Collaboration-Enabled Intelligent Internet Architecture: Opportunities and Challenges

Yi Zhao, Ke Xu, Jiahui Chen, and Qi Tan

Abstract

Since intelligent algorithms such as deep learning (DL) have strong expressiveness, flexibility, and scalability for complex problems, some DL-based methods have been applied to Internet architecture-related scenarios, such as congestion control and malicious traffic detection. However, DL-based models have relatively high requirements for resources such as data and computing, and the existing Internet architecture requires further evolution to break through these limitations. In this article, we propose the collaboration-enabled intelligent Internet architecture, which can leverage intelligence to facilitate the evolution of Internet architecture in more complex scenarios. Specifically, we first discuss the inherent opportunities and challenges of enabling the Internet architecture to be intelligent through collaboration, which are brought by the imbalance of Internet supply and demand, distributed organizational structure, and the lack of built-in security. Immediately after, we present the newly proposed collaboration-enabled intelligent Internet architecture, which consists of heterogeneous hardware infrastructure and a collaboration-oriented software service platform. Through the complementarity of these two components (i.e., providing hierarchical computing and full exploitation of hierarchical capabilities), it promotes the collaboration of intelligent algorithms built into the Internet architecture. Moreover, some flexible algorithmic modules for the proprietary requirements of the Internet architecture are built into the software service platform. Finally, we take multi-classification malicious traffic detection as a case study, and demonstrate the advantages of enabling Internet architecture to be intelligent through collaboration.

Introduction

The explosive growth in the number of Internet users and applications requires continuous optimization of services provided by the Internet, such as deterministic security, high throughput, and low latency. Therefore, the Internet architecture has been evolving to continuously optimize various performance metrics. However, these problems that the Internet architecture solves are also increasingly complex, for example, the proliferation of state dimensionality and the coexistence of multiple optimization objectives. Taking malicious traffic detection as an example, the existing traffic scrubbing requires high monetary expenditures because attackers will hide their attack characteristics in complex traffic patterns, and traffic blackhole will violently endanger legitimate traffic. Similarly, although explicit congestion notification (ECN) is widely utilized by congestion control schemes, traditional static ECN-based congestion control cannot adapt to high-speed production networks [1], failing to provide high-bandwidth and low-latency transmission services.

To solve complex problems in various scenarios, the evolution of Internet architecture toward artificial intelligence (AI) has achieved remarkable results. For example, to address the issue that static ECN-based congestion control has become a bottleneck in high-speed datacenter network, Yan *et al.* [1] propose an intelligent solution based on deep reinforcement learning (DRL). The DRL-based solution automatically configure ECN marking threshold according to the environmental state, which significantly improves the data transmission efficiency. Fu *et al.* [2] integrate frequency domain features and intelligent algorithms to detect malicious traffic, which is more effective against unknown attacks.

Although intelligent algorithms such as deep learning (DL) or deep neural networks (DNNs), have obvious advantages in complex problems, they require sufficient data and computing resources as a basis. However, partial devices (e.g., routers and switches) in the existing Internet, cannot provide the corresponding resources. In other words, resource constraints limit the widespread deployment of intelligence in existing Internet architecture. The existing Internet architecture requires the evolution of hardware foundation, software services and intelligent algorithms to support intelligence.

To enable more Internet devices[1] in the transmission path (not just end devices or bypass devices) with intelligence capabilities, we find that collaboration is a path that naturally matches the Internet architecture. First of all, the devices in the Internet follow a distributed organizational structure and cooperate with each other to perform various transmission tasks. Second, collaborative learning frameworks (e.g., federated learning [3, 4]) allow individuals to jointly optimize models under limited computing and storage resources, reducing resource requirements and protecting individual privacy.

In this article, we propose a collaboration-en-

[1] Note that the device here is not just hardware, but also covers the tasks it supports, such as malicious traffic detection and congestion control.

Digital Object Identifier: 10.1109/MNET.001.2200227

The authors are with the Department of Computer Science and Technology, Tsinghua University, China; Ke Xu (corresponding author) is also with Zhongguancun Laboratory, China.

abled intelligent Internet architecture, which not only involves the collaboration of intelligent algorithms, but also integrates hardware and software services. Under our proposed collaboration-enabled intelligent Internet architecture, the intelligent activities of a single individual are illustrated in Fig. 1, which mainly includes three stages: *perception*, *decision-making*, and *collaboration*. Specifically, in the *perception* stage, the individual perceives various states of the Internet, thereby providing the necessary inputs for the *decision-making* stage. Moreover, through device perception, the existing and synergistic computing resources can be identified to provide computing guarantees for the *decision-making* stage. In the *decision-making* stage, the control plane and the data plane are separated, and each has intelligent capabilities, which is an effective intelligent implementation approach. Among them, data plane AI can directly participate in Internet services (e.g., malicious traffic detection and congestion control), and control plane AI can optimize the corresponding configuration. On the basis of independent intelligence, individuals also need to cooperate with each other. In the *collaboration* stage, individuals participate in data-oriented collaboration, model-oriented collaboration and computation-oriented collaboration. Note that these intelligent activities of each individual are supported by our proposed collaboration-enabled intelligent Internet architecture.

