PRIVACY-PRESERVING THREAT SHARING ACROSS ORGANIZATIONS

Rahul Bhardwaj

B.E. 4th Year, Computer Science & Engineering Department, Chandigarh University, Punjab

Pooja

B.E. 4th Year, Computer Science & Engineering Department, Chandigarh University, Punjab

Ritik Raushan

B.E. 4th Year, Computer Science & Engineering Department, Chandigarh University, Punjab

Akanksha Jain

B.E. 4th Year, Computer Science & Engineering Department, Chandigarh University, Punjab

Azhar Ashraf Gadoo

Professor, Department of, Computer Science & Engineering, Chandigarh University, Punjab

ABSTRACT –

Cybersecurity threats have become quite sophisticated, and organizations depend on real-time threat intelligence sharing to protect themselves against the rise of attacks. However, privacy, data confidentiality and competitive risks often restrict their collaboration to the data exchange only. In this paper one, we present a privacy-preserving threat-sharing framework allowing parties to exchange sensitive threat intelligence information while preventing sensitive internal information leak. only get access to the raw data, while aggregated threat data can be shared with lead analytics. We explore its applicability in threat-sharing within varying contexts, showing organizations manners of leveraging aggregated intelligence without revealing avenues for proprietary or sensitive data compromise. We show that the use of privacy-preserving mechanisms can greatly facilitate cross-organizational collaboration for cybersecurity and can be compliant with regulatory and legal obligations. This paper provides insights into the broader discussion of secure cyber defence strategies, stressing the role of privacy in promoting collaboration against cyber threats.

Keywords: Cybersecurity, Threat Intelligence Sharing, Privacy-Preserving Framework, Cryptographic Techniques, Differential Privacy, Secure Multi-Party Computation (MPC), Cross- Organizational Collaboration.

I. INTRODUCTION

With the world shifting to a digital-first approach, Cyberspace has certainly evolved as well — Cybersecurity threats have become more advanced and widespread, affecting businesses from every industry. To protect themselves effectively against such threats, organizations necessarily rely on threat intelligence sharing, in which they exchange information about cyberattacks, vulnerabilities, and other malicious activities. Together, such elements enable organizations to detect, respond, and recover from security incidents before they become catastrophic, ultimately driving improved security performance across the organization.

But notwithstanding the value of threat intelligence sharing, open exchange of threat information faces significant hurdles: privacy issues, legal and regulatory constraints, competitive risk, and data sensitivity — all serve to inhibit organizations from freely exchanging threat information. Organizations are afraid that the threat intelligence they contribute could risk leaking anything from proprietary developments or exposing internal weaknesses to breaking compliance requirements such as GDPR, CCPA or others industry-specific ones. All these issues have created a trust deficit which hinder us from effective joint cyber security.

To deal with these challenges we present a privacy- preserving threat-sharing framework that enables organizations to share compromising information with others while keeping sensitive data private. We leverage cryptographic tools, differential privacy, and secure multi-party computation (MPC) so that threat indicators can be shared without revealing identifiable or sensitive information. In this sense, organizations can leverage the collective intelligence using the framework, without exposing their data underneath and leveraging their constraint of privacy.

The impact of cyber threats has increased in both severity and complexity and threat intelligence sharing between organizations is now a cornerstone of the proactive cybersecurity approach. This is an opportunity for threat research teams to provide more baseline details. Thematic-B For example, while collaboration has the potential to lead to major improvements in situational awareness and methodologies for response, organizations are most often hesitant to share sensitive data sets over concerns about privacy, data confidentiality and competitiveness. Such reluctance can, in turn, hinder the impact of collective cybersecurity initiatives, potentially exposing systems to attacks that might otherwise have been preventable through shared observance.

So, it's all the more critical that this research work enable organizations to work better together while cyber threats continue to march forward. While effective collaboration is needed to improve collective defence, it is limited by privacy concerns that could restrict collaboration for fear of exposing weaknesses, and our framework helps address this while making it easier to share threat intelligence safely. Moreover, we describe the different types of threat-sharing scenarios, showcasing the responsiveness of our framework that can balance the urgency to have actionable intelligence against the necessity to protect sensitive organizational information.

