaborate effectively. The absence of unified protocols for key exchange, encrypted model formats, and secure communication hinders widespread adoption. Additionally, variations in regulatory requirements and data schemas across jurisdictions complicate interoperability. Developing standardized APIs, encryption libraries, and regulatory-aligned frameworks will be vital for enabling scalable, compliant, and interoperable threat intelligence ecosystems. Initiatives by organizations such as the HomomorphicEncryption.org consortium and national cybersecurity agencies are beginning to address this need, but broader collaboration between academia, industry, and government is required (Hsu *et al*., 2020; Belykh *et al*., 2022; Stripelis *et al*., 2022).

While homomorphic encryption offers a compelling solution to the privacy challenges in AI-driven cybersecurity, its current limitations in computational efficiency, model integration, robustness, and standardization must be addressed through targeted research and development. Innovations in cryptography, machine learning, and systems architecture alongside policy harmonization and industry standards will be necessary to bring HE-based cybersecurity systems from pilot projects to mainstream deployment. The future of privacy-preserving threat intelligence sharing depends on overcoming these challenges to achieve a balance between data security, operational efficiency, and collaborative effectiveness.

3. Conclusion

Homomorphic encryption (HE) represents a groundbreaking advancement in AI-driven cybersecurity, offering a robust solution to the enduring challenge of preserving data privacy while enabling collaborative threat intelligence sharing. By allowing encrypted data to be processed without decryption, HE ensures that sensitive information such as indicators of compromise, user behavior, and system logs remains confidential throughout the analysis lifecycle. This capability is particularly vital in high-stakes sectors like finance, healthcare, and critical infrastructure, where regulatory requirements and trust barriers often hinder the open exchange of threat data.

The integration of HE into cybersecurity systems brings several key benefits. It enables secure AI inference and, increasingly, encrypted training, facilitating collaborative analytics across untrusted domains. It protects proprietary models and sensitive inputs while supporting compliance with data protection laws like GDPR and HIPAA. Moreover, HE empowers organizations to contribute to shared defense ecosystems without compromising confidentiality or competitive integrity.

However, limitations remain. High computational overhead, latency, and limited compatibility with complex machine learning models pose significant obstacles to real-time deployment and scalability. Additionally, challenges related to adversarial robustness, model optimization, and standardization still need to be addressed before HE-based systems can become mainstream.

Despite these challenges, homomorphic encryption is poised to play a pivotal role in the future of cybersecurity. Its unique ability to facilitate privacy-preserving collaboration makes it a critical enabler of cross-organizational threat intelligence platforms. As cyber threats evolve and data privacy becomes increasingly vital, there is a compelling need for continued innovation, including more efficient cryptographic schemes, privacy-preserving AI architectures, and interoperable frameworks. Broad cross-sector collaboration among academia, industry, and government will be essential to advance HE from research labs into widespread, impactful cybersecurity deployments.