To pave the way for collaboration-enabled intelligent Internet architecture, we first discuss the opportunities and challenges for collaboration to enable intelligent Internet architecture from different perspectives, including existing foundations and development trends. Subsequently, due to the inability of the existing Internet architecture to guarantee computing and data, we propose the collaboration-enabled intelligent Internet architecture, which integrates heterogeneous hardware infrastructure and collaboration-oriented software service platform to support collaboration. Through the cooperation of each other, the evolution of the Internet architecture can be accelerated to adapt to more unknown scenarios. Moreover, inspired by the proprietary requirements of Internet architecture, the referred platform designs a variety of flexible and diverse intelligent algorithmic modules. In addition, we take the multi-classification malicious traffic detection as a case study to illustrate the positive effects of collaboration experimentally. We summarize the key contributions of this article as follows:

- Based on a comprehensive analysis of supply-demand imbalance, distributed organizational structures, and security flaws, we for the first time discuss the inherent opportunities and challenges of enabling the Internet architecture to be intelligent through collaboration.
- Through the joint innovation of hardware and software platforms, as well as intelligent algorithmic modules, we propose the collaboration-enabled intelligent Internet architecture, which facilitates the evolution of Internet architecture in more complex scenarios.
- Via case studies on multi-classification malicious traffic detection with two datasets and Non-IID configuration, we experimentally demonstrate the salient advantages that collaboration brings to Internet architecture.

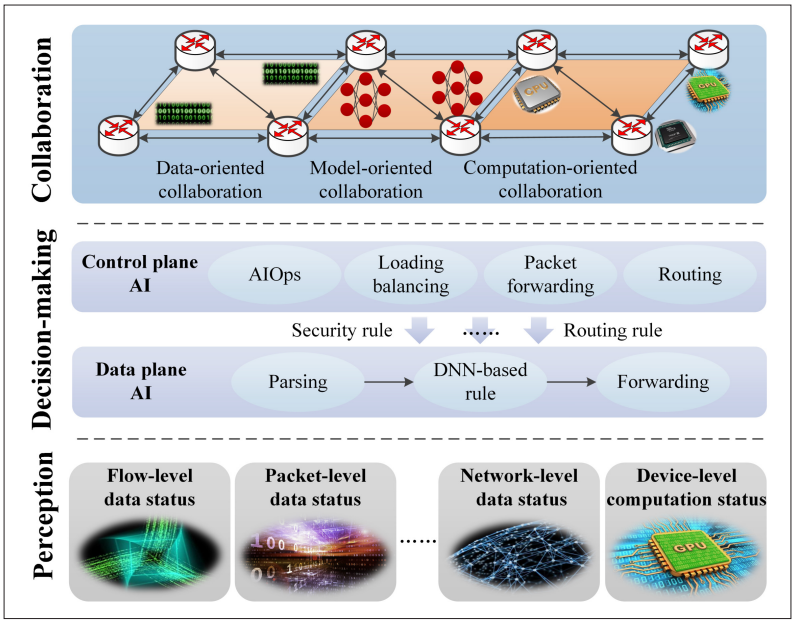

FIGURE 1. Under our newly proposed collaboration-enabled intelligent Internet architecture, part of the activities related to intelligence that a single individual can participate in.

Related Work

In recent years, the demands of the Internet in terms of deterministic security, high throughput, and low latency have been continuously improved. Due to the advantages of intelligent algorithms such as DL or DNN in dealing with complex problems, many supporting technologies for the Internet are further optimized with intelligence [2, 5]. For example, in high-throughput scenarios, unsupervised learning methods [2, 6] are applied to improve the accuracy of network intrusion detection. Chen *et al.* [5] proposed a DRL-based system to achieve datacenter-scale traffic optimization. However, existing intelligence for Internet architecture are mainly deployed on a single network device. Even though multiple devices are intelligent, they lack cooperation with each other. For example, although DRL-based scheme for dynamic ECN marking thresholds [1] is deployed on multiple switches, the agents on these switches are independent of each other, and there is no cooperative utilization of states observed by different agents.

