HIGH SCHOOL EDITION
Journal of Student Research
Volume 13 Issue 2 (2024)

Securing Digital Lives: Personalized Measures for Comprehensive Data Protection for Home Networks

Rishi Vora[1], Sarada Prasad Gochhayat[#], Virgel Torremocha[#] and Jothsna Kethar[#]

[#]Advisor

ABSTRACT

This research paper addresses the increasing cyber threats targeting home networks and the lack of comprehensive security solutions tailored for consumers. It proposes a comprehensive solution that addresses data protection, threat monitoring, and impact mitigation, which could be automated through AI and Federated Learning (FL) to simplify security for non-experts. The paper conducts a literature review and qualitative analysis to examine cyber threats and security research, proposing an architecture that utilizes FL across home devices. It discusses challenges such as handling biases and diverse devices, limitations of interoperability, and hardware requirements. The paper emphasizes the urgent need for automated and personalized cybersecurity tailored for consumers to address the escalating threats to home networks, arguing that FL has the potential to enable this while addressing privacy concerns associated with centralized AI.

Introduction

Protecting the privacy and security of internet data has become increasingly critical, given the evolving threats of malware, identity theft, and potential exposure of private information online. Despite various available firewalls and antivirus solutions, these tools often fall short in preventing interactions with risky websites, managing cookies, and guarding against accidental data exposure to high-risk online platforms. Comprehensive solutions tend to be expensive and primarily designed for large enterprises capable of monitoring and mitigating real-time internet traffic risks, leaving a significant gap for a user-friendly and unified solution that effectively addresses these challenges for home networks. Despite the willingness of home users to invest in such solutions, these solutions remain elusive. This paper aims to identify core research problems and propose an approach to develop comprehensive solutions for enhancing home network security and privacy.

Implementing strong and comprehensive online security requires taking a personalized approach that focuses specifically on protecting one's data. As highlighted in Ikonen's paper, the modern threat landscape targets a wide range of vulnerabilities across different devices and platforms utilized in everyone's digital lives (Ikonen, 2014). However, the paper also guides customized security measures individuals can take to safeguard their unique, personal online environment and the data within it. Adopting the strategy with an emphasis on covering all potential entry points for one's data allows for truly holistic protection tailored specifically to one's needs. However, the common consumer is not trained to execute these strategies. Moreover, the comprehensive solution is so tedious that even knowledgeable professionals find it challenging to ensure secure methods of communication and data storage every time. There is a need to simplify cybersecurity for common consumers.

This study reviews the impact of cyber threats followed by a discussion on the evolution and advancement of cyber threats. Most research and literature about cybersecurity focuses on business impact and how to secure enterprises from cyber threats. This paper highlights the gaps in cyber security specifically with regards to home network security. As the number of households with connected devices and broadband networks grows,

hackers have a greater opportunity to attack home networks to use their resources for monetary gains. This paper emphasizes the importance of securing home networks and contributes research by presenting approaches for comprehensive cybersecurity solutions that are more suitable for common consumers. To match the evolving cyber threats and use of AI by hackers, cybersecurity solutions must be enhanced by embedding AI-based security and privacy intelligence into network devices and ISPs that power the home networks. This research recommends the use of Federated Learning to enhance cybersecurity solutions for home networks. Further research is recommended to study efficient architectures and algorithms for personalized security and privacy solutions using Federated Learning.

Methodologies

The research aims to explore cyber threats' risks and impacts on home networks, identifying opportunities for simpler, cost-effective cybersecurity solutions for consumers. It involves a secondary literature review, analyzing primary studies and research articles. The research procedure included in-depth exploration and brainstorming sessions. The qualitative research highlights the potential for mass benefit by developing straightforward, automated cybersecurity solutions accessible to non-experts. Emphasis is placed on the importance of offering high-quality cybersecurity to the public, given society's growing reliance on the internet and electronic devices.

Impact of Escalating Cyber Threats

Cybersecurity threats are rapidly escalating and posing growing risks to personal data and financial well-being. Each year, an alarming 71.1 million people fall victim to cyber crimes such as phishing scams, from which individuals lose $225 on average (Purplesec, 2023). Moreover, personally identifiable information (PII) has a market value of roughly $200 per stolen record, incentivizing cyber criminals to compromise more users. In 2021 alone, the top five cyber crimes were extortion, identity theft, personal data breach, non-payment, and phishing attacks. Perhaps most troubling is that criminals need only a $34 monthly investment to potentially net $25,000 monthly through online schemes, underscoring the high profit margins of cybercrime. As these threats multiply, it is becoming ever more urgent for individuals to implement comprehensive defensive measures to safeguard their diverse and expanding digital lives, focusing on proactively protecting valuable personal data assets.

While the costs to businesses and individuals from cybersecurity threats are increasing, cybersecurity solutions continue to play catchup even for large enterprises. The vulnerabilities for common internet consumers continue to grow rapidly. An Embark report estimates the cost of cybercrimes to reach $10.5 trillion by 2025 (McLean, 2024).