4. References

1. Abiodun OI, Jantan A, Omolara AE, Dada KV, Umar AM, Linus OU, *et al*. Comprehensive review of artificial neural network applications to pattern recognition. IEEE Access. 2019;7:158820-46.
2. Ahmed A, Krishnan VV, Foroutan SA, Touhiduzzaman M, Rublein C, Srivastava A, *et al*. Cyber physical security analytics for anomalies in transmission protection systems. IEEE Trans Ind Appl. 2019;55(6):6313-23.
3. Alavizadeh H, Jang-Jaccard J, Enoch SY, Al-Sahaf H, Welch I, Camtepe SA, *et al*. A survey on threat situation awareness systems: framework, techniques, and insights. arXiv [Preprint]. 2021 [cited 2025 Aug 8]. Available from: https://arxiv.org/abs/2110.15747.
4. Alloghani M, Alani MM, Al-Jumeily D, Baker T, Mustafina J, Hussain A, *et al*. A systematic review on the status and progress of homomorphic encryption technologies. J Inf Secur Appl. 2019;48:102362.
5. Asghar MR, Hu Q, Zeadally S. Cybersecurity in industrial control systems: issues, technologies, and challenges. Comput Netw. 2019;165:106946.
6. Bahrami PN, Dehghantanha A, Dargahi T, Parizi RM, Choo KKR, Javadi HH. Cyber kill chain-based taxonomy of advanced persistent threat actors: analogy of tactics, techniques, and procedures. J Inf Process Syst. 2019;15(4):865-89.
7. Basuchoudhary A, Searle N. Snatched secrets: cybercrime and trade secrets modelling a firm's decision to report a theft of trade secrets. Comput Secur. 2019;87:101591.
8. Belykh I, Bocian M, Champneys A, Daley K, Jeter R, Macdonald J, *et al*. The London millennium footbridge revisited: emergent instability without synchronization. SIAM News. 2022;55(3).
9. Breeding M. Protecting privacy on library websites: critical technologies and implementation trends. Chicago: ALA TechSource; 2019.
10. Brightwood S, Olaoye G, Andrew J. Strengthening network privacy via secure multi-party computation in cloud computing environments. [place unknown: publisher unknown]; 2022.
11. Carnovale S, Carnovale J, Strub D, Szalwinski A, Marek J. Guardians of intellectual property in the 21st century: the global supply chain industry. Rutgers Bus Rev. 2022;7(1):1-21.
12. Chillotti I, Gama N, Georgieva M, Izabachène M. TFHE: fast fully homomorphic encryption over the torus. J Cryptol. 2020;33(1):34-91.
13. Compagnucci MC, Meszaros J, Minssen T, Arasilango A, Ous T, Rajarajan M. Homomorphic encryption: the 'Holy Grail' for big data analytics and legal compliance in the pharmaceutical and healthcare sector? EPLR. 2019;3:144.
14. Costin A, Eastman C. Need for interoperability to enable seamless information exchanges in smart and sustainable urban systems. J Comput Civ Eng. 2019;33(3):04019008.
15. Cramer B, Stradmann Y, Schemmel J, Zenke F. The Heidelberg spiking data sets for the systematic evaluation of spiking neural networks. IEEE Trans Neural Netw Learn Syst. 2020;33(7):2744-57.
16. Cruickshank P, Rassler D. A view from the CT foxhole: a virtual roundtable on COVID-19 and counterterrorism with Audrey Kurth Cronin, Lieutenant General (Ret) Michael Nagata, Magnus Ranstorp, Ali Soufan, and Juan Zarate. CTC Sentinel. 2020;13(6):1-15.
17. Deebak BD, Memon FH, Dev K, Khowaja SA, Qureshi NMF. AI-enabled privacy-preservation phrase with multi-keyword ranked searching for sustainable edge-cloud networks in the era of industrial IoT. Ad Hoc Netw. 2022;125:102740.
18. Denuit M, Hainaut D, Trufin J. Generalized additive models (GAMs). In: Effective statistical learning methods for actuaries I: GLMs and extensions. Cham: Springer; 2019. p. 253-327.
19. Fakhar M, Haile A. AI for threat intelligence: enhancing adaptive cyber defense against persistent attacks. [place unknown: publisher unknown]; 2022.
20. Fang L, Li Y, Liu Z, Yin C, Li M, Cao ZJ. A practical model based on anomaly detection for protecting medical IoT control services against external attacks. IEEE Trans Ind Inform. 2020;17(6):4260-9.
21. Guembe B, Azeta A, Misra S, Osamor VC, Fernandez-Sanz L, Pospelova V. The emerging threat of AI-driven cyber attacks: a review. Appl Artif Intell. 2022;36(1):2037254.
22. Gupta S, Joseph S, Sasidharan D. The challenges in leveraging cyber threat intelligence. [place unknown: publisher unknown]; 2021.
23. Hamza R, Hassan A, Ali A, Bashir MB, Alqhtani SM, Tawfeeg TM, *et al*. Towards secure big data analysis via fully homomorphic encryption algorithms. Entropy. 2022;24(4):519.
24. Hamza R, Hassan A, Ali A, Bashir MB, Alqhtani SM, Tawfeeg TM, *et al*. Towards secure big data analysis via fully homomorphic encryption algorithms. Entropy. 2022;24(4):519.
25. Hassan MU, Rehmani MH, Chen J. Differential privacy techniques for cyber physical systems: a survey. IEEE Commun Surv Tutor. 2020;22(1):746-89.
26. Hicks KH, Friend AH, Federici J, Shah H, Donahoe M, Conklin M, *et al*. Other means. [place unknown: publisher unknown]; 2019.
27. Hsu A, Khoo W, Goyal N, Wainstein M. Next-generation digital ecosystem for climate data mining and knowledge discovery: a review of digital data collection technologies. Front Big Data. 2020;3:29.