In fact, the devices in the Internet are interconnected with each other and naturally have the ability to transmit information (i.e., cooperation through information exchange or sharing). Moreover, much literature [7, 8] confirms that collaboration can better explore the value of local data. For example, Hu *et al.* [8] propose a federated video analytics architecture, in which edge nodes transmit their own analysis results on the basis of maintaining privacy, which effectively improves the accuracy of video analysis. In addition, co-training a model directly through collaborative learning algorithms such as federated learning is also a way to achieve collaboration [3, 9]. For example, for unreliable wireless systems,

For the Internet architecture, there are both opportunities and challenges to achieve intelligence through collaboration. Existing research emphasizes the application of collaboration to a specific problem, or algorithm optimization.

Salehi *et al.* [9] propose a federated learning algorithm to enable resource-constrained devices to jointly train the intelligent model. However, collaborative learning also exposes vulnerabilities in poisoning attacks [10], backdoor attacks [4], and so on, and requires the incorporation of corresponding defense mechanisms at the beginning of the design. Especially in such an important scenario as the Internet architecture, security threats are more worthy of attention.

For the Internet architecture, there are both opportunities and challenges to achieve intelligence through collaboration. Existing research emphasizes the application of collaboration to a specific problem, or algorithm optimization. In this article, we integrate software and hardware to implement collaboration-enabled intelligent Internet architecture, which in turn supports collaboration in a wider range of scenarios.

Inherent Opportunities and Challenges for Internet Architecture

Since the beginning of ARPANET, the Internet architecture has been constantly evolving. These technological evolutions are due to continuous changes in the relationship between supply and demand, resulting in many advanced technologies.

The collaboration-enabled intelligent Internet architecture is also driven by a variety of internal opportunities and challenges, including supply-demand imbalance, distributed organizational structure, and necessary security assurance. In this section, therefore, we discuss why collaboration-enabled intelligent Internet architecture is in line with the technology development trend from the above-mentioned aspects.

Imbalanced Supply and Demand

The referred supply refers to the ability of the Internet to provide various network services, while the demand refers to users' expectations for Internet in terms of security, throughput, latency, and so on. Regarding the early Internet, users have none requirements for throughput and latency. Correspondingly, the Internet architecture only ensures that different devices or terminals can communicate with each other.

However, with the emergence and promotion of excellent technologies such as mobile Internet, cloud computing, and edge computing, the services provided by the Internet are also growing explosively, thereby, the number of users continues to increase. The contradiction between supply and demand is constantly changing. For example, cloud computing can utilize resources efficiently, but the communication cost cannot meet the requirement of low latency.

The evolution of the Internet architecture has lagged behind the rapid growth in demand. To better support the evolution of the Internet architecture, intelligence represented by DL or DNN has outstanding advantages, including:

- *High expressiveness:* Via nonlinear functions, complex spaces can be depicted. Moreover, extracting the essence of large-scale data can even tackle completely new issues.
- *Extensive flexibility:* For the same device or platform, whether it is the intelligent internal structure or the corresponding model parameters, it can flexibly adapt to new scenarios.

Overall, intelligence can significantly enhance the supply capacity of the Internet architecture, and promote the continuous evolution of the Internet architecture, to serve various emerging demands.

Distributed Organizational Structure

Although the application scenarios and architecture of the Internet continue to evolve, the Internet architecture has always followed the minimalist design principle.[2] By endowing the Internet architecture with intelligent capabilities, the Internet core network can also have strong expressiveness and extensive flexibility. That is, while continuing to follow the principle of extremely simplified design, intelligence enables various network devices in the core network to have a more inclusive management foundation and evolutionary capabilities.

With regard to empowering the Internet architecture with intelligence, large-scale data and high-performance computing resources bring new challenges. Similar to the minimalist design principle, the Internet has always followed *cross-domain*, *hierarchical*, and *open interconnection* since the beginning of its design. Through in-depth analysis of the organizational structure of various network devices in the Internet architecture, it can be found that the distributed organizational structure can provide a path for implementing intelligence.

Specifically, *open interconnection* allows sharing of information between different devices, such as raw data, model parameters or model gradients, and so on. Simultaneously, tasks of different devices, such as the training of malicious traffic detection models, can also be delegated to other devices. In addition, *cross-domain hierarchies* allow the Internet architecture to implement different levels of intelligence capabilities based on service scope and existing infrastructure. Moreover, collaborative learning frameworks represented by federated learning are also developing continuously, providing a solid foundation for implementing collaboration-enabled intelligent Internet architecture.

By exploiting the characteristics of distributed organizational structure, collaboration enables the existing Internet architecture to achieve intelligent capabilities in a scenario where computing and data resources are limited, and various network devices with significantly different software-level and hardware-level capabilities are utilized as the basis.

