AI-Driven Cybersecurity Strategies for ISPs: Balancing Threat Mitigation and Monetization

Nakul Singh[1] and Shreyas Kumar[2]
[1]AI and Cybersecurity Practitioner, San Francisco, USA
[2]Department of Computer Science and Engineering, Texas A&M University, USA

nakul.singh@ieee.org
shreyas.kumar@tamu.edu

Abstract: As traditional revenue streams from bundled internet, voice, and TV services decline due to the rise of OTT platforms like Netflix and voice-over-IP services such as WhatsApp, Internet Service Providers (ISPs) are seeking innovative strategies to remain competitive. This white paper highlights the pivotal role of AI-driven cybersecurity in securing household video and data traffic across broadband, video streaming, and smart home devices, offering ISPs a powerful tool to enhance customer experiences and boost Average Revenue Per User (ARPU). By leveraging AI technologies, ISPs can safeguard and optimize the flow of data across connected homes, ensuring a seamless, secure, and high-quality experience for users. AI-driven cybersecurity solutions enable ISPs to monitor and protect video streaming content, gaming applications, and smart home devices such as IP cameras. These solutions not only enhance security but also improve network performance by identifying and mitigating potential vulnerabilities in real time. By integrating AI-powered cybersecurity tools with real-time Quality of Experience (QoE) analytics, ISPs gain deep insights into user behavior and device interactions. This allows them to proactively address issues such as data breaches, service interruptions, and latency, ensuring uninterrupted and high-quality service delivery. Armed with these insights, ISPs can create personalized service bundles that combine premium cybersecurity features with high-demand offerings such as 4K streaming, low-latency gaming, and smart home automation. For example, ISPs can offer tailored packages that include advanced firewall protection, parental controls, and IoT device management alongside premium content and high-speed internet options. These AI-driven bundling strategies not only enhance the security and performance of connected devices but also unlock new revenue streams by upselling premium packages to customers. Additionally, value-added features such as real-time security alerts, periodic reports, and integrated support services foster customer trust and loyalty. By leveraging AI to optimize both security and service delivery, ISPs can reduce churn, increase customer satisfaction, and significantly boost ARPU. This strategic approach positions ISPs as leaders in the competitive broadband and entertainment landscape, enabling them to thrive in an era of evolving consumer demands and technological advancements.

Keywords: AI, Cybersecurity, Monetization, ISPs, Smart homes, QoE

1. Introduction

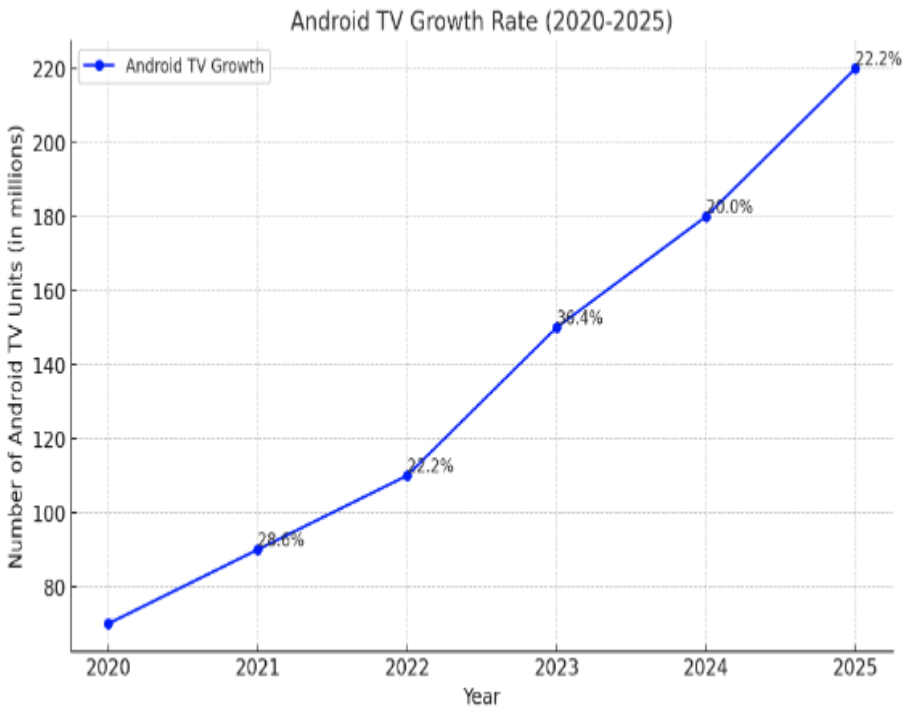
The global broadband and telecommunications industry is undergoing rapid transformation due to shifting consumer behaviors, emerging technologies, and increasing competition. Despite investments in next-generation connectivity solutions like 5G and fiber, Average Revenue Per User (ARPU) continues to decline, projected to fall by up to 4% (Baumgartner, 2024). Broadband ARPU varies significantly, from $54 per month in the U.S. to an average of $7 across APAC and as low as $2 in India. Meanwhile, OTT platforms and VoIP services continue to dominate the digital entertainment and communication market. For example, the Android TV (ATV) platform alone had a global market size of $5.6 billion in 2023 (Cognitive Market Research, 2023). This dominance further reduces ISPs' ability to differentiate themselves through traditional service bundles.