Evolving Landscape of Digital Security

According to a paper from Google Cloud, the cybersecurity environment is continuously changing, sometimes in unforeseen ways. Defenders must remain vigilant against evolving threats, especially considering that phishing remains the most common attack, as highlighted in the 2023 Comcast Business Cybersecurity Threat Report, finding that nine out of 10 attempts to breach its customers' networks started with phishing. According to a 2019 Forrester Research report, 80% of cybersecurity decision-makers expected AI to increase the scale and speed of attacks, and 66% expected AI "to conduct attacks that no human could conceive of." While cyber threats are evolving quickly with advanced technology, the common consumer remains exposed to escalating risks while cybersecurity solutions play catch up to these vulnerabilities.

As more people conduct their daily lives online, including banking, socializing, and working, implementing strong personal cybersecurity measures is crucial to safely navigate the modern digital world. A 2018 report by JSIS highlights the need for technical safeguards and collaborative policy approaches to build cyber resilience against escalating threats. It also examines frameworks for assessing and mitigating risk at organizational and national levels. Consequently, personally identifiable information has been found unencrypted in most of the top 25 data breaches discussed in an article exposing individuals to risks (Osakwe, 2021). A home network security threats report by Trend Micro discusses a new evolving threat to home networks where hackers utilize the devices inside the home networks for various kinds of cybersecurity attacks as well as utilize home network resources for monetary gains in the form of Bitcoin mining operations (Trend Micro, 2018). The average individual remains vulnerable to various modern cybersecurity threats, a concern that can be addressed by personalized solutions.

Mohsin's 2022 paper directly contributes to research on personalized digital security solutions by outlining the objectives of data privacy and cybersecurity. The paper clarifies the overarching goals of safeguarding personal information and systems, aiming to provide users with control over their data. Mohsin elaborates on technical strategies, such as encryption, patching, and firewalls, which could serve as the basis for a comprehensive yet customizable security framework designed to empower individuals. Recognizing that comprehensive protection requires vigilance across all interactive aspects of digital life, this paper aims to review gaps in how individuals manage personal data and security, suggesting necessary research to solve challenges while presenting a multi-layered thought process.

The 2017 editorial by Kuner et al. presents a nuanced perspective on the relationship between privacy and security, which is highly relevant to research on personalized digital protections. It explains that privacy is dependent on security, but tensions can arise when their priorities compete. Borky's paper presents valuable research on technical approaches highly relevant to designing comprehensive personalized privacy and security solutions (Borky & Bradley, 2018). It specifically explores reputation systems, credential services, pseudonymity, trust negotiation, distributed ledgers, blockchain, and confidential computing models. Unfortunately, these strategies are underutilized. The day-to-day business transactions conducted by regular consumers often use outdated software that lacks comprehensive data security and privacy solutions against advanced threats. Although modern software may employ these strategies, implementing them with existing software is challenging and time-consuming. Personal data protection continues to be challenging due to the ever-evolving nature of cyber threats. The trend of people working from home post-COVID-19 has further exacerbated the need for the protection of home networks for individuals and enterprises.

Connected Home Security Challenges

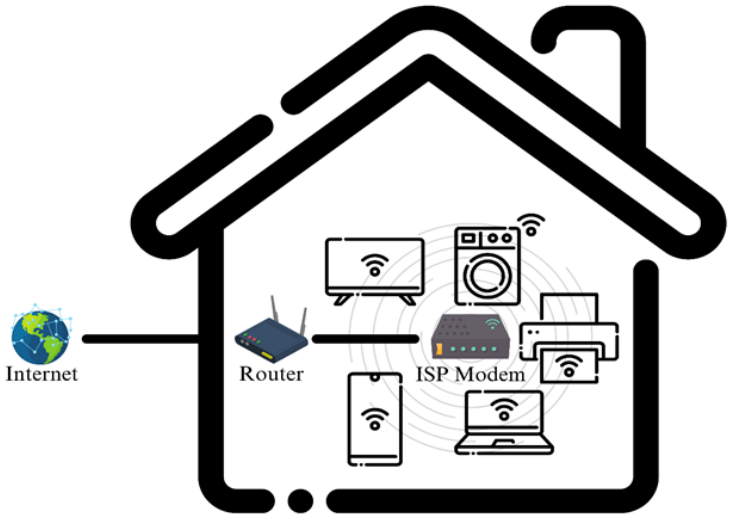

Figure 1. Typical Modern Home Network Diagram

Arabo's 2015 paper describes the growing challenges with cyber security as a threat posed by not just the technology, but also humans who trust their devices and are too busy to pay attention to the security risks. Most sensitive, financial, medical, and personal information is stored and accessed via the devices in the home network and collected by the service providers via a plethora of online applications. Password protection is the most common form of protection which is insufficient against sophisticated AI-based cybersecurity threats. Figure 1 shows a typical modern family home network with a variety of devices connected to the Wi-Fi network. Each of these devices generates vast amounts of data that gets transmitted from one's home network to the internet.