Necessary Security Assurance

The minimalist design principle at the beginning of the Internet construction weakens the security factor, and its distributed organizational structure strengthens the difficulty of defending against security threats. Therefore, the evolution of intelligent Internet architecture enabled by collabo-

[2] This refers that the implementation of the Internet edge (e.g., end devices and protocols) is relatively complex, while the Internet core network (e.g., routers) is simple and only performs simple forwarding functions.

ration should fundamentally focus on necessary security assurance.

In fact, collaboration-enabled intelligent Internet architecture creates new opportunities, as well as new risks and challenges. With regard to new opportunities, intelligence enables the Internet architecture to more efficiently detect and defend against various security threats. However, intelligent models are vulnerable to adversarial attacks [11], and the vulnerability will bring security risks to the intelligence-based Internet. Moreover, distributed collaboration makes attacks against AI models more stealthy. In addition, the premise of collaboration is the sharing of information. Even if the shared information is not the raw data, the shared information contained in gradients or parameters is essentially a mapping of the raw data, and there is still a risk of privacy leakage.

Although opportunities and challenges coexist, we can still solve the corresponding challenges through proper design and implementation, and maximize the positive utility brought by collaboration-enabled intelligent Internet architecture. In addition to considering these challenges in our design and implementation, today's Internet has deployed some mature technologies to circumvent the potential risks of collaboration. For example, source and path verification technologies [12, 13] can ensure the authenticity of the source and have traceability characteristics, which can provide a basis for the detection and punishment of poisoning attacks based on data tampering. With the existing Internet as the inaccessible basis, therefore, it is reasonable and achievable to facilitate technological evolution with our proposed collaboration-enabled intelligent Internet architecture.

Collaboration-Enabled Intelligent Internet Architecture

The collaboration-enabled intelligent Internet architecture refers to the utilization of collaborative learning such as federated learning as the main approach, with human-like intelligent decision-making as the typical basis, and the existing Internet authentic and trusted technologies as the cornerstone to promote complex heterogeneous Internet architecture to achieve intelligent evolution. While promoting intelligent optimization, this architecture also provides basic services related to intelligence for upper-layer applications on the Internet, such as static resources (e.g., computing and storage) and dynamic tasks (e.g., model training and inference).

In this article, we emphasize the joint optimization of hardware and software, to achieve the collaboration-enabled intelligent Internet architecture. Moreover, flexible and diverse algorithmic modules oriented to the proprietary requirements of Internet architecture are an important part and are built into the algorithm library in the software platform. To clarify our proposed collaboration-enabled intelligent Internet architecture, in this section, we first introduce the global collaboration structure, including each key components and the relationship between these components. Then, the heterogeneous hardware infrastructure and collaboration-oriented software service platform are introduced respectively. Finally, we emphasize multiple algorithmic modules oriented to the proprietary requirements of Internet architecture.

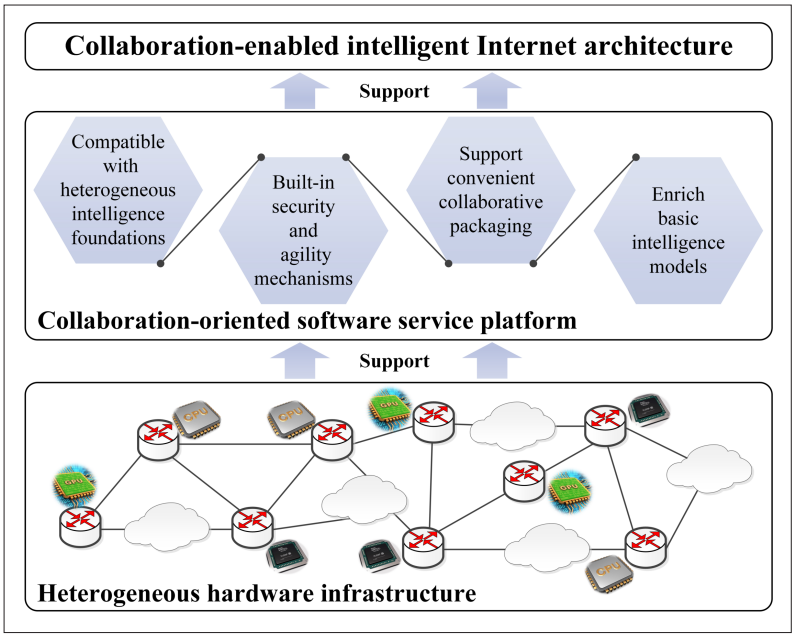

FIGURE 2. An overview of the global collaboration of the collaboration-enabled intelligent Internet architecture, consisting of heterogeneous hardware infrastructure and collaboration-oriented software service platform. The former provides computing resources for the latter, and the latter fully exploits the former's various resources to jointly support the collaboration-enabled intelligent Internet architecture, thereby, achieving complementarity.