The growth of Android TV reflects this trend, with units projected to rise from 70 million in 2020 to 220 million by 2025.

As consumers increasingly rely on digital services, security threats have escalated (Arghire, 2023; Purdue University, 2023). *Vulnerabilities in video streaming apps, insecure communications, and weak authentication mechanisms expose users to risks such as data breaches and unauthorized access.* To remain competitive, ISPs must go beyond speed and reliability by integrating AI-driven cybersecurity and personalized service offerings into their business models.

This white paper proposes AI-driven cybersecurity as a strategic solution to safeguard household data and enhance customer experiences (CX). By integrating AI-driven security into their offerings, ISPs can:

- Unlock new revenue streams.
- Increase ARPU.
- Reduce churn and operational expenses.



Personalized smart home services and CX-driven offerings are emerging as critical differentiators, enabling ISPs to thrive in a dynamic market. Successful implementation of this strategy not only creates new monetization opportunities but also positions ISPs as trusted partners in securing the connected home ecosystem.

2. Background

Internet Service Providers (ISPs) have traditionally relied on bundled service internet, voice, and TV to generate revenue. However, the rise of over-the-top (OTT) platforms like Netflix and communication apps like WhatsApp has disrupted this model, reducing traditional revenue streams. With non-industry players offering affordable streaming and VoIP services, consumers now have more choices than ever. As a result, ISPs are pushed to compete on high-speed connectivity and low latency, often depending on advanced residential gateways and routers. Yet, while hardware-centric models remain essential, they do not create sustainable new revenue streams.

Simultaneously, the rapid adoption of smart TVs, smartphones, and IoT devices has expanded the attack surface for cyber threats. Households face increased risks from insecure streaming apps, weak authentication mechanisms, and compromised smart home integrations. To address these vulnerabilities, ISPs are turning to AI-driven cybersecurity solutions embedded within residential gateways and routers. *These hybrid solutions not only secure connected homes but also offer ISPs opportunities to enhance customer experiences and unlock new monetization strategies.*

2.1 Commercial Landscap

The market for AI-driven cybersecurity solutions in routers includes offerings from major players like Netgear, Cisco, and TP-Link, providing basic threat detection, firewall management, and parental controls. Advanced models incorporate machine learning to identify unusual network patterns, offering proactive defense. However, these solutions often focus on isolated functions and lack comprehensive integration with ISP infrastructure.

A significant gap exists in delivering real-time, adaptive security measures fully integrated with ISP level analytics and services. Many products lack deep insights into user behavior and device interactions, limiting their ability to provide value-added services for ISPs. This paper addresses these gaps in already commercially available routers by proposing a strategy that enhances security and presents different ideas to create new revenue streams for ISPs.

3. Essential Features of AI-Enhanced Cybersecurity Software in Residential Routers

Modern residential routers have evolved beyond basic network monitoring to integrate AI-driven cybersecurity software. These next-gen routers provide unified wireless networking, smart home management, and advanced security. Acting as central hubs for devices like Android TVs, IP cameras, and IoT sensors, they offer personalized insights and improve Quality of Experience (QoE). Embedded AI enables real-time monitoring, alerts, and seamless security enhancements without additional hardware.

Key Features of AI-Driven Cybersecurity Software:

1. Home Insights for Security: 15% of U.S. households have abandoned their monitoring services, citing false alarms, high fees, and perceived lack of value as key reasons. AI-driven software enhances home security by analyzing RF signals to detect and classify devices connected to the network. This allows routers to monitor the real-time presence or absence of known devices (residents). Unlike traditional security cameras, AI software offers deeper insights and extends coverage through MESH extenders, enabling broader home monitoring.

- Use Case: If a regularly present device is no longer detected, the system can flag it as a potential issue (e.g., tampering or removal). It can also notify users if an unknown device connects, ensuring comprehensive security.