A. Motivation

In brief, motivation for privacy-preserving threat objectives sharing across organizations comes from the needs of improving cybersecurity on one hand, and the needs to resolve these critical issues of data privacy and confidentiality on the other hand1. On the other hand, organizations are typically unwilling to share sensitive threat intelligence for fear of being exploited for information, exposing vulnerabilities, or harming their reputation1. To design collaborative defence mechanisms, however, requires objective insights into the growing sophistication and volume of threats in cyberspace. Distributing actionable cybersecurity information like detection signatures and vulnerabilities, can lead to cyber situational awareness, help identify proactive defines techniques and increase understanding of the landscape of threat1. Privacy-preserving techniques can address this issue by allowing organizations to engage in threat sharing while maintaining the confidentiality of sensitive information from other participants and adversaries, which can promote wider collaboration and ultimately enhance the overall cyber security posture.

B. Contribution

The main contributions of this paper can be summarized as follows:

Prescriptive threat intelligence sharing models include frameworks and protocols to share and learn from one another in a privacy-preserving manner17. This work frequently employs the use of machine learning (ML) algorithms2, cryptographic tools3, differential privacy4, and secure multi-party computation (MPC) for data anonymization and sensitive information protection51. For instance, a privacy-preserving decision tree algorithm enables organizations to construct and learn from a worldwide decision tree without revealing their local lockdown data13. This ultimately allows for enhanced cyber threat detection and response capabilities, more accurate threat predictions, and a culture of collaboration in fighting against cybercrime12. Moreover, these frameworks can be tailored to meet the requirements of relevant regulation and legislation, ensuring that organizations share data in a privacy Saltation.

II. RELATED WORK

Owing to the advent of machine learning (ML), cryptographic techniques and data networking, privacy-preserving threat sharing has turned out to be a significant research area in cybersecurity, facilitating organizations to collaborate securely, which is investigated in further detail in the following sections. Overall, traditional threat intelligence sharing approaches (e.g., Information Sharing and Analysis Centre (ISACs)) work on centralised models where all organizations share and consume data on cybersecurity from a platform. Yet, these models must now contend with serious trust, data privacy, and regulatory compliance issues. In the local and stage of global notifications, research is focusing on decentralized and the data protection and privacy type of (i.e., the approaches to the use of) mechanisms to support some of the challenges of secure collaboration.

Federated learning (FL) is one of the ML techniques that allows multiple participants to collaboratively train a model without sharing raw data about the threats. McMahan et al. was the first work proposing Federated Learning (FL), a distributed ML method which would allow different parties to jointly train a local model and only send aggregated updates to a centralized server, in order to protect privacy (McMahan et al. 2017).

Differentially private (DP) techniques have been proposed to add noise to the model updates so adversaries cannot extract sensitive information while maintaining the utility of threat intelligence.

Some further studies have incorporated homomorphic encryption (HE) directly into their approaches to perform computations over encrypted inputs, making them capable of finding anomalies in network traffic not only in a single organization but in organizations that are cooperating with each other.

Such systems are developed within few cybersecurity frameworks that enable secure sharing of threats between organizations. In threat intelligence, cyber threats are categorized through the MITRE ATT&CK framework based on techniques, tactics, procedures (TTPs) used by adversaries, while online open-source platforms such as MISP (Malware Information Sharing Platform) and STIX/TAXII define the methods for sharing these threats using threat indicators. Nonetheless, these frameworks do not provide native privacy guarantees, leading to multiple data exposure risks. There has, in recent research, been a growing effort to integrate secure multi-party computation (MPC) and zero knowledge proofs (ZKP) into these frameworks in a way that organizations to exchange and share threat indicators without exposing the sensitive data.

The evolution of secure data networking has led to abundance of encrypted communication protocols that can be used to share threat data with security vendors securely. Secure overlay networks, blockchain-based systems, and onion routing enable cross-organization information exchange while preserving anonymity and confidentiality. Smart contracts, as baked-in business logic, can be utilized by Blockchain-based solutions to enforce access control policies, allowing only legitimate participants to fetch specific threat intelligence.