Global Collaboration

As illustrated in Fig. 2, the implementation of collaboration-enabled intelligent Internet architecture mainly includes two components, namely heterogeneous hardware infrastructure and collaboration-oriented software service platform. Note that algorithmic modules oriented to the proprietary requirements of Internet architecture are build into the latter.

Specifically, the two-level components in Fig. 2 are not only independent of each other, but also gradually deepened from the bottom up and cooperate with each other. Regarding the heterogeneous hardware infrastructure, considering that the current Internet architecture has obvious limitations in terms of computing and data resources, it is necessary to develop a proprietary hardware infrastructure to ensure the basic resources required by collaboration-enabled intelligent Internet architecture. Moreover, it will be compatible with the existing Internet architecture. As for the collaboration-oriented software service platform, it mainly provides a basic collaborative learning framework, which enables various intelligent optimization algorithms to efficiently adapt to heterogeneous hardware infrastructure and Internet conditions. Furthermore, the software service platform also contains an algorithm library, which focuses on the design and optimization of corresponding algorithms, without additional consideration of hardware infrastructure and basic software platforms.

In addition, these two components can be independently deployed to parts of the existing Internet, and components at any level can pro-

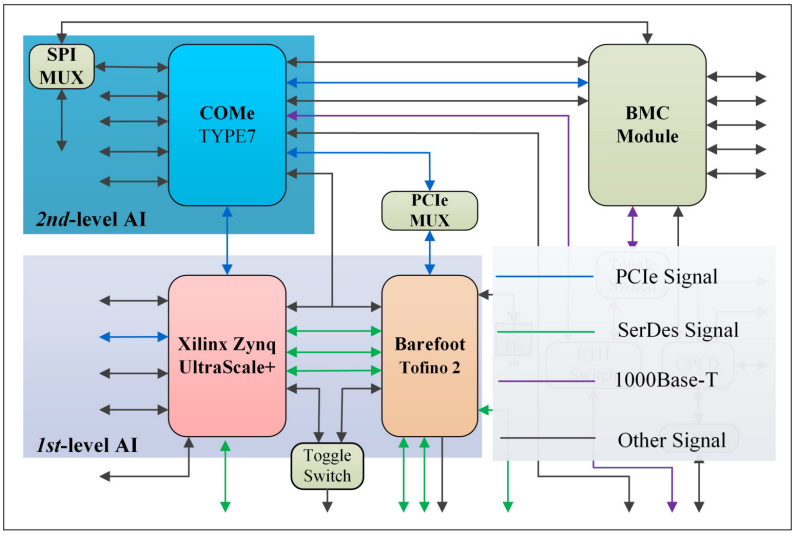

FIGURE 3. An overview of the hardware structure with some sensitive information hidden. In addition to supporting traditional transmission tasks (e.g., forwarding and routing), it not only supports intelligent tasks (e.g., DNN-based model training and inference), but can also serve as an auxiliary basis for intelligent tasks of other resource-constrained devices. Note that *3rd*-level AI refers to GPU servers, which is linked to the FGPA (i.e., Xilinx) and switch (i.e., Barefoot Tofino 2) chips via the SerDesA signal.

mote the intelligence of Internet architecture. It is worth noting that simultaneous deployment can achieve the effect of 1 + 1 >> 2.

Regarding the global collaboration, in addition to the joint optimization of these two levels, it is also important to carry out the collaboration between individuals through the support of these two levels. Specifically, some intelligent activities that individuals can participate in have been illustrated in Fig. 1.

Heterogeneous Hardware Infrastructure

Whether it is traditional machine learning, current DNN-based models, or other AI technologies, data and computing are indispensable key factors. However, various hardware infrastructures in the current Internet architecture, such as routers and switches, have uneven capabilities in terms of storage and computing, and even some hardware infrastructures are completely unable to provide corresponding resources. On the basis of compatibility with the existing Internet architecture, we propose, design, and implement a hardware infrastructure with hierarchical intelligence capabilities, ensuring an intelligent foundation for different tasks.

As illustrated in Fig. 3, our proposed hardware infrastructure integrates resources such as Tofino, FPGA, CPU, and GPU to achieve hierarchical intelligence capabilities. Taking malicious traffic detection as an example, *1st*-level AI[3] can directly perform model inference on the data plane. The required optimal trainable parameters here come from *2nd*-level AI.[4] Moreover, the *3rd*-level AI supports larger model training, which can be transferred to *1st*-level AI and *2nd*-level AI through module transformation such as pruning. In addition to serving local devices and tasks, these hierarchical intelligence capabilities, especially the *3rd*-level AI, can also collaborate with other devices.