2. Video streaming app QoE Analytics: Quality of Experience (QoE) analytics is critical for Internet Service Providers (ISPs) to understand how well their video streaming app services meet user expectations. With the integration of video streaming QoE analytics, the software allows ISPs to track and monitor the real-time performance of video streaming services, focusing on parameters like event titles, resolution, frame data, buffering, app usage time, and connection speed. The AI within the router correlates this data with network traffic to assess the end-to-end QoE, ensuring video streams deliver optimal quality and identifying any performance or security issues.

- Use Case: If buffering or low-quality streaming is detected, the system can isolate whether the issue is related to local network congestion, the content delivery network (CDN), or a device problem.

3. Enhanced Parental Controls: By leveraging AI insights, ISPs can offer enhanced parental control features. The AI can track content usage and even block access to specific platforms or content types based on age appropriateness or user preferences. This improves user experience by making the home network safer for families.

- Use Case: Parents can set restrictions for certain apps or streaming services, ensuring their children only access appropriate content while enjoying a smoother streaming experience.

4. Streaming App Popularity: The system can track which streaming apps are being used most frequently, providing valuable insights for ISPs to secure and optimize service delivery. If certain apps are being used frequently, the system can prioritize traffic for those apps to ensure the best possible user experience and even provide marketing opportunities for ISPs.

- Use Case: The router might prioritize bandwidth for popular apps or automatically suggest bundled services based on usage trends.

5. Proactive Service Monitoring: The AI-driven software provides proactive service monitoring by building custom dashboards for ISPs. These dashboards allow for real-time tracking of video app stability and can alert providers when issues like app crashes, instability, or low QoE metrics occur. This reduces the need for costly support interventions (truck rolls and customer care calls), which directly lowers operational expense (OPEX) and improves service efficiency.

- Use Case: If the system detects a pattern of crashes or app freezes, the ISP can be alerted and potentially fix the issue remotely without requiring user intervention.

6. App Usability Insights: The software analyzes loading times and performance issues to identify network bottlenecks, CDN problems, enabling ISPs to optimize usability and satisfaction.

- Use Case: If loading times for a specific streaming app are unusually high, the system can identify whether it's a problem with the local network, the app itself, or external factors like CDN issues.7

7. Data Privacy and Encryption: The AI-driven cybersecurity software prioritizes user privacy by implementing end-to-end encryption (E2EE) for all data transmissions, including video streaming and IoT communications.

Additionally, sensitive data is anonymized to ensure that personal information cannot be traced back to individual users. These measures not only protect against cyber threats but also ensure compliance with global data privacy regulations such as GDPR and CCPA.

8. Vulnerability Scanning and Patch Management: This module would actively scan video streaming apps, smart home devices, and connected services for known vulnerabilities, misconfigurations, or outdated software. It could automatically notify the user or service provider about critical patches and updates, or even schedule updates to improve security. By integrating with a database of known CVEs (Common Vulnerabilities and Exposures), the software could proactively monitor and patch vulnerabilities, particularly in streaming apps or IoT devices that have weak security practices or outdated firmware.

- Use Case: If a known security flaw in a video streaming app is identified, the software would flag this and either guide the user to update the app or automatically install a patch if possible.

9. End-to-End Encryption (E2EE) for Video Streaming & IoT Communication: The software could implement Transport Layer Security (TLS) or DTLS (Datagram TLS) for securing streaming traffic and communications between home devices. For IoT devices, protocols like MQTT over TLS or HTTPS can be used. Additionally, the software must also address DDoS attacks, botnets, and ransomware targeting smart home devices or streaming services.

- Use Case: To protect user data and streaming traffic from eavesdropping or man-in-the-middle (MITM) attacks, ensure that all communication between devices (Android TV, streaming apps, IoT devices, and the router) is encrypted.

10. AI-Driven Anomaly Detection (for Insecure Communications): The AI in the router could continuously monitor all inbound and outbound traffic, looking for any deviations from typical usage patterns, which could indicate a breach, insecure communication, or data exfiltration attempts.

- Use Case: If the router detects that an IoT device is sending data to an external server at an unusual rate or to an unrecognized IP address, an alert is triggered for the user or service provider to take action.

11. Smart Home Device Security Monitor: This software component focuses on IoT device vulnerabilities and integrates with popular smart home ecosystems (like Amazon Alexa, Google Home, or Apple HomeKit). It can detect insecure devices and configurations and alert users about potential risks. It continuously monitors the devices for insecure default settings (e.g., open ports, weak passwords), misconfigurations, and vulnerabilities.

- Use Case: If a smart thermostat is using weak or default credentials, the software would notify the user to change the password or update the device firmware.