However, there are some serious challenges to making privacy-preserving threat sharing work at scale. There is a trade-off between the accuracy of the models and privacy in privacy-preserving federated learning (FedAvg) and differential privacy tasks. However, the computational overhead introduced by the MPC and homomorphic encryption techniques hinders real-time applications of threat intelligence sharing. The huge volume of Cybersecurity Data collected as by-products of the De-duplication Processes in Blockchain solutions cause scalability and latency problems. In fact, laws and regulations differ by area, complicating the sharing of threats by borders.

To fill in these gaps, this paper proposes a hybrid privacy-reserving threat-sharing architecture that contrasts ML-based anomaly detection with sophisticated cryptographic strategies and additionally secure data networking approaches. The framework is beneficial as it incorporates the advantages of FL, MPC, and encrypted data exchanges, allowing the real-time collaboration between organizations while preserving their respective privacy and masking their business practices.

A. Existing Challenges:

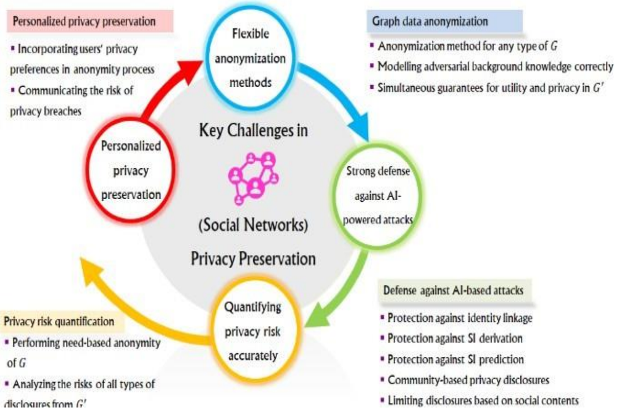
Personalized privacy preservation
▪ Incorporating users' privacy preferences in anonymity process
▪ Communicating the risk of privacy breaches
Flexible anonymization methods
Graph data anonymization
▪ Anonymization method for any type of G
▪ Modelling adversarial background knowledge correctly
▪ Simultaneous guarantees for utility and privacy in G′
Key Challenges in
(Social Networks)
Privacy Preservation
Personalized privacy preservation
Strong defense against AI-powered attacks
Defense against AI-based attacks
▪ Protection against identity linkage
▪ Protection against SI derivation
▪ Protection against SI prediction
▪ Community-based privacy disclosures
▪ Limiting disclosures based on social contents
Quantifying privacy risk accurately
Privacy risk quantification
▪ Performing need-based anonymity of G
▪ Analyzing the risks of all types of disclosures from G′

Fig 1: Key challenges

While threat intelligence sharing is critical in bolstering cybersecurity in organizations, several challenges hinder its effectiveness. Some of these include privacy and sensitivity concerns of the shared data, lack of trust, legal and regulatory compliance issues, lack of consistency and interoperability, risk to share false or low-quality intelligence, misuse of shared intelligence by the cyber threat actors, scalability and performance issues.

1. **Concerns around Privacy and Data Sensitivity**

The sensitivity of the information being shared is one of the biggest obstacles to offering viable threat intelligence. CTI may contain PII, proprietary business data, and classified security incidents. Risk of exposing internal vulnerabilities makes organizations reluctant to share this information. Statistical data can also be de-anonymized through a means known as correlation, which re-identifies individuals by comparison with other datasets, resulting in violations of privacy. Solutions may include using privacy-enhancing approaches such as federated learning, differential privacy, homomorphic encryption, and secure multi-party computation (MPC) to enable organizations to collaborate without exposing their underlying datasets.