28. Iqbal Y, Tahir S, Tahir H, Khan F, Saeed S, Almuhaideb AM, *et al*. A novel homomorphic approach for preserving privacy of patient data in telemedicine. Sensors. 2022;12(12):4432.
29. Janghyun K, Barry H, Tianzhen H. A review of preserving privacy in data collected from buildings with differential privacy. J Build Eng. 2022;56:104724.
30. Jimmy F. Emerging threats: the latest cybersecurity risks and the role of artificial intelligence in enhancing cybersecurity defenses. Valley Int J Digit Libr. 2021;1:564-74.
31. Kaufhold MA, Fromm J, Riebe T, Mirbabaie M, Kuehn P, Basyurt AS, *et al*. CYWARN: strategy and technology development for cross-platform cyber situational awareness and actor-specific cyber threat communication. In: Mensch und Computer 2021-Workshopband. Bonn: Gesellschaft für Informatik eV; 2021. p. 10-18420.
32. Kaur D, Uslu S, Rittichier KJ, Durresi A. Trustworthy artificial intelligence: a review. ACM Comput Surv. 2022;55(2):1-38.
33. Khan A, Sohail A, Zahoora U, Qureshi AS. A survey of the recent architectures of deep convolutional neural networks. Artif Intell Rev. 2020;53:5455-516.
34. Khurana R, Kaul D. Dynamic cybersecurity strategies for AI-enhanced ecommerce: a federated learning approach to data privacy. Appl Res Artif Intell Cloud Comput. 2019;2(1):32-43.
35. Kolluru V, Mungara S, Chintakunta AN. Securing the IoT ecosystem: challenges and innovations in smart device cybersecurity. Int J Cryptogr Inf Secur. 2019;9(2):10-5121.
36. Lekkala S, Avula R, Gurijala P. Big data and AI/ML in threat detection: a new era of cybersecurity. J Artif Intell Big Data. 2022;2(1):32-48.
37. Loonam J, Zwiegelaar J, Kumar V, Booth C. Cyber-resiliency for digital enterprises: a strategic leadership perspective. IEEE Trans Eng Manag. 2020;69(6):3757-70.
38. Manda JK. Cybersecurity automation in telecom: implementing automation tools and technologies to enhance cybersecurity incident response and threat detection in telecom operations. Adv Comput Sci. 2021;4(1).
39. Marapu NR. Future-proofing national cybersecurity: the role of AI in proactive threat hunting and framework optimization. Int J Artif Intell Data Sci Mach Learn. 2022;3(4):27-37.
40. Kacheru G. The future of cyber defence: predictive security with artificial intelligence. Int J Adv Res Basic Eng Sci Technol. 2021;7(12):46-55.
41. Marcolla C, Sucasas V, Manzano M, Bassoli R, Fitzek FH, Aaraj N. Survey on fully homomorphic encryption, theory, and applications. Proc IEEE. 2022;110(10):1572-609.
42. Lewechi FE. Zero trust framework for AI-enabled digital twin: integrating security, fairness, and compliance monitoring. Int J Multidiscip Res Growth Eval. 2023;4(6):1339-1347. doi:10.54660/IJMRGE.2023.4.6.1339-1347.
43. Mittal S, Ramkumar KR. Research perspectives on fully homomorphic encryption models for cloud sector. J Comput Secur. 2021;29(2):135-60.
44. Murugesan A, Saminathan B, Al-Turjman F, Kumar RL. Analysis on homomorphic technique for data security in fog computing. Trans Emerg Telecommun Technol. 2021;32(9):e3990.