12. Access Control and Least Privilege Enforcement for IoT and Apps: The router software would enforce strict policies to restrict which devices can communicate with one another. For example, IoT devices might be allowed to communicate only with certain apps or services, reducing the attack surface and limiting unauthorized access.

- Use Case: The system could block an IoT device from communicating with external servers unless explicitly allowed by the user, reducing the risk of data leakage.

13. Device Fingerprinting & Behavioral Analytics: It analyzes the unique characteristics of each connected device like the hardware ID, device name, or network usage patterns and stores this information. If a device suddenly behaves out of pattern, it could trigger an alert or block the device until further validation.

- Use Case: If a streaming app starts to make unusually frequent requests to external servers (indicating a bot or a malicious app), the router's software would identify this anomaly and either isolate the device or alert the user.

14. Multi-Factor Authentication (MFA) for App Access & Device Management: The router software could enforce two-factor authentication (2FA) using SMS, email, or even biometric authentication (like fingerprint or face recognition) for app logins or device access. Additionally, it could integrate with OAuth or SAML for external service authentication.

- Use Case: When accessing the router's web interface or the video streaming app, the user would need to verify their identity via an additional layer (like a push notification or one-time password) beyond just the regular password.

4. AI Algorithms in Cybersecurity

The AI-driven cybersecurity solutions proposed in this white paper rely on a combination of machine learning (ML) and deep learning (DL) algorithms to detect and mitigate threats in real time. Below are the key algorithms and their roles:

1. Neural Networks for Anomaly Detection:

- *Convolutional Neural Networks (CNNs): Used for analyzing network traffic patterns and identifying anomalies. CNNs are particularly effective in detecting unusual patterns in video streaming traffic, such as sudden spikes in data usage or unauthorized access attempts.*
- *Recurrent Neural Networks (RNNs): Ideal for time-series data, RNNs are used to monitor continuous network traffic and detect deviations from normal behavior, such as unusual data exfiltration or botnet activity.*

2. Deep Learning for Threat Classification:

- *Deep Neural Networks (DNNs): These are employed to classify threats based on historical data. For example, DNNs can differentiate between a legitimate video streaming request and a Distributed Denial of Service (DDoS) attack by analyzing packet headers and payloads.*
- *Generative Adversarial Networks (GANs): GANs are used to simulate potential cyberattacks, allowing the system to train on synthetic attack data and improve its ability to detect real-world threats.*

3. Reinforcement Learning for Adaptive Security:

- *Q-Learning: This algorithm enables the system to adapt its security policies based on real-time feedback. For example, if a particular IoT device is repeatedly flagged as vulnerable, the system can automatically enforce stricter access controls or isolate the device from the network.*

4. Natural Language Processing (NLP) for Phishing Detection:

- *BERT (Bidirectional Encoder Representations from Transformers): NLP models like BERT are used to analyze email content and detect phishing attempts by identifying suspicious language patterns or malicious links.*

5. Technical Challenges and Risk Mitigation

1. Resource Constraints on Routers:

- *Residential routers often have limited processing power and memory, which can pose challenges for running resource-intensive AI algorithms. To mitigate this, model quantization and pruning techniques are used to reduce the size of ML models without compromising accuracy.*
- *Additionally, federated learning can be employed to train AI models across multiple routers, reducing the computational burden on individual devices.*

2. Data Privacy Concerns:

- *The AI software anonymizes sensitive data before processing it, ensuring compliance with global data privacy regulations such as GDPR and CCPA. For example, personally identifiable information (PII) is stripped from network traffic logs before they are analyzed by the AI algorithms.*
- *Differential privacy techniques are also used to ensure that individual user data cannot be traced back to specific households.*

3. Integration with Legacy Systems:

- *Many ISPs still rely on legacy infrastructure, which may not be compatible with modern AI-driven solutions. To address this, API-based integration is used to connect the AI software with existing systems, ensuring seamless operation without requiring a complete overhaul of the network.*

4. False Positives in Threat Detection:

- *AI algorithms may occasionally flag legitimate traffic as malicious, leading to false positives. To reduce this risk, ensemble learning techniques are used, where multiple models are combined to improve accuracy. For example, a decision from a CNN can be cross-verified by an RNN before a threat is flagged.*

6. Go-To-Market and Monetization Strategy

ISPs can have access to substantial amounts of data and information related to customer engagement in a household through AI-driven hybrid solutions that merge video streaming and broadband services. This solution helps manage connected devices in a smart home, such as SmartTVs, gaming consoles, IP cameras, thermostats, and IoT sensors (motion, temperature, etc.), while offering enhanced security and personalization. The goal is to monetize these capabilities to increase ARPU (Average Revenue Per User) through premium features and upsell opportunities.