In the paper, Arabo details some key challenges with the security of personal networks in the form of viruses, malware, malicious open Wi-Fi networks, lost or stolen devices, abuse of services, and unauthorized control of devices. Most internet users lack an understanding of implementing basic security measures and the risks of financial impact that stem from data breaches.

While humans naturally trust others, security relies on a zero-trust approach. Social engineering-based cybercrimes rely on people's trust in each other and continue to grow. Social media increases security challenges where people expose a large amount of their personal and private information, which makes it easy for cybercriminals to identify cybersecurity targets. A simple example of social engineering is a targeted question from a hacker who poses to be an online friend and extracts information to answer security questions about online accounts. This could cause a takeover of online accounts.

Home networks by default do not come equipped with anything more than the most basic security measures and no tooling to detect, track, or manage data security and privacy breaches. The only solution to address these challenges is the creation of a comprehensive solution for cyber security that every person using the internet can easily implement. And the solution needs to be preventing data breaches through all modalities - use of the internet, social interactions, and physical security.

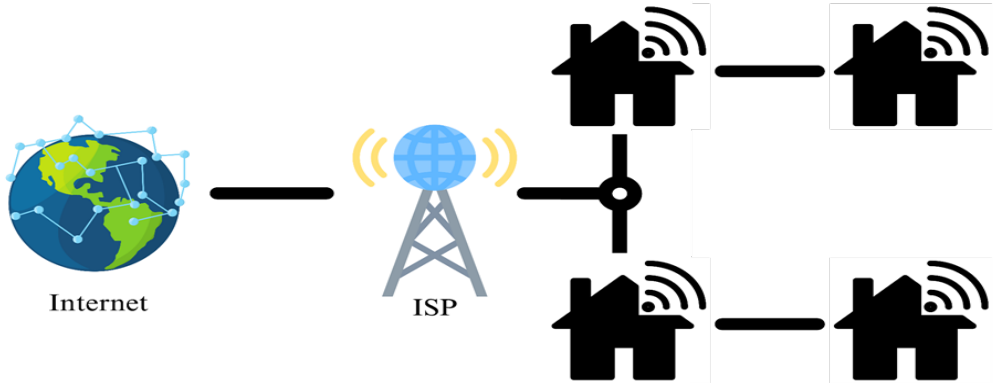

Figure 2. Interconnected Home Networks via ISP

Figure 2 shows a typical architecture of how home networks are connected to the internet via ISPs. ISPs benefit from minimizing cyber threats to their customers. It saves bandwidth usage on their networks and establishes better customer trust. An estimated 125 million households in the US alone have broadband internet according to a study by Statistica (Taylor, 2024). This number will continue to grow. This provides a very large attack surface for cybercriminals, as well as creates a great opportunity to utilize the collective resources of so many home networks to gather intelligence and share as part of an AI-based cybersecurity solution.

Cybersecurity solutions need significant investment to utilize the latest AI innovations to match the escalating challenges of cybercrimes. ISPs can play a major role because of the troves of data they have from their customers' internet usage.

Modern AI relies on centralized systems with very large ML models trained on advanced and expensive GPU cluster networks. Unfortunately, such investments are not practical in the case of home security solutions. They need better AI solutions that can avail the latest innovations in AI at a fraction of the cost. The advantage of home networks is that most home networks have actively connected devices that are dormant and their computing capacity is readily available for use. Before delving into AI-based cybersecurity solutions, it is necessary to review a comprehensive approach to cybersecurity for home networks. It clarifies the need for AI-based intelligence in achieving a comprehensive cybersecurity solution.

Comprehensive Approach for Personal Security at Home

A comprehensive security solution for personal data and home networks requires a 360-degree approach that extends beyond mere reliance on software solutions. While software and hardware-based defenses are crucial, they have limitations in protecting against identity theft. Scams through various mediums often persuade many people, especially naive or unsuspecting people to share sensitive information such as their name, email, date of birth, and more. These actions create vulnerabilities for identity theft. Educating individuals about the risks of phishing, malware, data breaches, social engineering tactics, and potential financial losses can discourage them from inadvertently sharing personal data and becoming victims of identity theft. Although cybersecurity solutions go beyond software-based approaches, this paper's primary focus is on emphasizing the effectiveness of software-based solutions in defending against cyber threats. The right cyber security solution will minimize the need for consumers to learn complex security protection methods. Holistic end-to-end security embeds the knowledge to set up complex security protections automatically based on the devices in the home network, types of data stored on those devices, internet activity, and other personal attributes. To ensure privacy and security, none of this personalized information can be transmitted out of the home network to a central system.

