# Research Statement | Yunming Xiao, Fall 2024

My research centers on computer networks and systems that underpin Internet services and infrastructure. My overarching goal is to address the evolving demands driven by rapid growth of users, increased reliance on online services, and rising security and privacy concerns. Balancing multifaceted goals in **performance, security**, **privacy**, and **reliability** is a challenging task. Moreover, given the extensive deployment of existing services and infrastructure, rebuilding them from scratch is not a viable option – instead, we must creatively innovate within the constraints of existing systems. This further amplifies the challenge.

To address these challenges, my strategy follows a three-step process: ***measure***, ***build***, and ***deploy***. First, I conduct comprehensive measurements to identify vulnerabilities or mismatches with today's demands. I further analyze the root causes and derive insights for informed design decisions. Next, armed with these insights, I build systems that address the identified gaps with new designs, by revisiting past premises and leveraging techniques from other domains, such as cryptography and machine learning, which have become much more powerful in recent decades. Whenever possible, I take it a further step to deploy the systems I have built, so that my research would produce tangible, real-world impacts beyond publications.

As an example of this approach, in terms of my work on Internet services, I first conducted extensive measurements across a wide range of services, including web browsing behaviors [1-3], emerging web technologies [4, 5], and Internet-of-Things (IoT) [6-8]. I then developed new systems that address the vulnerabilities or adapt to evolving demands. For instance, after identifying a privacy issue in web browsing, I created Snatch [1], a system that restructures cookie content to mitigate privacy leaks, while accelerating online streaming analytics. In terms of deployment, my research on DVPN [4] has influenced developers to create more an efficient ecosystem, and a multimedia system that I created has gained media attention and been installed by over 30,000 users worldwide [8]. Likewise, I have collaborated extensively with Internet infrastructure providers to measure, build, and deploy systems at multiple layers of the infrastructure [9-15], resulting in real-world deployments in Tencent's Cloud, spanning tens of data centers, millions of servers, with a global user base.

My work has been published in top-tier conferences, including SIGCOMM, NSDI, SIGMETRICS, EuroSys, ATC, CoNEXT, and WWW, with a EuroSys Best Student Paper award. My research has received support from the National Science Foundation (NSF), where I contributed to drafting grant proposals that helped secure two NSF awards totaling 1.15 million USD. In terms of service, I have been invited to serve on the program committee for both networking and security venues, such as ACM CCS and APNet, and to serve as journal reviewers for JSAC and SIGCOMM CCR.

# Current Research

## Internet Services

The Internet has undergone significant evolution since its inception. Today, its services cater to a much broader range of purposes, from simple web browsing to complex online applications, and from traditional PCs to the IoTs which has become an integral part of daily life. Additionally, user demands have shifted: while performance was the primary concern when Internet was invented, security and privacy have received more attention today. Below, I highlight several projects that address these evolving challenges.

**Privacy in Web Browsing [1].** My inquiry began with web browsing. While widespread HTTPS has improved security by encrypting the channel between users and web servers (or in fact, the content delivery network), concerns over trustworthiness of web providers have grown with rising privacy awareness. HTTP cookies, used for personalization, pose privacy risks since they often store user identifiers that allow provider to track user information indefinitely, usually without users' knowledge. Additionally, my measurements show that these cookies limit the ability of edge systems to efficiently process data until it reaches distant data centers. To protect user privacy, I propose revising this system premise by introducing "semantic cookies" which embed necessary data directly instead of pointers to user databases. This allows faster analytics at the edge without changing existing HTTP protocols. I further developed Snatch [1], the first edge analytics prototype using semantic cookies. Global experiments show Snatch preserves privacy while speeding up anonymous user analytics. Snatch has won the *Best Student Paper Award* at EuroSys 2024.

**Domain Name Service [3].** The Internet is complex and multi-layered, and preserving security and privacy requires all layers to work together. With this in mind, my next project focused on the domain name service (DNS), the

"phonebook" of the Internet. Similar to web browsing, while DNS traffic can now be encrypted via HTTPS/TLS, the trustworthiness of DNS resolvers is increasingly questioned. DNS over Tor addresses this but my measurements revealed performance issues. Instead, I proposed that resolvers should operate "in the blind," resolving domain names without accessing their content, using a cryptographic method called Private Information Retrieval (PIR). However, integrating PIR into DNS faced three challenges: (i) PIR relies on a pre-populated database, but DNS caches are updated dynamically, which blind resolvers cannot handle; (ii) PIR is slow and struggles with DNS's high traffic and frequent updates; and (iii) new security risks. To address them, I proposed a custom DNS extension, optimized performance, and new security measures. The result is PDNS [3], a privacy-preserving DNS that augments, rather than replaces, current DNS. Evaluations show PDNS achieves privacy protection with competitive performance.