Using data analytics on customer data, segmentation is the foundation for every effort to increase ARPU. One-size-fits-all strategies are a thing of the past, and research confirms that end customers require more personalization from their ISPs. Through a deep understanding of real-time subscriber health and Quality of Experience (QoE) metrics across locations, devices, and applications running on multiple platforms in a connected smart home, ISPs can unlock significant growth opportunities. According to a Ciena blog post on AI monetization, communication service providers can drive revenue growth by leveraging AI to deliver personalized services, optimize network performance, and enhance customer experiences. For example, AI-driven insights can enable ISPs to offer tailored service bundles, such as combining premium cybersecurity features with high-demand offerings like 4K streaming and smart home automation (Sant'Anna, 2024).

ISPs can use a super bundling subscription strategy that involves offering consumers a package of multiple subscription services at a discounted price (Baumgartner, 2024). By integrating AI-driven cybersecurity and smart home management into these bundles, ISPs can create compelling value propositions that drive customer adoption and loyalty. For instance, offering advanced parental controls, real-time security alerts, and personalized insights as part of a premium package can significantly enhance the customer experience while increasing ARPU. Furthermore, the Ciena blog highlights that AI-driven solutions can improve operational efficiency by automating threat detection, network optimization, and customer support. This not only reduces operational costs but also ensures a seamless and secure experience for users. By adopting these strategies, ISPs can differentiate themselves in a competitive market and position themselves as trusted partners in securing the connected home ecosystem.

See Figure 1 sourced from Sant'Anna, 2024.

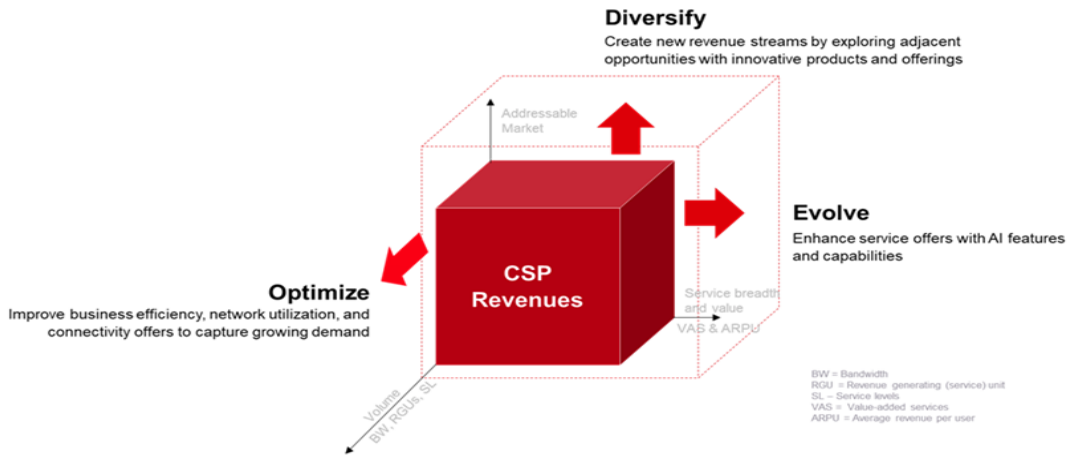


Figure 1: The three dimensions of revenue growth

7. Monetization Opportunities for the ISP

Here's how the ISP can monetize and increase ARPU through AI-driven cybersecurity and smart home management:

1. AI-Driven Cybersecurity Service (Premium Protection)

The AI-driven cybersecurity software inside the router offers real-time threat detection through use of neural networks and deep learning, vulnerability scanning, and automatic protection for all connected devices in the home network (SmartTV, gaming consoles, IP cameras, IoT devices, etc.).

- Monetization: Offer this as a premium service for $8/month, enhancing the security of users' connected devices against malware, phishing, hacking, and privacy violations.
- Example:
- *SmartTV: Protection from malware, data theft from third-party apps, or unauthorized access.*
- *Gaming Console: Protection from DDoS attacks, hacks, or malware targeting the console.*
- *IP Cameras: Protection against unauthorized access or remote hijacking.*
- *IoT Devices: Monitoring and protection against vulnerabilities, like thermostat or sensor hacks.*
- *Compliance as a Competitive Advantage: AI-driven cybersecurity services help ISPs build customer trust and gain a competitive edge by ensuring global data privacy compliance.*

2. Smart Home Management (Automation, Monitoring, and Control)

The router can offer integrated smart home management, which includes device monitoring, energy optimization, and automated actions for smart home devices like thermostats, lights, and sensors.