In summary, our proposed hardware infrastructure has the following characteristics.

Hierarchical Capabilities: Since individual network devices serve a variety of applications or protocols, the demands for data and computing resources also have diverse characteristics. Hierarchical storage and computing capabilities can ensure that a single network device can meet diverse intelligence demands, and it also provides more possibilities for further evolution. Note that the hierarchical capabilities here correspond to a single network device, which has atomic properties compared to the Internet. In other words, the referred hierarchical capabilities are compatible with the hierarchy in the current Internet and can also meet various demands.

Backward Compatibility: Tasks such as network transmission naturally require the cooperation of multiple devices. The newly proposed hardware infrastructure can cooperate and be compatible with the existing hardware infrastructure.

Collaboration-Oriented Software Service Platform

As introduced earlier, collaboration is the key to bringing intelligence to the Internet architecture. Moreover, part of hierarchical capabilities of the hardware infrastructure also depend on collaboration. To facilitate the efficient evolution of Internet architecture, we propose a novel collaboration-oriented software service platform. The newly proposed platform can exist in a variety of service forms, such as services embedded in individual network devices and web-based services.

Figure 4 briefly illustrates the core functional modules of the collaboration-oriented software service platform via a hierarchical structure, which mainly include the following.

Compatible with Various Resources: Considering that collaboration involves diverse subjects, the platform is as compatible as possible with diverse data resources and computing resources to maximize availability. Therefore, the referred platform is compatible with data resources from the perspective of access interface and format adapter, and compatible with computing resources from the perspective of core hardware and operating system.

Solid Guarantee Foundation: As discussed above, collaboration creates new risks and challenges. By supporting a variety of security protocols, such as homomorphic encryption, asymmetric encryption (a.k.a., public-key cryptography), Diffie–Hellman key exchange (D-F), and zero-knowledge (Z-K) proof, the platform naturally possesses security properties. Moreover, with a variety of convenient development frameworks and containerized management technologies, the implementation of evolution technologies can be accelerated.

Automatic Collaborative Packaging: On the basis of simple models provided by any individual, the platform supports automatic packaging for collaborative learning, and allows to customize relevant configurations, such as communication modes, synchronization methods, and so on.

Multi-Dimensional Intelligent Algorithm: To better serve various network transmission tasks and facilitate the more efficient development of intelligent solutions based on collaboration, the platform also establishes an algorithm library from multiple dimensions, including network architec-

[3] Regarding *1st*-level AI, it is emphasized that AI technologies can directly serve tasks of the data plane. For example, we can transform the AI model into a data plane table to directly distinguish whether the data packet is legitimate. Alternatively, we can also directly utilize FPGA or Tofino 2 to implement some AI models for intelligent inference.

[4] Regarding *2nd*-level AI, it has relatively lower requirements for timeliness than *1st*-level AI. *2nd*-level AI can perform some model training tasks to provide *1st*-level AI with optimized parameters. In addition, *2nd*-level AI can also utilize the AI model to perform some configuration optimization tasks.

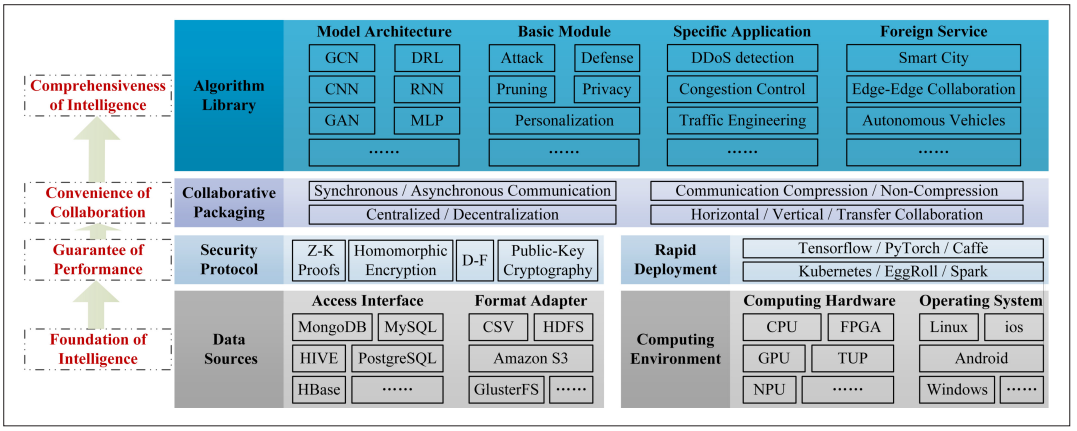

FIGURE 4. The hierarchical division of the core functional modules in the collaboration-oriented software service platform. Among them, the foundation of intelligence refers to compatibility with various data sources and computing environments. The guarantee of performance focuses on security and efficiency. Convenience and comprehensiveness refer to the advantageous environment of intelligent algorithms based on collaboration.

ture of intelligent models, flexible configuration of basic modules, various network applications, and expanding external services.