The key elements of a comprehensive solution require a 360-degree approach. A comprehensive solution can be classified into three categories:

1. Data Protection - It is paramount to keep all online data encrypted and offline data protected from potential threats to prevent data breaches.
2. Threat Monitoring - Constant monitoring against evolving security threats for online accounts, financial transactions, and data breaches.
3. Threat Mitigation - Insure against security threats and conduct thorough audits as well as revise security measures regularly.

All the 3 classes of solutions are only effective if they have continuous improvement by learning from emerging risks and employing mitigations for those risks.

Data Protection

To protect personal and confidential data, several security measures are discussed that range from data encryption to the use of firewalls, Virtual Private Networks, and others. However, these solutions pose overhead for extremely busy consumers who want to get their internet up and running for various purposes like work, education, entertainment, and news, among others. In short, people's lives and livelihoods depend on having internet connectivity at all times. However, there is a lack of awareness of the risks of data protection. Instead of leaving to train people how to protect their data, what is required is automated data protection. All PII must be stored in an encrypted manner automatically on disk and must also be encrypted in all data transmission. All suspicious calls must be filtered. For example, people get various scam calls that ask people for their social security, birthday, and other confidential information pretending that they are calling from the bank or some other authorities. Most of the time these calls use spoofed phone numbers that are invalid. Such calls must be blocked. Using collective intelligence from 125 million households can prove to be a great asset for such automation. An NSA Cybersecurity Information Sheet provides comprehensive approaches for protecting home networks and data against cyber threats. Implementing the recommended best practices by the NSA requires expertise and knowledge that most consumers lack. The automation of such approaches is a reliable way for common consumers to reap their benefits.

One of the best practices recommended is to use a strong password with multi-factor authentication. A Cybernews article describes how easy it is to crack passwords. Having a strong password is not sufficient. If one uses the same password across all their online accounts, cybercriminals can access all those accounts. Automation needs to help consumers from making such mistakes. Another best practice recommended is to protect the home network. Most routers and modems have a publicly known network admin account with a default password that is in their support documentation online. That makes it very easy to take control of someone's home network administration after one gets wifi access. Cybersecurity automation must detect these default passwords and prompt homeowners to change them.

Threat Monitoring

Several security solutions come in the form of apps to help monitor suspicious activities on various devices. However, no solution is completely cyberthreat-proof, and there is a need for better automation to protect consumers' credit, bank accounts, passwords, social media content, and other aspects of their digital footprint. Not only do apps have to monitor activities on their devices but also their online accounts across the internet. AI-based solutions can track all traffic from personal devices, remember the history of accounts online used, and track any surprising activities online with their accounts. For example, if there is any access to any of their accounts from a location where there are no devices owned by the household, it would be a source of suspicious

activity. Currently, this kind of comprehensive monitoring is not feasible. All legitimate businesses need to enable access to cybersecurity systems.

Every modern device is usually equipped with basic access control and minimal encryption. However, modern security threats are significantly more sophisticated and present high vulnerability to various forms of attack. A security solution to cyber crimes must be constantly evolving to increase its sophistication and continuously monitor all risks for data breaches and mitigate those risks.

While computers have options for antivirus software for PCs, other devices like smart TVs, smart speakers, and other IoT devices do not have antivirus available. Apple devices are usually designed with better security in mind and tend to have reduced risks of data breaches and malicious software. However, they are not immune to phishing, social engineering, and email spam attacks. A study from Deloitte states that "91% of all cyber attacks begin with phishing emails to an unexpected victim" which highlights the importance of email-based attacks. Home security networks must take additional steps to prevent such scam emails. While the primary responsibility of this lies with the email service provider, one cannot rely on such in-depth security to be available from a completely free email service. Plus their service terms and conditions give them immunity from any damages from users clicking on those phishing emails. Email servers used by large enterprises come with significant controls and restrictions that minimize phishing attacks and have dedicated security policies and teams to handle these phishing risks. Such solutions must be extended to consumers via advanced email apps. The use of Federated Learning implemented in the email apps that scan suspicious emails and either block them or flag them to alert consumers to be careful before opening those higher-risk emails will minimize the cybersecurity risks.

Threat Mitigation

While prevention is the best cure, modern and sophisticated cyber criminals may outwit cybersecurity measures and be successful. To mitigate against damages in the event of a data breach or an online account hack, the most important mitigation is the detection and isolation of the data loss or financial loss. Automation must alert consumers of any such breaches and promptly walk through the consumer to change passwords for all other accounts quickly if 1 of the accounts was hacked. Consumers do not have the expertise and knowledge of what actions to take after an identity theft occurs. Automation must personalize recommendations for the consumer based on their digital footprint for a comprehensive set of steps including complaints to FTC and all the necessary authorities. Additionally, it is not sufficient to monitor just consumer activities, but also to monitor government services sites. In 2020, WA state claimed $647 million in fraudulent unemployment claims. These fraudulent claims occurred in the names of people who were working and were due to stolen identity information. These people were surprised when WA state or their HR departments contacted them about their fraudulent claims. Automation solutions must also monitor and alert the most common government benefit services both local and federal to alert consumers.