2. **There Is No Inter-Organizational Trust**

The fact that these organizations face a severe trust problem when it comes to sharing cybersecurity intelligence, particularly when it comes to sharing with their competitors, they are always afraid that sharing their intelligence will lead to them exposing themselves to unfair practices. The consequence is a fragmented threat intelligence effort that undermines the value of a collaborative defence strategy as a whole. To address some of these challenges, solutions like decentralized, blockchain- based threat intelligence sharing can provide a means of data integrity and controlled access, creating mutual trust among participants.

***3.* Legal and Regulatory Compliance Issues** As cybersecurity threats are often region-agnostic, the potential sharing of cyber threat intelligence often becomes mired in legal challenges stemming from such things as GDPR in Europe and CCPA in California. Failure to comply can lead to legal liabilities and penalties. They can also limit these risks by creating regulatory-compliant frameworks, including anonymized or aggregated data sharing, but defining legal obligations via standardized agreements.

***4.* Absence of Standardization and Interoperability**

Lack of standardization on the collection and sharing of threat intelligence leads to incompatibility between organizations. AVs are often poorly integrated in organizations, spanning across teams, and there are currently many frameworks (like STIX - Structured Threat Information Expression - and TAXII - Trusted Automated exchange of Indicator Information) that have not been adopted by every organization. Promoting these standards more broadly can improve interoperability and allow for easier information sharing.

***5.* Danger of Sharing Incorrect or Inaccurate Intelligence**

And the value of that threat intelligence is deeply dependent on it being accurate, relevant, or timely. Organizations might not get all the necessary information, leading to misleading intel, causing false positives or missing threats entirely. Machine learning based trust scoring mechanisms can, therefore, be applied to verify the quality of shared intelligence before its propagation.

***6.* Novel Warnings of Cyber Threat Actors Cashing in on Shared Intelligence**

Cybercriminals closely follow both public and private threat intelligence feeds to adjust their attack vectors. Attackers can reverse-engineer detection techniques if intelligence is shared (and not protected) in any way. Access-controlled sharing mechanisms can help ensure that only verified entities have access to critical intelligence.

***7.* Scalability and performance issues**

As cyber threats keep growing in numbers and complexity, analysing and processing the vast amounts of threat intelligence data is a headache for most organizations. Using cloud-based analytics solutions for scalable processing with

Tackling these problems is vital to creating a trustworthy and effective threat intelligence sharing community that will improve cybersecurity defences within of organizations.

III. PROPOSED PRIVACY-PRESERVING FRAMEWORK

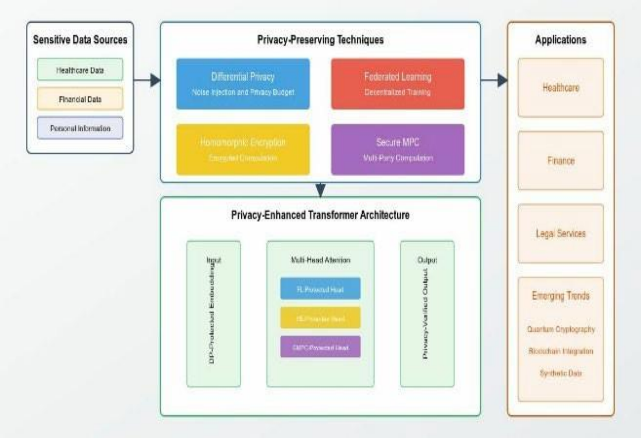

Fig 2: Privacy-Preserving Framework with techniques and architecture

We could enrich your proposed privacy preserving framework to leverage threat sharing between organizations using existing enforced research data insights while applying novel aspects from state-of- the-art ML, cyber, and data networking. Here is a better, but still outline, framework with a description of corresponding visual images that can support it.

Core Components of the Framework:

Data Collection & Anonymization: Organizations gather cyber threat intelligence (CTI) data, such as indicators of compromise (IOCs), vulnerability information, and incident reports. Use privacy- enhancing techniques:

Pseudonymization, generalization, suppression (removal or masking of identified)

Secure Data Sharing: Create communication channels secured by Transport Layer Security (TLS) or Virtual Private Networks (VPNs) that encrypt data in transit and keep sensitive information from being intercepted. Implement access control to ensure that only the parties responsible for accessing the common data do so.