- Monetization: Offer smart home management as a premium service for $10/month, where users can control devices, automate actions (like adjusting the thermostat or lights), and receive insights about energy usage and security events.
- ISP targets the household with relevant offers such as discounts on a new smart thermostat or soundbar, potentially earning affiliate revenue or cross-selling other hardware.
- Example:
- *Thermostat: Automate temperature changes based on real-time data or occupancy, leading to energy savings.*
- *Smart Lighting: Set schedules or automate lighting based on room usage, time of day, or presence detection.*
- *Sensors: Automate actions like turning on lights or sending alerts if a motion sensor detects unexpected activity.*

3. Parental Control and Content Filtering

For families, the AI-driven software can offer advanced parental controls to limit screen time, block inappropriate content, and monitor usage across all devices.

- Monetization: Offer parental control features as an add-on for $5/month.
- Example:
- *Set limits on gaming time on consoles, restrict access to adult content on the SmartTV, and monitor app usage on mobile devices.*

4. Personalized Insights and Analytics

The AI software can provide users with data insights on their network's performance, device health, and security status. Users can receive personalized reports on data usage, device behavior, and potential areas of improvement (e.g., improving Wi-Fi performance or securing vulnerable devices).

- Monetization: Offer analytics and reports as an additional service for $5/month.
- Example:
- *The system could detect poor performance on the gaming console or SmartTV and offer recommendations to optimize bandwidth or upgrade the internet plan for smoother performance.*

5. Targeted Ads and Cross-Promotions

- Monetization: Using insights from device usage, the ISP targets the household with relevant offers such as discounts on a new smart thermostat or soundbar, potentially earning affiliate revenue or cross-selling other hardware.

Example Household Setup:

Let's assume a household has the following connected devices:

- SmartTV (for video streaming)
- Mobile Phones (multiple)

- Gaming Console (for online gaming)
- IP Cameras (for home security)
- IoT Devices: Thermostat, motion sensors, door/window sensors, and smart lights.

ARPU Calculation Before and After AI-Driven Cybersecurity and Smart Home Management

1. Before (Standard Internet Service)

In the standard scenario, the ISP might only be providing basic internet access, which includes Wi-Fi connectivity and basic router features.

- Base internet plan: $50/month
- Total ARPU: $50/month

2. After (With AI-Driven Cybersecurity and Smart Home Management)

Now, with the AI-driven cybersecurity software and smart home management integrated into the router, the ISP can offer the following premium services:

- Basic Internet Service: $50/month (unchanged)
- AI-Driven Cybersecurity: $8/month
- Smart Home Management: $10/month
- Parental Control & Content Filtering: $5/month
- Personalized Insights & Analytics: $5/month

3. Total ARPU after monetization:

- $50 (Base Internet) + $8 (Cybersecurity) + $10 (Smart Home Management) + $5 (Parental Control) + $5 (Analytics) = $78/month

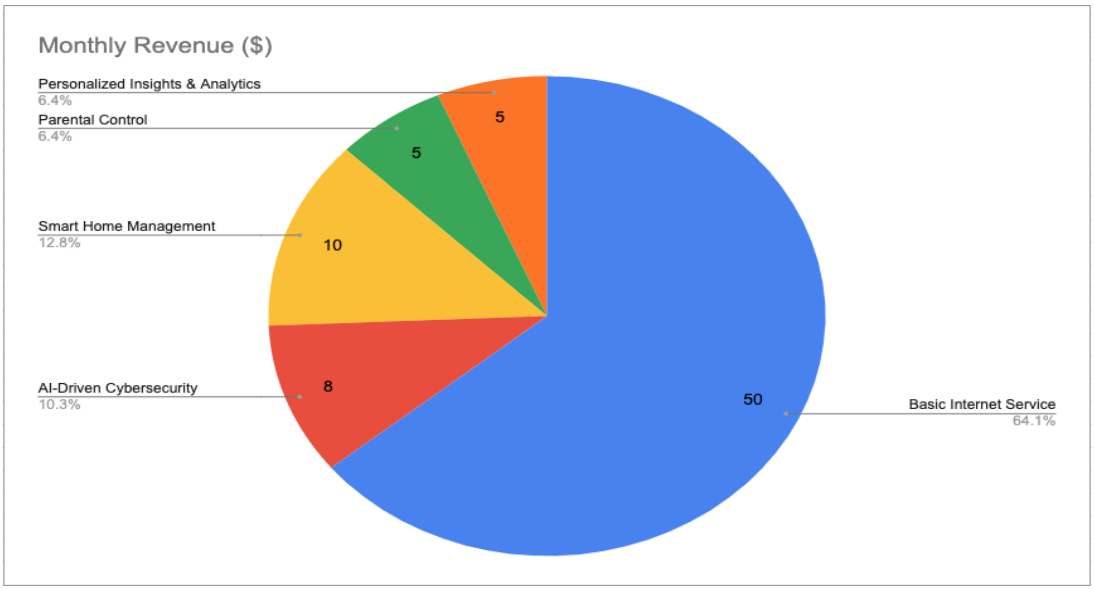
4. ARPU Increase Calculation

- Before: $50/month (basic internet service)
- After: $78/month (with premium AI-driven cybersecurity, smart home management, and personalized insights)
- ARPU Increase: $78 - $50 = $28/month