45. Olukoya O. Assessing frameworks for eliciting privacy & security requirements from laws and regulations | Computers & Security | 117 | 102697.
46. Palle R, Punitha A. Privacy-preserving homomorphic enc ryption schemes for machine learning in the cloud. ESP J Eng Technol Adv. 2021.
47. Perumallaplli R. AI in real-time cybersecurity: enhancing threat detection in dynamic networks. SSRN [Preprint]. 2019 [cited 2025 Aug 8]. Available from: https://ssrn.com/abstract=5228547.
48. Podschwadt R, Takabi D, Hu P, Rafiei MH, Cai Z. A survey of deep learning architectures for privacy-preserving machine learning with fully homomorphic encryption. IEEE Access. 2022;10:117477-500.
49. Rajkumar V, Prakash M, Vennila V. Secure data sharing with confidentiality, integrity and access control in cloud environment. Comput Syst Sci Eng. 2022;40(2).
50. Rantos K, Spyros A, Papanikolaou A, Kritsas A, Ilioudis C, Katos V. Interoperability challenges in the cybersecurity information sharing ecosystem. Computers. 2020;9(1):18.
51. Raza H. Proactive cyber defense with AI: enhancing risk assessment and threat detection in cybersecurity ecosystems. [place unknown: publisher unknown]; 2021.
52. Reddy ARP. The role of artificial intelligence in proactive cyber threat detection in cloud environments. NeuroQuantology. 2021;19(12):764-73.
53. Lewechi FE. Zero trust framework for AI-enabled digital twin: integrating security, fairness, and compliance monitoring. Int J Multidiscip Res Growth Eval. 2023;4(6):1339-1347. doi:10.54660/IJMRGE.2023.4.6.1339-1347.
54. Ren Y, Xiao Y, Zhou Y, Zhang Z, Tian Z. CSKG4APT: a cybersecurity knowledge graph for advanced persistent threat organization attribution. IEEE Trans Knowl Data Eng. 2022;35(6):5695-709.
55. Repetto M, Carrega A, Rapuzzi R. An architecture to manage security operations for digital service chains. Future Gener Comput Syst. 2021;115:251-66.
56. Riebe T, Kaufhold MA, Reuter C. The impact of organizational structure and technology use on collaborative practices in computer emergency response teams: an empirical study. Proc ACM Hum-Comput Interact. 2021;5(CSCW2):1-30.
57. Sana MU, Li Z, Javaid F, Liaqat HB, Ali MU. Enhanced security in cloud computing using neural network and encryption. IEEE Access. 2021;9:145785-99.
58. Schlette D, Caselli M, Pernul G. A comparative study on cyber threat intelligence: the security incident response perspective. IEEE Commun Surv Tutor. 2021;23(4):2525-56.
59. Seker E. Cyber threat intelligence understanding fundamentals. Milli Təhlükəsizlik Və Hərbi Elmlər Elmi-Praktiki Jurnal. 2019:75-8.
60. Lewechi F. Blockchain-orchestrated IAM for multi-cloud AI systems: identify federation with ethical controls. Int J Multidiscip Evolut Res. 2023;4(2):139–149. doi:10.54660/IJMER.2023.4.2.139-149.
61. Shahjee D, Ware N. Integrated network and security operation center: a systematic analysis. IEEE Access. 2022;10:27881-98.