Necessary Cyber Security Software Features

These features are focused on defining the ideal data security and privacy software features for consumers.

Connectivity and Interoperability

Have software that can connect and interoperate with all devices on the home network to enable security scans more easily. Just like the HTTP and TCP/IP protocols are common standards for communication on the internet, there is a need for embedding controls that prevent data privacy. This means that the insecure transfer of PII and critical data must be restricted.

Vulnerability Testing and Security Risks

Software must include vulnerability testing against all apps installed on all devices to flag security risks to consumers to take appropriate action. Vulnerable testing must constantly evolve to use the techniques used by hackers such as fuzzing that injects invalid, malformed, or unexpected inputs into a system to reveal software defects and vulnerabilities. Vulnerability is a form of ethical hacking. For a more robust vulnerability detection and mitigation, known open-source hacker tools must be integrated as part of the vulnerability detection process. Common consumers will not know how to handle the results of these detected vulnerabilities and will require solutions to be either automatically executed by the software, or a simplified and thorough guide to help consumers understand what actions they need to take and ensure those actions are completed.

Data Encryption

Make data storage enable encryption so that even if there is a breach to access the stored data, it has one more layer of protection.

Browser Security

Browsers must be enhanced with embedded security checks that flag any critical data being transmitted without encryption to minimize identity theft risks.

Email Client Security

All email clients must be enhanced to plugin security monitoring that detects phishing, scams, social engineering, and downloads of suspicious software. Various AI-based techniques help learn and improve the detection of security risks.

Simplified Security and Privacy Settings

Users must have very simple security and privacy level settings. For example, a student who does not have bank accounts or financial data stored or accessed via a device can choose to simplify data privacy management while focusing on access to age-appropriate content takes higher priority. A person renting an apartment without high financial risks can focus on simplifying financial data protection and instead focus on ease of use, whereas a business owner who stores all the critical business accounts and tax documents can choose to lose some ease of use to secure critical data.

Centralized Management

Security software must be able to secure critical data across all devices - laptops, mobile phones, tablets, or other storage devices with the same set of security and privacy controls managed via a centralized console. Automating the propagation of default security settings that help set such security and privacy controls on data will significantly enhance data protection. AI-based detection of highly confidential data can be utilized to tag such data for an added layer of protection.

Encryption for Data Transmission

All critical data transmission must be encrypted independent of the medium of transmission including email, or messaging apps. Automating the use of VPNs on all devices that access the internet can ensure all transmissions are encrypted.

Notification Monitoring

All processes running on the devices must be authorized and not generate spam notifications to invite consumers to click on suspicious websites. Such notifications must be suppressed automatically. AI-based anomaly detection can help create a learning mechanism to detect and block such spam notifications.

Federated Learning for Home Network Security

Any future security solution must avail the latest advancements in AI to handle the dynamic nature of this ever-growing threat. Most AI solutions require a centralized infrastructure and advanced ML models. While large-scale AI-based security solutions work well for large organizations, they are out of reach for consumers who seek to protect data and devices within their home networks. A cyber security company can develop AI-based security solutions and can offer them to consumers at affordable prices, however, these centralized AI solutions require the data from these home networks to be transmitted to centralized AI systems, which violates data security and privacy requirements. Sensitive data from someone's email client cannot be sent to a central ML system over the internet even if they are encrypted because it violates the data privacy of the user. Federated Learning (FL) offers a mechanism to solve data security and privacy concerns as well as provides a much more cost-effective approach for constantly evolving security solutions. Thereby making it an ideal technique to employ against the constantly evolving cyber threats. Before diving into how FL can be employed to solve home network security, let's understand how FL works.

As discussed in a Federated Learning research paper, FL represents an emerging machine-learning paradigm where the overarching machine-learning model is decentralized and resides on individual edge devices (McMahan et al., 2017). Unlike traditional centralized approaches, FL as presented in the paper eliminates the need to transmit raw user data from devices to a central cloud for storage and processing. Instead, the machine learning algorithm operates locally on each device, and only the model update parameters are communicated to the central server for global model aggregation. As discussed in another paper about Federated Learning, this novel FL framework not only enhances data privacy by circumventing the transmission of raw user data but also safeguards the confidentiality of local device data from potential malicious access during transmission or storage (Victor et al., 2022).

Federated learning provides a unique opportunity to enhance home network security cost-effectively. Federated learning structure and data flow are well illustrated in the 2007 paper by Shen et al.