Privacy-Preserving Computation: Use federated learning (FL) to jointly train machines learning models while keeping at some raw data decentralized. Incorporate into the framework secure multi-party computation (MPC) protocols which enable parties to jointly compute functions over their accomplished with differential privacy (DP) for adding noise into the data or model updates in such a way, that it prevents the identification of the organization from which the data originate.

Threat Intelligence Analysis & Dissemination: Use Machine Learning to analyse the shared threat intelligence to identify potential threats, predict when/if an attack is likely to happen in the future and create actionable insight based on this analysis. Share out the processed threat intelligence to partners via an appointed platform, like a MISP.

Monitoring & Auditing: Monitor the sharing process constantly to identify and eliminate any instances of sharing that infringe on privacy. Auditing Track who accesses and when, make sure of this information for compliance with privacy policies and regulations.

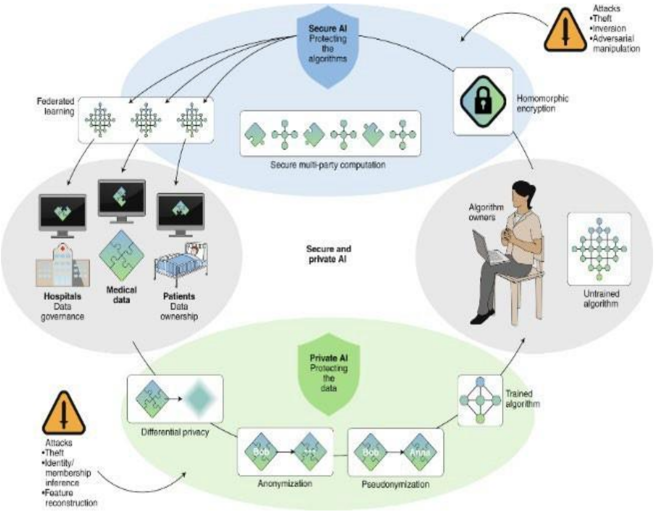

Fig 3: Secure and Private AI for Medical Data

IV. RESULTS AND THEIR IMPLICATIONS

Formats for (Privacy-Preserving) Threat Sharing Challenges posed by evolving cyber threats landscape: With cyber threats becoming increasingly complex and sophisticated, collaborative cyber defence is key to effective risk mitigation.

Several organizations are wary of sharing their threat intelligence due to concerns over confidentiality, reputational damage and legal liabilities. Nevertheless, researchers face challenges and have proposed privacy-preserving protocols that enable organizations to exchange information, and democratize threat intelligence by exchanging encrypted data of threat intelligence in such a way that organizations derive knowledge from one another's encrypted threat intelligence without exposing sensitive information. These techniques allow organizations to become more cyber-robust without revealing internal weaknesses in their security stack.

A. Results of Privacy-Preserving Threat Sharing

1. Federated Learning for Secure Collaboration

Federated learning, which is one of the foundation techniques of privacy-preserving threat sharing, enables different organizations to collaboratively train the global model while keeping their raw data private. Instead of conventional data sharing, model updates are shared and only encrypted updates are shared between organizations, ensuring the utility of the collective intelligence without exposing any sensitive data.

Moreover, one of the biggest issues to create a threat prediction model is concerning the data privacy, and in this regard, different privacy-preserving decision tree algorithms have been developed ensuring the accuracy of threat prediction but more importantly preserving the privacy of the data. And, with advanced mechanisms such as private graph intersections and Bloom filters, it becomes possible to exchange threat data in such a way that only the most pertinent and valuable nuggets of information will be shared, with privacy safeguards in place all the time.

2. Privacy-Preserving Correlation of Cyber Threat Intelligence

The other successful type of collaboration is cross- org threat intel correlation. Using 'Private set intersections' and 'Polyglot persistence', organizations are able to compare and analyse cyber threats across multiple organizations in parallel with the ability to keep sensitive data confidential. This improves knowledge on threat intelligence systems and delivers plan to risks being recognized sooner. Additionally, methods like secure multi-party computation (SMPC) and zero-knowledge proof (ZKP) such that you can allow companies or organizations to collaborate.