Flexible and Diverse Intelligent Algorithm Modules

After the hardware infrastructure and collaboration-oriented software service platform are in place, the development of intelligent collaboration algorithms has become the core component. In fact, from the perspective of algorithm design, important indicators such as security and efficiency can be further guaranteed. Moreover, the Internet architecture has some proprietary requirements. For example, security is an important goal to pursue, but the vulnerability of the Internet architecture is prominent. Therefore, our proposed collaboration-enabled intelligent Internet architecture emphasizes the pursuit of the following characteristics through some algorithmic modules.

Security and Robustness: In this regard, we build a detection module for adversarial attacks such as poisoning attacks, and isolate malicious cooperative individuals in a timely manner. Moreover, an automatic adversarial training module is built to allow individuals to actively enhance their own robustness against adversarial attacks.

Controllable Privacy: For this, we first build a privacy quantification and release module that allows data owners to autonomously decide how much sensitive information to share. Correspondingly, the collaborators build an information extraction module to extract as much valuable information as possible from the limited private data.

Flexibility and Efficiency: With this aim, we build a plug-and-play personalized pruning module based on knowledge distillation to flexibly adapt to various scenarios and improve inference efficiency. Moreover, the pruning module can automatically achieve the trade-off between the basic conditions and the optimization goal.

Experiments

To illustrate the intelligence advantages that collaboration brings to the Internet architecture, in this section, we take the multi-classification malicious traffic detection task as a case study. Specifically, malicious traffic detection can be deployed at multiple levels such as the data plane, control plane, and application layer. Moreover, the relevant intelligent solutions are of obvious significance [2]. Next, we briefly clarify the experimental configuration and analyze the experimental results.

Experimental Configuration

Regarding the experimental configuration, we introduce datasets, parameter setting and evaluation criteria separately.

Datasets: Our experiments are carried out on two publicly available datasets, that is, *KDDCUP99* (http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html) and *UNSW-NB15* (https://research.unsw.edu.au/projects/unsw-nb15-dataset), both of which are widely adopted by scholars [14, 15]. Regarding *KDDCUP99*, we utilize an officially provided subset, namely *DATASET I*, which contains 494,021 samples. It involves 23 categories, that is, one legitimate and 22 malicious (e.g., DoS and Probing), and the feature dimension of each sample is 41. The official partition from *UNSW-NB15*, namely *DATASET II*, is also a dataset with multiple categories, that is, one legitimate and nine malicious (e.g., Fuzzers, Backdoors, DoS, and Worms). It contains 257,673 samples and the feature dimension of each sample is 45. After removing irrelevant features, our experiments utilize features in 42 dimensions. In terms of dataset partitioning, both datasets follow 70 percent of samples for training and 30 percent for testing.

To be more in line with the real world, the training samples owned by all 10 individuals participating in the experiment (namely #1 to #10, respectively) are Non-IID. Specifically, we denote the number of legitimate samples in the training set by $N_{legitimate}$. For each individual, firstly, the same amount (i.e., $\square N_{legitimate}/10\square$) of legitimate traffic samples is randomly[5] obtained. For the remaining types of samples (i.e., malicious traffic), each individual is randomly assigned some sample labels, illustrated in Table 1. Specifically, 0 represents the label of initially assigned legitimate samples. Regarding malicious samples, the ranges of labels for *DATASET I* and *DATASET II* are [1, 22] and [1, 9], respectively. We denote the total number of samples with label j as N_j, and

	#1	#2	#3	#4	#5	#6	#7	#8	#9	#10
DATASET I	0, 3, 6, 7, 11, 14–17, 19–21	0, 1, 3, 4, 8, 16, 20	0, 1, 6–9, 13, 14, 18, 20	0, 2, 5, 7–11, 13, 14, 21	0–2, 5, 7–9, 13–15, 17, 18, 20, 22	0, 2, 8, 10	0–5, 11, 12, 16–18, 20	0–6, 8–10, 13, 16, 18, 20–22	0, 8, 10, 15, 17	0–16, 18, 19, 21, 22
DATASET II	0, 1, 2, 7, 9	0, 1, 4	0, 8	0, 1, 5, 9	0, 2, 4, 8	0, 7–9	0, 2, 5, 9	0, 2, 3, 5, 7	0, 2, 3, 6	0, 4, 6–8

TABLE 1. Details of sample labels owned by each individual.