By integrating AI-driven cybersecurity and smart home management into the router, the ISP creates new revenue streams through premium services that cater to the growing needs of connected homes.

This strategy not only increases ARPU but also enhances customer loyalty and differentiates the ISP in a competitive market, providing a clear path for upselling and customer retention.

Here is a pie chart illustrating the contribution of different services to the new ARPU (Average Revenue Per User). The chart shows how the original ARPU ($50) is enhanced through premium services such as AI-driven cybersecurity, smart home management, parental controls, and personalized insights. These value-added services help to increase the total ARPU to $78 per month.



The cost-benefit analysis of AI-driven cybersecurity for ISPs reveals significant financial advantages. Initial costs include upgrading routers, developing AI software, and integrating systems, alongside ongoing operational and training expenses. However, the benefits outweigh these costs. ISPs can increase ARPU by offering premium cybersecurity services, reduce churn through enhanced customer trust, and achieve operational savings via automated threat detection and network optimization. Improved customer satisfaction further drives revenue growth. The return on investment is substantial, with a rapid break-even period. Overall, AI-driven cybersecurity not only boosts revenue but also strengthens customer loyalty and operational efficiency, positioning ISPs for long-term success in a competitive market.

8. Real-World Use Cases

One notable example of AI-driven cybersecurity in action is Comcast's xFi Advanced Security (Kangas, n.d.), which leverages artificial intelligence to protect connected homes from cyber threats. As highlighted in the Comcast Xfinity Cyber Health Report (Comcast, 2020) the implementation of AI-powered security solutions has led to significant improvements in network safety and customer satisfaction. The report highlights that Comcast's xFi Advanced Security blocked over 1.5 billion cyber threats in 2022 alone, with a 30% reduction in malware infections across protected networks. Additionally, Comcast observed a 20% increase in customer satisfaction among users of the service, as the AI-driven system proactively identifies and mitigates threats in real time, ensuring a seamless and secure online experience. This case study demonstrates how ISPs can leverage AI-driven cybersecurity not only to enhance security but also to drive customer loyalty and reduce churn. Similarly, AT&T's Internet Security and Deutsche Telekom's IoT Security solutions have reported a 25% reduction in customer churn and a 40% decrease in IoT-related security incidents, respectively (AT&T, 2023). These real-world examples underscore the potential of AI-driven cybersecurity to unlock new monetization opportunities, increase ARPU, and position ISPs as trusted partners in securing the connected home ecosystem.

9. Conclusion and Call to Action (CTA)

In this white paper, we discuss a range of strategies, technologies, and platforms designed to help Internet Service Providers (ISPs) better compete in the rapidly evolving broadband and video entertainment landscape. As ISPs embrace AI-driven cybersecurity and smart home management, they must also prioritize data privacy and regulatory compliance. By doing so, they can build trust with customers, differentiate themselves in a competitive market, and unlock new monetization opportunities. The time to act is now, ISPs that invest in privacy-compliant, customer-centric solutions will be best positioned to thrive in the digital economy.

ISPs must transition to customer experience-driven models that prioritize customer satisfaction over traditional hardware differentiation. By leveraging AI-driven software within routers and investing in personalized services, ISPs can reduce churn, increase ARPU, and stay competitive in an ever-evolving digital market. A deeper understanding of device usage, as illustrated in the examples above, allows ISPs to create new revenue streams by offering tailored services that meet the unique needs of each household.

Customer experience (CX) has emerged as the key differentiator in the broadband and telecom industry. Competing solely on price, coverage, or speed is no longer enough. The white paper outlines how ISPs can significantly improve home security, enhance the Quality of Experience (QoE) for video streaming, and protect IoT devices. By merging AI, cybersecurity, and service optimization into a unified offering, ISPs can distinguish themselves in a crowded market.

To stay relevant, ISPs must shift their mindset and become more experience-driven companies. This shift will help them tackle one of the most pressing industry challenges: customer churn while allowing them to offer more engaging, personalized, and satisfying experiences. Now is the time for ISPs to embrace digital innovation and leverage the full potential of excellent customer experience (CX).