**Emerging Web Technology [4].** I have also explored emerging web systems, like Web3, which uses technologies like blockchain to build a decentralized and transparent web. Specifically, I focused on decentralized VPN (DVPN), which enhances security and privacy by distributing traffic across multiple parties, reducing data centralization. Several DVPN systems have become popular by allowing users to monetize idle bandwidth. My measurement of DVPN ecosystem [4] shows that DVPNs rival commercial VPNs in footprint and performance. But there are also concerns: traffic monitoring is still possible, DVPNs lack security features like traffic filtering, and current pricing is inefficient. To address these issues, I developed RING, a third-party system that allows providers to join multiple DVPN networks, optimize pricing, and improve security and usability. The measurement insights were also shared with DVPN developers, and one major developer, Mysterium, then implemented a more efficient pricing mechanism.

**Internet of Things security [6-8].** The average US household now has over 10 IoT devices, but these setups are vulnerable to various adversaries. A key distinction between attackers and legitimate users is the physical interaction (e.g., via a mobile app) required to operate IoT devices. These interactions can be used for frictionless authentication, but vendor-specific implementation is complex and costly. My analysis of IoT traffic suggests that most of the traffic, despite being encrypted, follows predictable, recurring patterns, while human-driven traffic exhibits learnable behaviors. Building on this, I designed FIAT, the first third-party frictionless authentication system for home IoT. FIAT operates passively on network traffic, requiring no modifications to IoT devices or apps. Evaluation shows that FIAT achieves high accuracy with minimal impact on the user experience.

While many IoT devices are simple, some, like Smart TVs, have more complex setups. For example, Kodi is a multimedia platform where users can install custom software called "add-ons", which are custom Python scripts. This poses risks, as malicious add-ons can track user behavior or cause harm. To investigate this, I first built de-Kodi [7], a platform that systematically analyzes Kodi add-ons. My analysis revealed that some add-ons do exhibit malicious behavior. However, since Kodi lacks a central add-on repository and they are spread across the web, it is hard to fully assess the problem. To address this, I further developed SafeKodi [8], a Kodi add-on that helps users identify and remove malicious add-ons while collecting feedback on installed add-ons to further expand scrutiny. SafeKodi's launch was very successful, receiving widespread media coverage and attracting over 30,000 users worldwide. As a result, this study not only sheds light on the Kodi ecosystem but also actually enhances user safety.

## Internet Infrastructure

Supporting these emerging Internet services is the underlying infrastructure, which has also significantly evolved over the past decades. Heterogeneous hardware – such as GPUs, programmable switches, SmartNICs, and FPGAs – has become common for performance acceleration, but realizing their full potential requires a careful design. Meanwhile, the growing scale and complexity of infrastructure have made management more challenging, with reliability becoming a prominent concern. With collaborators in industry and academic, I have gained insights from real-world environments, proposed solutions to address these challenges, and deployed systems at scale.

**Machine Learning Acceleration [9].** Specialized accelerators like GPUs are widely used for modern ML tasks, but previous research has pointed out inefficiencies due to CPU bottlenecks and suboptimal accelerator scheduling. To address both inefficiencies, I developed Conspirator [9], a control plane design that uses SmartNICs to eliminate CPU bottlenecks by enabling efficient data transfer without host CPU involvement. Conspirator also includes a new scheduling algorithm that optimizes the use of different accelerators and adapts to changing workloads, addressing scheduling inefficiencies. Evaluation shows Conspirator reduces end-to-end completion time, is more cost-effective and energy-efficient, and improves GPU usage. Conspirator has also led to multiple patent filings.

**Traffic Engineering [10].** TE is crucial for the performance of distributed applications. However, measurements show that some Internet services, such as online gaming, suffer from poor TE. Specifically, flows from the same gaming

server may be routed on different paths with varying latency, degrading service quality. This is because existing TE operates on aggregated traffic but not individual flows. To address this, my colleagues and I developed MegaTE [10], the first system to manage individual traffic flows at the virtual instance level (container/VM), scaling TE to millions of endpoints. MegaTE shifts the TE paradigm from centralized control to a bottom-up approach using eBPF-based segment routing and control plane optimization Simulations show that MegaTE supports 20x more endpoints with the same runtimes compared to previous solutions. MegaTE has been rolling it out in Tencent Cloud WAN.

**Cloud Gateway Reliability [11-13].** Let us move on to the reliability issues. Cloud gateways are the junction of data center and Internet. They integrate various networking functions to satisfy diverse application-layer demands. To handle growing workloads and reduce forwarding delays for time-sensitive operations, Tencent has adopted a heterogenous architecture where each node is composed of programmable switches, FPGAs, and commodity servers. This shift from traditional router/DPDK-based architectures requires new designs. Over the past few years, with my collogues, I have developed network functions for this new hardware, including lightweight BGP non-stop routing (NSR) [11], migration strategies for the new gateway architecture [12], and a packet tracing and analysis system for troubleshooting [13]. These solutions have been successfully rolled out in Tencent Cloud.