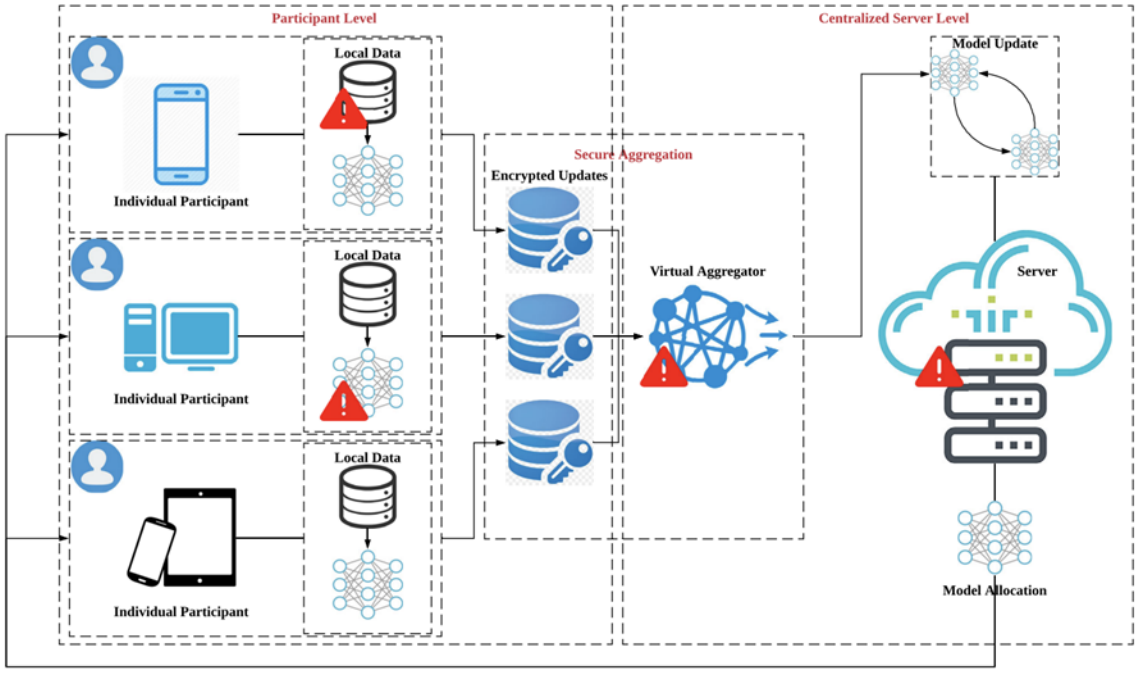

Figure 3. Federated Learning Structure and Data Flow (Shen et al., 2007).

The central server controls the training of the global model and distributes it to clients. Clients also receive training subtasks. The selected clients work on the same training task as assigned by the central server. Each client is a device that collects data and performs training on its data. The only information that ever needs to be transmitted is model updates. Training is divided into epochs. In each epoch, the server allocates a training task to clients that are ready to learn. The client trains the model with its local data and sends the updated model parameters as encrypted training results. These results are sent to an aggregator for compilation which further minimizes the data required to be sent to the central server. The aggregator averages the parameters. These aggregators follow a "secure aggregation protocol" which allows the encrypted parameter updates to be processed without knowing the true data. Aggregated results are sent to the central server that updates the global model. This completes one epoch, and the central server repeats the cycle with new training tasks for the next training epoch.

In this paper, before exploring how to apply FL to home network security, the challenges of home network security and recommendations will be discussed.

Proposed Use of Federated Learning for Cybersecurity Software

To enhance security software with Federated Learning for security management, a system where actions taken by users, such as blocking phone numbers or marking emails as SPAM/Junk, are aggregated and analyzed to identify potential security or privacy risks. This collective intelligence can then be used to automatically flag suspicious emails, messages, websites, or content for all users, helping to minimize security and data privacy risks for naive users. Additionally, by distributing these settings to a centralized system, users can benefit from the collective actions of others, improving the overall security of the system.