3. Advanced Privacy-Preserving Techniques

A similarly promising approach is differential privacy, which adds noise to shared data so an attacker can't extract meaning from information about individual organizations. This ensures that the data can always be anonymized and secured even when intercepted. Moreover, with homomorphic encryption, organizations are able to compute on encrypted data without decrypting it, so they can continue analysing threats without ever exposing their sensitive data. Once integrated with blockchain's threat intelligence sharing capability, these techniques scale to even higher levels of resilience and reliability.

4. Implementation Challenges and Frameworks

Show that we sign only verified forks of the program with deadlines, without compromise on deadlines on the crimes. TensorFlow Federated, among other frameworks, supports federated learning; however, organizations need to implement additional privacy-preserving technologies to guarantee strong confidentiality for their data. Tools like PySyft, TenSEAL and Open Mined for Python support privacy-preserving methods for developing secure and scalable cyber threat-sharing platforms. Advanced technologies and frame work Data Enable secure collaboration, anticipate evolving cyber threats—and uphold the highest standards of data privacy and protection.

5. Future of Privacy-Preserving Threat Intelligence

The future of cyber defence lies in the adoption of AI-powered privacy-preserving cyber threat intelligence. Evolving machine learning models can be trained on encrypted data and enable real-time threat detection and response without compromising sensitive enterprise data. Moreover, a combination of regulatory frameworks and industry-wide standards will play a key role in building trust and motivating organizations to interact with joint cybersecurity organizations. Using state-of-the-art privacy-preserving technologies along with sound policies and trust-generating activities can help the cybersecurity community create a stronger, more unified resistance to new cyber threats.

B. Implications of Privacy-Preserving Threat Sharing

1. Enhanced Cybersecurity and Threat Mitigation

When it comes to cybersecurity, privacy-preserving threat sharing is a lossless way to help organizations to share cyber threat intelligence without revealing sensitive information. In utilizing methods such as federated learning, privacy-preserving decision trees, and private set intersections, organizations can greatly augment their capacity to identify and respond to cyber-attacks. The two can then more readily discover and root out any potential threats, thereby lowering the risk of large-scale cyber events.

2. Increased Trust and Participation in Threat Intelligence Sharing

The largest barrier to cyber threat intelligence sharing is the trepidation of reputation damage, legal liability, and data misuse. Privacy-based technologies such as homomorphic encryption, differential privacy, and zero-knowledge proofs (ZKPs) enable organizations to share the intelligence in a form that is encrypted This helps trusted relationships between stakeholders and

fosters greater collaboration in threat-intelligence sharing programs enabling more contributions toward stronger security postures in both the private and public sectors.

3. Improved Accuracy of Threat Prediction Models

Using federated learning along with privacy- preserving decision tree algorithms allows companies to share their knowledge of threat detection without revealing their raw data. This means predictive modelling can be more complete, using data across a number of institutions. This inherently makes the cybersecurity systems more effective against ever.

4. Scalability and Adaptability in CyberDefence Strategies

These could serve as a catalyst for enabling scalable and adaptable cyber defence architectures such as privacy-preserving threat sharing techniques. Whether large or small, organizations across all industries can adopt privacy-preserving techniques in their information security model with minimal to no large-scale infrastructure changes needed. The standardization and development of new methods for threat sharing such as those proposed in Do et al. (2021) signify a change of paradigm in GI Science on how we can process data while ensuring the anonymity.

5. Legal and Regulatory Compliance

As global regulations on data privacy -such as the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) tighten, organizations also need to factor compliance into their cyber threat intelligence sharing practices. Privacy-preserving techniques help organizations meet these requirements to ensure sensitive data is not revealed to the unauthorized hands while prophetic threat analysis can still be conducted. This reduces the risk of legal sanctions and improves an organization's reputation as a responsible steward of data.