By focusing on personalized services, smart home integration, and targeted advertising, ISPs can unlock significant growth opportunities. This strategy positions them to meet evolving consumer demands while maximizing revenue potential and enhancing customer satisfaction. As the digital landscape continues to evolve, the need for ISPs to prioritize experience and security is clearer than ever.

References

Arghire, I. (2023) *1.3 Million Android TV Boxes Infected by 'Vo1d' Malware* [Online]. SecurityWeek. Available at: https://www.securityweek.com/1-3-million-android-tv-boxes-infected-by-vo1d-malware/ [Accessed 26 January 2025].

AT&T. (2023) Cybersecurity Report [Online]. Available at: https://cdn-cybersecurity.att.com/docs/industry-reports/cybersecurity-insights-report-edge-ecosystem.pdf [Accessed 2 February 2025].

Baumgartner, J. (2024) *Charter leans harder into convergence with 'Life Unlimited'* [Online]. Light Reading. Available at: https://www.lightreading.com/cable-technology/charter-leans-harder-into-convergence-with-life-unlimited [Accessed 28 January 2025].

Baumgartner, J. (2024) *Comcast focuses on market segmentation as broadband losses continue* [Online]. Light Reading. Available at: https://www.lightreading.com/cable-technology/comcast-focuses-on-market-segmentation-as-broadband-losses-continue [Accessed 25 January 2025].

Cognitive Market Research. (2023) *Android TV Box Market Report* [Online]. Available at: https://www.cognitivemarketresearch.com/android-tv-box-market-report [Accessed 25 January 2025].

Comcast. (2020) *2020 Comcast Xfinity Cyber Health Report* [Online]. Available at: https://s46512.p629.sites.pressdns.com/wp-content/uploads/dlm_uploads/2020/11/Cyber-Security-Booklet_Digital_Final3.pdf [Accessed 2 February 2025].

Electronics Specifier. (n.d) *Fixed wireless access forecast 2023-2027* [Online]. Available at: https://www.electronicspecifier.com/news/analysis/fixed-wireless-access-forecast-2023-2027 [Accessed 27 January 2025].

European Union (2018) General Data Protection Regulation (GDPR). Brussels: European Union.

Kangas, S. (n.d.) *Artificial Intelligence* [Online]. Comcast. Available at: https://corporate.comcast.com/cyber-health-report/artificial-intelligence [Accessed 31 January 2025].

Kumar S.,Menezes, A., Giri, S. and Kotikela, S. 2024. What The Phish! Effects of AI on Phishing Attacks and Defence. 4th International Conference on AI Research (ICAIR), 05-06 Dec, Lisbon, Portugal.

Mobilise Global. (2023) *5 Ways to Increase ARPU in Telecom Industry* [Online]. Available at: https://www.mobiliseglobal.com/5-ways-to-increase-arpu-in-telecom/ [Accessed 31 January 2025].

National Institute of Standards and Technology (NIST) (2023) NIST Cybersecurity Framework. Gaithersburg, MD: National Institute of Standards and Technology.

Purdue University. (2023) *Purdue Researchers Uncover Vulnerabilities in Smart TVs* [Online]. Available at: https://engineering.purdue.edu/ECE/News/2023/purdue-researchers-uncover-vulnerabilities-in-smart-tvs [Accessed 26 January 2025].

Sant'Anna, F. (2024) *Artificial Intelligence Monetization: A New Revenue Growth Agenda for Communication Service Providers* [Online]. Ciena. Available at: https://www.ciena.com/insights/blog/2024/artificial-intelligence-monetization-a-new-revenue-growth-agenda-for-communication-service-providers [Accessed 2 February 2025].

State of California (2020) California Consumer Privacy Act (CCPA). Sacramento: State of California.

StreamTV Insider. (n.d) *Google, Android TV now boasts 150M monthly active devices* [Online]. Available at: https://www.streamtvinsider.com/video/google-android-tv-now-boasts-150m-monthly-active-devices [Accessed 26 January 2025].

Telecom Review. (2023) *Global Telcos in Q1 2023: ARPU Trends* [Online]. Available at: https://www.telecomreview.com/articles/reports-and-coverage/7215-global-telcos-in-q1-2023-arpu-trends/ [Accessed 26 January 2025].

Telecom Review. (2023) *Telecoms revenue per user is falling despite 5G and fibre rollouts* [Online]. Available at: https://www.telecoms.com/5g-6g/telecoms-revenue-per-user-is-falling-despite-5g-and-fibre-rollouts [Accessed 27 January 2025].