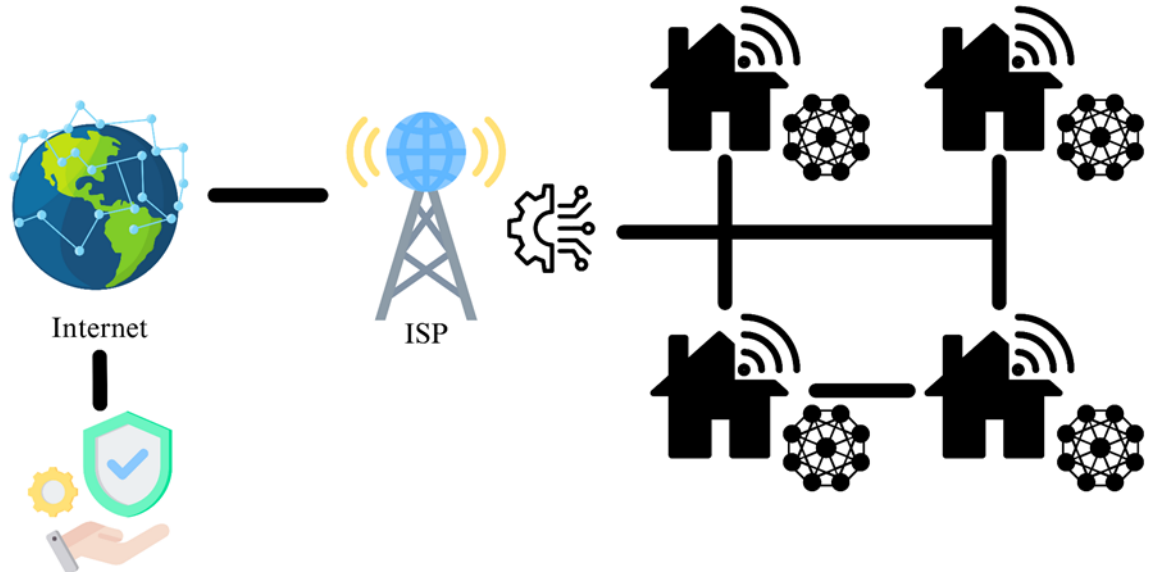

Figure 4. Federated Learning cyber security software architecture

A proposed Federated Learning-based cybersecurity software architecture is shown in Figure 4. Devices in various home networks can act as individual participants in the Federated Learning for cybersecurity software. ISPs can be set up as localized virtual aggregators of these model updates that can then be sent to the central servers in the cyber security system. The Cybersecurity central system is constantly monitoring and learning about the evolving cybersecurity threats continuously and thereby also evolving its defenses to block those emerging threats. However, much more work is needed in this area to create a viable and cost-effective solution. There are some challenges with the system when people generate conflicting signals. For example, some citizens may treat emails they get about political causes that they do not support as spam while others who support them would like more of that content. Federated learning algorithms will need to be enhanced to handle biases in the signals that may arise from various reasons and separate those from centralized learning systems for spam emails related to security and privacy risks. Since the actual data source information is unavailable and only model parameter updates are available, dealing with such biases and noise is much harder for the central server. Hence more intelligence may need to be incorporated into the client models. Spam email filters will need to add more sophistication than using user spam signals from the individual participants. Security solutions typically maintain blacklists to block known high-risk websites. Similarly, whitelists will help to prevent blocking legitimate sites. However, static or manually maintained lists are temporal and get out of date quickly. Automation of managing such lists will need additional AI-based advanced solutions that can gather intelligence from various sources and utilize more than just a list of sites or domain names to differentiate between high-risk and legitimate sites.

Conclusion and Recommendation

The cybersecurity risks to home networks continue to grow with the proliferation of smart devices in the home network that lack security and privacy protection. There are well-known security best practices and security solutions available for enterprise networks. However, those assume that security experts at those enterprises can easily manage complex solutions. Simplifying those enhanced security solutions for common consumers is challenging. Developing comprehensive online security involves managing cybersecurity risks through thor-

ough threat assessments, vulnerability analyses, and impact evaluations tailored to an individual's digital environment. Understanding threats, such as criminals seeking monetary gain or nation-states engaging in cyber-espionage, is critical for appropriate protective measures. Assessments should identify vulnerabilities like weaknesses in home router configurations, outdated software, or reused credentials. Identifying critical data and systems, such as financial accounts. This risk-based approach provides insight into personal risks, allowing for the selection and implementation of strong, multilayered security controls. To simplify this process, AI can play a significant role. While regular AI techniques may not be sufficiently secure, as they require sending data to a central system. Federated Learning offers a secure and cost-effective solution by utilizing distributed storage and compute capacity on consumer devices. This approach enables comprehensive safeguarding of an individual's digital life and data by addressing threats, reducing vulnerabilities, and lessening potential impacts.

Limitations

This study focuses on cyber threats to home networks. However, the threats are common to all networks on the internet. This study highlights some additional vulnerabilities unique to home networks as well as gaps in cybersecurity solutions to promote further research in this area. While cybersecurity has a much higher impact on businesses than homes, these boundaries are blurred with more people working from home. Hence, steps towards comprehensive cybersecurity at home are much more critical in the post-COVID-19 era.

Many papers and articles provide holistic cybersecurity recommendations for home security. However, most of those assume a level of expertise necessary to implement the recommendations. The more fundamental challenge with common consumers is the gap in awareness of cyber threats and risks to online data and its impact on their lives. Education helps only the people who are aware, and curious to solve these challenges. However, it leaves behind the folks who are unaware and have the same risks. The comprehensive solution must minimize the expertise required for common consumers. This paper proposes an approach towards such a solution. However, further work is needed to investigate how to automate the areas of cybersecurity for consumers. In the enterprise environment, there are strict security policies that enable security. However, in the home environment, there is a much higher emphasis on ease of use and enabling access to the internet for young kids, seniors, and people who are still learning to understand and use the internet. The same kind of security policies that are successful in protecting the work environment will create significant hurdles for ease of use in the home environment. Hence the challenge of automating cybersecurity policies is significantly harder in the home environment. This paper discusses the use of Federated Learning to solve cybersecurity in home networks. However, the diversity of devices in home networks limits interoperability between these home networks and centralized learning systems. This limited interoperability prevents some home networks from participating in the Federated Learning-based solution. Federated Learning minimized the costs of learning by distributing the responsibility locally in each home network. Home networks will require a certain minimum hardware capacity to be eligible to process the learning of the models.