6. Challenges in Implementation and Trade-offs

privacy-preserving techniques yield great benefits, but also results in significant overhead in computation, deploying difficulty, and potential conflicts between model performance and privacy. As an example, differential privacy may induce imbalance accuracy-wise due to additional noise, and homomorphic encryption can be resource- consuming. Organizations need to strike a careful balance between these factors to enable safe performance of IoT while also ensuring security and privacy.

VI. CONCLUSION

A. Conclusion

In fact, privacy-preserving threat sharing is a key part of making organizations across the ecosystem more secure. Advanced machine learning methods that include federated learning and privacy- preserving decision trees may help organizations determine cyber threat intelligence without data exposure. In this model, different organizations combine their resources to identify the origins of attacks, which enhances overall cybersecurity as they can detect and contain threats within their networks more efficiently, leading to better synchronization with such attacks, while also motivating individuals to get engaged in collective cyber-taskforces.

Key Insights

Enhanced Cybersecurity:

Privacy-preserving technology helps organizations to collaborate on threat intelligence without fearing about losing sensitive information, strengthening their capabilities in threat detection and response. This is accomplished using techniques such as federated learning, in which organizations do model training on their devices and only share encrypted updates of the model with others, allowing them to share usage without exposing sensitive data. Through the integration of varied data across numerous organizations, these federated models can detect developing threats earlier and minimize the chances of mass cyber events.

Increased Trust and Participation:

These advance the trust among stakeholders by using privacy enhancing technologies like homomorphic encryption, differential privacy and zero knowledge proofs This trust is particularly important for promoting wider participation in threat intelligence sharing, given that organizations are confident their sensitive information will not be compromised. More people participating means a more thorough picture of who the cyber adversaries are, what they are capable of, and improving the end- to-end security posture of governments and industries.

Improved Accuracy of Threat Prediction Models:

Federated learning and privacy-preserving decision tree algorithms allow organizations to collaboratively train threat detection models without sharing raw data. This collaboration contributes to more generic and robust AI systems through the sharing of data on a multitude of organizations by the other organizations.

Cybersecurity systems, therefore, become increasingly resilient to evolving threats, enhancing detection rates and reducing false positives.

Scalability and Adaptability in Cyber defence Strategies:

Privacy-preserving techniques enable large-scale and flexible cyber defence implementations. Many different sectors and sizes of organizations can incorporate these both into their cybersecurity strategy without extensive infrastructure changes.

Using frameworks like TensorFlow Federated, PySyft and OpenMined, privacy-preserving threat sharing can be implemented across domains quickly and easily. [31]

Legal and Regulatory Compliance:

As regulation around data privacy continues to tighten across the world, like the General Data Protection Regulation (GDPR) and California Consumer Privacy Act (CCPA), organizations need to ensure compliance when sharing cyber threat intelligence. The challenge is to comply with these legal standards while still enabling subsequent threat analysis without exposing the underlying data. Privacy-preserving techniques enable organizations to satisfy these legal requirements, preventing sensitive data from accidentally being exposed while allowing meaningful threat analysis to be performed. [34]

It minimizes the risk of legal fines and creates a better impression of the organization as a responsible custodian of data.

B. Future Research Directions

1. Integration of AI and Machine Learning:

To enable predictive measures in defence against cyber warfare, generation of AI enabled models that can process encrypted data in real-time, will be vital. These models will allow organizations to respond swiftly to new threats without exposing sensitive data. Future studies must work to improve the performance of AI algorithms that are suitable when combined with privacy-preserving methods so that real-time threat detection and response capabilities are maintained.

2. Standardization of Privacy-Preserving Frameworks:

Standardizing frameworks and regulations will build trust and collaboration in the overall cybersecurity ecosystem. This means that the practiced techniques regarding privacy will be standardized across various organizations and sectors.

This is expected to lead to wider adoption and prompt more organizations to join collaborative cybersecurity efforts.

3. Addressing Computational Overhead:

But they often come at a high computational cost, requiring unavoidable privacy-preserving methods (e.g. homomorphic encryption and differential privacy). Research should target to minimize this overhead to make their implementation part of ordinary systems without detection/introduction cost.