To elaborate on the BGP design [11], BGP is the only inter-domain protocol, but its failures can cause significant packet loss and instability. NSR ensures connectivity during failures by replicating BGP and TCP connection status for immediate recovery. However, traditional NSR solutions depend on OS kernel modifications, which are impractical for virtualized gateways. To address this, I proposed TENSOR, a lightweight, kernel-modification-free replication design by leveraging Netfilter. TENSOR supports gateway virtualization, ensures high performance, resolves the "split-brain" issue in NSR, and reduces development, deployment, and maintenance costs by orders of magnitude.

**Data Center Network Reliability [14].** Communication between servers within a data center also suffers from reliability issues. Measurements in production data centers show that gray failures, such as silent packet drops, are a major source of inefficiencies and failures. Flow re-pathing is identified as a fast and effective mitigation strategy, but its implementation is hindered by the wide use of equal-cost multi-path (ECMP) for load balancing in data centers. More concretely, ECMP introduces randomness that conflicts with precise traffic control (PTC) like flow re-pathing. To solve this, my collogues and I developed Programmable ECMP (P-ECMP) [14], a programming model, compiler, and runtime that utilizes ECMP groups – an often-overlooked feature – to provide effective PTC for critical traffic, while maintaining ECMP for the majority. Evaluations show that P-ECMP successfully enables various PTC and outperforms existing alternatives. P-ECMP has been deployed in Tencent Cloud for network failover.

# Future Directions

Reflecting on my current work, my design philosophy is to **renovate** existing Internet services rather than rebuild them from scratch. Rebuilding is impractical and less impactful because today's Internet services have been deployed at scale, and any incompatible system will struggle to gain adoption. More importantly, demands continuously evolve. So even if we design and deploy new systems that meet today's requirements, they will likely require costly adjustments in the future. Therefore, I argue that renovation is a more sustainable approach.

I also plan to expand my research beyond just the systems perspective. Many of the Internet renovations I have proposed rely on the latest cryptographic primitives and ML algorithms. However, through my experiences, these tools usually cannot be directly applied to current Internet systems. Systems need to be modified to adopt these primitives effectively. In the future, I plan to also explore whether new primitives can be designed to fit in the current systems. More concretely, rather than treating cryptography or ML as black boxes, I will contribute directly to these fields when necessary. For example, unlike PDNS [3], one potential project is developing more efficient PIR schemes tailored to the DNS system, which operates as a proxied system. Additionally, since DNS records are structured as a tree, optimizing PIR for this tree-like data organization could significantly enhance performance.

**Short-Term Goal – Internet Renovations.** My short-term research goal is to continue improving Internet services. The rationale is that existing Internet services are diverse and nested. For instance, a single click on a webpage involves multiple protocols and services, such as DNS, CDNs, and more. As a result, user security and privacy cannot be fully protected unless the entire chain of services is secure. Building on my previous work, I plan to address open issues such as end-to-end DNS authentication, more efficient web application firewalls for CDNs, and a more robust DVPN. Additionally, I aim to explore more Internet services such as advertisement systems, public key infrastructure,

and more decentralized applications, all of which could significantly benefit from renovations. Beyond these individual efforts, I further aim to develop a general framework for evaluating existing systems to systematically identify vulnerabilities, and building practical, secure, and privacy-preserving solutions. This framework will ensure that security and privacy are embedded as fundamental features of future Internet services.

**Medium-Term Goal – Cloud Ecosystem.** As cloud rapidly expand in functionality and scale, effectively managing resources while maintaining performance and reliability has become a critical challenge. Compared to many Internet services, the cloud is still relatively young, allowing for more significant and dramatic innovations. I plan to explore solutions that enhance both the software and hardware aspects of the cloud. On the software side, one key research question is how to address issues like resource circular dependencies, which can degrade system performance and resilience. It is also valuable to develop systems that intelligently and efficiently allocate resources while avoiding common pitfalls in cloud orchestration. On the hardware side, there are intriguing problems such as managing heterogeneous hardware for optimal performance while keeping this complexity invisible to users and even programmers. Ensuring reliability across diverse hardware also remains a significant challenge that I aim to tackle.