Acknowledgments

I would like to thank my family and Gifted Gabber for advising the writing process for this paper. Professor Gochhayat, Professor Torremocha, and Coach Jothsna, all provided great support and guidance throughout the research process.

References

Arabo, A. (2015). Cyber security challenges within the connected home ecosystem futures. Procedia Computer Science, 61, 227-232.

Borky, J. M., & Bradley, T. H. (2018). Protecting Information with Cybersecurity. Effective Model-Based Systems Engineering, 345–404. https://doi.org/10.1007/978-3-319-95669-5_10

Comcast Business. (n.d.). 2023 Comcast Business Cybersecurity Threat Report. Comcast Business - Official Site. https://business.comcast.com/community/browse-all/details/2023-comcast-business-cybersecurity-threat-report

Cunningham, C., Hannon, C., Malik, M., Paik, R., Paramesh, R., Samford, H., ... & Beyer, J. ADDRESSING SYSTEMIC CYBERSECURITY RISK.

Deloitte. (2020, January 9). 91% of all cyber attacks begin with a phishing email to an unexpected victim: Deloitte Malaysia: Risk advisory: Press releases. Deloitte Malaysia. https://www2.deloitte.com/my/en/pages/risk/articles/91-percent-of-all-cyber-attacks-begin-with-a-phishing-email-to-an-unexpected-victim.html

DPM. (2023, December 19). 10 things you need to know about data breaches. Data Privacy Manager. https://dataprivacymanager.net/10-things-you-need-to-know-about-data-breaches/

FINRA. (n.d.). Common cybersecurity threats. FINRA.org. https://www.finra.org/rules-guidance/guidance/common-cybersecurity-threats

Forrester. (n.d.). Forrester: The emergence of offensive Ai - Darktrace. https://www.darktrace.com/de/resources/research-forrester-offensive-ai.pdf

Google Cloud. (n.d.). Cybersecurity forecast 2024. https://services.google.com/fh/files/misc/google-cloud-cybersecurity-forecast-2024.pdf

Ikonen, M. (2014). Cyber Security: Home User's Perspective.

Jančis, M. (2023, November 15). 8 most popular password cracking techniques: learn how to protect your privacy. Cybernews. https://cybernews.com/best-password-managers/password-cracking-techniques/

Maurer, T., & Nelson, A. (2021). The global cyber threat. Finance & Development, 24-27.

McLean, M. (2024, January 4). 2024 must-know cyber attack statistics and Trends. Embroker. https://www.embroker.com/blog/cyber-attack-statistics/

McMahan, B., & Ramage, D. (2017, April 6). Federated learning: Collaborative machine learning without centralized training data. Google Research Blog. https://blog.research.google/2017/04/federated-learning-collaborative.html

Mohsin, K. (2022). Data Privacy and Cybersecurity. Available at SSRN 4299439.

NSA. (2023, February). Best practices for securing your home network. Department of Defense. https://media.defense.gov/2023/Feb/22/2003165170/-1/-1/0/CSI_BEST_PRACTICS_FOR_SECURING_YOUR_HOME_NETWORK.PDF

Osakwe, M. (2021, May 13). The guide to identifying and securing pii leakage. Nightfall AI. https://www.nightfall.ai/blog/identifying-and-securing-pii-leakage-in-2021

Pratt, M. (2023, September 7). Emerging cyber threats in 2023 from AI to Quantum to data poisoning. CSO Online. https://www.csoonline.com/article/651125/emerging-cyber-threats-in-2023-from-ai-to-quantum-to-data-poisoning.html

Purplesec. (2023, February 22). 2023 Cyber Security Statistics Trends & Data. PurpleSec. https://purplesec.us/resources/cyber-security-statistics/

Taylor, P. (2024, January 18). U.S. households with Broadband internet 2021. Statista. https://www.statista.com/statistics/183614/us-households-with-broadband-internet-access-since-2009/#:~:text=Number%20of%20U.S.%20households%20with%20broadband%20internet%20access%202000%2D2021&text=The%20number%20of%20households%20in,the%20biggest%20online%20markets%20worldwide

Trend Micro. (2018, February 27). A look into the most noteworthy home network security threats of 2017. Security Roundup. https://www.trendmicro.com/vinfo/us/security/research-and-analysis/threat-reports/roundup/a-look-into-the-most-noteworthy-home-network-security-threats-of-2017

Victor, N., Alazab, M., Bhattacharya, S., Magnusson, S., Maddikunta, P. K. R., Ramana, K., & Gadekallu, T. R. (2022). Federated learning for iout: Concepts, applications, challenges and opportunities. arXiv preprint arXiv:2207.13976.