62. Shneiderman B. Bridging the gap between ethics and practice: guidelines for reliable, safe, and trustworthy human-centered AI systems. ACM Trans Interact Intell Syst. 2020;10(4):1-31.
63. Shrestha R, Kim S. Integration of IoT with blockchain and homomorphic encryption: challenging issues and opportunities. In: Advances in computers. Vol. 115. Amsterdam: Elsevier; 2019. p. 293-331.
64. Lewechi F. Blockchain-orchestrated IAM for multi-cloud AI systems: identify federation with ethical controls. Int J Multidiscip Evolut Res. 2023;4(2):139–149. doi:10.54660/IJMER.2023.4.2.139-149.
65. Spanakis EG, Sfakianakis S, Bonomi S, Ciccotelli C, Magalini S, Sakkalis V. Emerging and established trends to support secure health information exchange. Front Digit Health. 2021;3:636082.
66. Srinivas J, Das AK, Kumar N. Government regulations in cyber security: framework, standards and recommendations. Future Gener Comput Syst. 2019;92:178-88.
67. Steingartner W, Galinec D, Kozina A. Threat defense: cyber deception approach and education for resilience in hybrid threats model. Symmetry. 2021;13(4):597.
68. Stripelis D, Gupta U, Saleem H, Dhinagar N, Ghai T, Anastasiou RC, *et al*. Secure & private federated neuroimaging. arXiv [Preprint]. 2022 [cited 2025 Aug 8]. Available from: https://arxiv.org/abs/2205.05249.
69. Sundaramurthy SK, Ravichandran N, Inaganti AC, Muppalaneni R. AI-powered operational resilience: building secure, scalable, and intelligent enterprises. Artif Intell Mach Learn Rev. 2022;3(1):1-10.
70. Tadi V. Integrating advanced data engineering with machine learning and AI for early detection and mitigation of cyber threats in real-time criminal investigations. J Sci Eng Res. 2022;9(3):216-32.
71. Tanikonda A, Pandey BK, Peddinti SR, Katragadda SR. Advanced AI-driven cybersecurity solutions for proactive threat detection and response in complex ecosystems. J Sci Technol. 2022;3(1).
72. Tounsi W, Rais H. A survey on technical threat intelligence in the age of sophisticated cyber attacks. Comput Secur. 2018;72:212-33.
73. Tounsi W. What is cyber threat intelligence and how is it evolving? In: Cyber-vigilance and digital trust: cyber security in the era of cloud computing and IoT. Hoboken: Wiley; 2019. p. 1-49.
74. Van Haastrecht M, Golpur G, Tzismadia G, Kab R, Priboi C, David D, *et al*. A shared cyber threat intelligence solution for SMEs. Electronics. 2021;10(23):2913.
75. Wagner TD, Mahbub K, Palomar E, Abdallah AE. Cyber threat intelligence sharing: survey and research directions. Comput Secur. 2019;87:101589.
76. Chadwick DW, Fan W, Costantino G, De Lemos R, Di Cerbo F, Herwono I, *et al*. A cloud-edge based data security architecture for sharing and analysing cyber threat information. Future Gener Comput Syst. 2020;102:710-22.
77. Wong WP, Tan HC, Tan KH, Tseng ML. Human factors in information leakage: mitigation strategies for information sharing integrity. Ind Manag Data Syst. 2019;119(6):1242-67.
78. Wu Y. Cloud-edge orchestration for the Internet of Things: architecture and AI-powered data processing. IEEE Internet Things J. 2020;8(16):12792-805.
79. Xu R, Baracaldo N, Joshi J. Privacy-preserving machine learning: methods, challenges and directions. arXiv [Preprint]. 2021 [cited 2025 Aug 8]. Available from: https://arxiv.org/abs/2108.04417.
80. Zhong H, Sang Y, Zhang Y, Xi Z. Secure multi-party computation on blockchain: an overview. In: Parallel Architectures, Algorithms and Programming: 10th International Symposium, PAAP 2019; 2019 Dec 12-14; Guangzhou, China. Singapore: Springer; 2020. p. 452-60.