**Long-Term Goal – Industrial Infrastructure.** In the long term, I plan to extend my research from digital infrastructure to industrial systems. Digital infrastructures like the cloud rely heavily on industrial systems such as power grids, cooling systems, 5G, satellite, and more. As the digitalization of industrial infrastructure accelerates, these systems are expected to become more intelligent through enhanced computational capabilities. This presents a timely opportunity for the computing community to make significant contributions. Integrating these infrastructures will pose complex computing and networking challenges, much like cloud management today, but more intricate due to the diversity of systems involved. I have already started delving into this direction by designing a co-simulator [15], enabling the co-optimization of industrial infrastructures. Beyond that, I envision a broader picture: creating a new language, runtime, and control platform to codify, manage, and optimize interdependencies across infrastructures.

# References **(* Equal Contribution, # Corresponding Author)**


[1] **Yunming Xiao**, Yibo Zhao, Sen Lin, Aleksandar Kuzmanovic. *Snatch: Online Streaming Analytics at the Network Edge*. In EuroSys 2024. ***Best Student Paper Award***.

[2] Shihan Lin, Suting Chen, **Yunming Xiao#**, Yanqi Gu, Xiaowei Yang, Aleksandar Kuzmanovic. *PreAcher: Secure and Practical Password PreAuthentication by Content Delivery Networks*. To appear in NSDI 2025.

[3] **Yunming Xiao**, Chenkai Weng, Ruijie Yu, Peizhi Liu, Matteo Varvello, Aleksandar Kuzmanovic. *PDNS: Collusion Resistant DNS With Private Information Retrieval.* In Submission.

[4] **Yunming Xiao**, Matteo Varvello, Aleksandar Kuzmanovic. *Moneitizing Spare Bandwidth: The Case of Distributed VPNs*. In SIGMETRICS 2022.

[5] **Yunming Xiao**, Sarit Markovich, Aleksandar Kuzmanovic. *Blockchain Mining: Optimal Resource Allocation*. In ACM Advances in Financial Technologies (AFT) 2022.

[6] **Yunming Xiao**, Matteo Varvello. *FIAT: Frictionless Authentication of IoT Traffic*. In CoNEXT 2022.

[7] Marc Anthony Warrior, **Yunming Xiao**, Matteo Varvello, Aleksandar Kuzmanovic. *De-Kodi: Understanding the Kodi Ecosystem*. In WWW 2019.

[8] **Yunming Xiao**, Matteo Varvello, Marc Anthony Warrior, Aleksandar Kuzmanovic. *Decoding the Kodi Ecosystem*. In Transactions on the Web (TWEB), 2023.

[9] **Yunming Xiao**, Diman Zad Tootaghaj, Aditya Dhakal, Lianjie Cao, Puneet Sharma, Aleksandar Kuzmanovic. *Conspirator: SmartNIC-Aided Control Plane for Distributed ML Workloads.* In USENIX ATC 2024.

[10] Congcong Miao*, Zhizhen Zhong*, **Yunming Xiao***, Feng Yang*, Senkuo Zhang*, Yinan Jiang, Zizhou Bai, Chaodong Lu, Jingyi Geng, Zekun He, Yachen Wang, Xiangneng Zou, Chuanchuan Yang. *MegaTE: Extending WAN Traffic Engineering to Millions of Endpoints in Virtualized Cloud*. In SIGCOMM 2024.

[11] Congcong Miao*, **Yunming Xiao***, Marco Canini, Ruiqiang Dai, Shengli Zheng, Jilong Wang, Jiwu Bu, Aleksandar Kuzmanovic, Yachen Wang. *TENSOR: Lightweight BGP Non-Stop Routing*. In SIGCOMM 2023.

[12] Congcong Miao*, **Yunming Xiao***, Dongbo Gu, Yinchao Yang, Miantao Wan, Chao Pei, Jilong Wang, Aleksandar Kuzmanovic, Zaoxing Liu. *Seamless Migration of Stateful Gateway in Large-Scale Cloud*. In Submission.

[13] **Yunming Xiao**, Yinchao Yang, Xuqian Li, Dongbo Gu, Miantao Wan, Chao Pei, Aleksandar Kuzmanovic, Congcong Miao. *UPath: Unified Packet Tracing and Analysis for Heterogeneous Cloud Gateways*. In Submission.

[14] Yadong Liu*, **Yunming Xiao***, Xuan Zhang, Weizhen Dang, Huihui Liu, Xiang Li, Jilong Wang, Aleksandar Kuzmanovic, Ang Chen, Congcong Miao. *Unlocking ECMP Programmability for Precise Traffic Control.* To appear in NSDI 2025.

[15] Jiaheng Lu, **Yunming Xiao**, Shmeelok Chakraborty, Silvery Fu, Yoon Sung Ji, Ang Chen, Mosharaf Chowdhury, Nalini Rao, Sylvia Ratnasamy, Xinyu Wang. *OpenInfra: A Co-simulation Framework for the Infrastructure Nexus*. In HotInfra 2024.