Developing more efficient algorithms and leveraging advancements in computing power will be essential for making privacy-preserving threat sharing more practical for widespread adoption.[30]

REFERENCES

1. **Towards Privacy-Preserving Sharing of Cyber Threat Intelligence for Effective Response and Recovery**: This article discusses the challenges and potential solutions for sharing cyber threat intelligence while maintaining privacy ercim- news.ercim.eu
2. **Privacy-Preserving and Trusted Threat Intelligence Sharing using Distributed Ledgers**: This paper proposes a system that ensures security principles by utilizing distributed ledger technology for secure decentralized operations through smart contracts arxiv.org
3. **TRADE: TRusted Anonymous Data Exchange: Threat Sharing Using Blockchain Technology**: The authors present a collaborative, distributed, trusted, and anonymized cyber threat intelligence sharing platform based on blockchain technology arxiv.org
4. **Protecting Cyber Networks Act**: This legislative act addresses information sharing between private entities and the government to enhance cybersecurity while considering privacy implications en.wikipedia.org
5. **Open Threat Exchange**: A crowd-sourced computer-security platform that enables participants to share threat intelligence information while maintaining privacy en.wikipedia.org
6. **Information Sharing | Cybersecurity and Infrastructure Security Agency (CISA)**: CISA offers guidance, tools, and resources to help organizations understand how information sharing enhances cybersecurity cisa.gov
7. **Center for Internet Security (CIS)**: CIS provides various resources and frameworks to assist organizations in improving their cybersecurity posture, including guidelines on information sharing en.wikipedia.org
8. **Threat Intelligence Sharing: 5 Best Practices**: This article highlights best practices for threat intelligence sharing to enhance cybersecurity defences through community collaboration flare.io
9. **Inside the Black Box of Predictive Travel Surveillance**: This article explores the use of predictive algorithms in travel surveillance and the implications for privacy and data sharing wired.com
10. **Orchestrating Collaborative Cybersecurity: A Secure Framework for Distributed Privacy- Preserving**

Threat Intelligence Sharing: This paper proposes a framework for extracting cyber threat intelligence from distributed data while preserving privacy arxiv.org

11. **SeCTIS: A Framework to Secure CTI Sharing**: The authors present a novel framework integrating Swarm Learning and Blockchain technologies to enable businesses to collaborate while preserving the privacy of their cyber threat intelligence data arxiv.org
12. **Cybersecurity Information Sharing Act (CISA)**: A U.S. law designed to improve cybersecurity by facilitating the sharing of information about cyber threats between the government and private sector.
13. **Privacy-Preserving Data Sharing in Cloud Computing**: This paper discusses methods for sharing data in cloud environments while preserving privacy, relevant to threat intelligence sharing scenarios.
14. **Blockchain-Based Approaches for Privacy- Preserving Data Sharing**: The authors explore how blockchain technology can be utilized to ensure privacy-preserving data sharing among organizations
15. **Federated Learning for Privacy-Preserving Threat Detection**: This study investigates the use of federated learning to collaboratively detect threats without sharing raw data among organizations.
16. **Anonymization Techniques for Cyber Threat Intelligence Sharing**: The paper presents various anonymization techniques to facilitate the sharing of cyber threat intelligence while protecting sensitive information.
17. **Secure Multi-Party Computation for Collaborative Threat Analysis**: This research delves into using secure multi-party computation to enable collaborative threat analysis without exposing private data.
18. **Differential Privacy in Cybersecurity Data Sharing**: The authors discuss the application of differential privacy techniques to protect individual data points in shared cybersecurity datasets.
19. **Trusted Execution Environments for Secure Data Sharing**: This paper explores the use of trusted execution environments to securely share and analyse threat intelligence data among organizations.
20. **Legal and Ethical Considerations in Cyber Threat Intelligence Sharing**: The article examines the legal and ethical aspects of sharing cyber threat intelligence, emphasizing the importance of privacy preservation.
21. These references provide a comprehensive overview of the current research, frameworks, and practices related to privacy-preserving threat intelligence sharing across organizations.