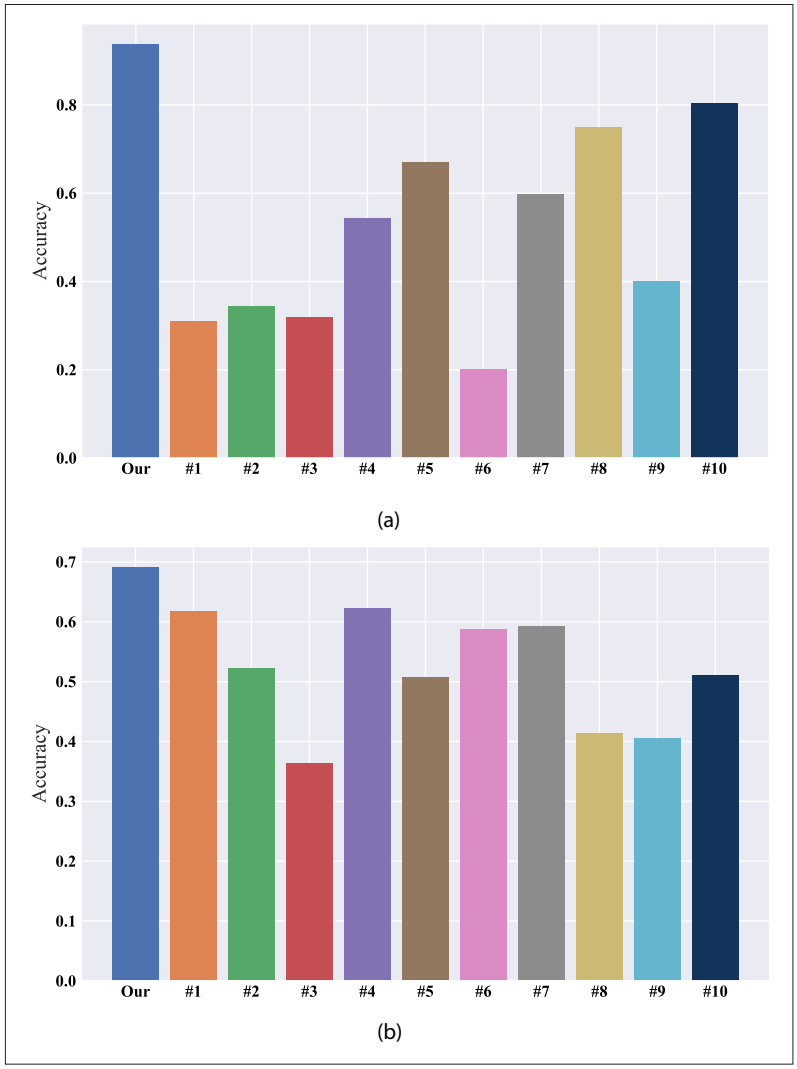

FIGURE 5. Experimental evaluation results with Non-IID configuration, where our refers to the collaboration-based method proposed in this article, and #1 to #10 refer to the locally independently trained models, respectively: a) *DATASET I*; b) *DATASET II*.

$\mathcal{M}_i$ denotes the set of labels possessed by the i-th individual. For each $j \in \mathcal{M}_i$, $min(\lfloor N_j/10 \rfloor + 100, N_j)$ malicious traffic samples with label j will be assigned to the i-th individual.

Unlike the training set, both the collaboration-enabled model proposed in this article and the model of each individual are evaluated on the same testing set. The total number of samples with label j in the testing set is denoted as N'_j. Due to the imbalance of *DATASET I*, the samples of label 3 and label 4 account for a large proportion, so the number of samples for both labels is 2000, while the number of samples for other labels is $min(1000, N'_j)$. *DATASET II* does not have a similar label imbalance issue, so all testing samples are utilized for experimental evaluation.

Parameter Setting: To demonstrate the advantages of collaboration, in addition to training a model per individual, we also train a collaboration-enabled model. Since it is a multi-classification task, the loss function is cross entropy. Except the activation function of the last layer is *softmax*, the rest of the activation functions are *ReLU*. To speed up local training convergence for individuals, the optimizer is Adam instead of SGD. For *DATASET I* and *DATASET II*, the initial learning rate are $lr = 0.015$ and $lr = 0.01$, respectively, both of which decay to $0.9 * lr$ per 20 epochs.

Evaluation Criteria: We utilize classification accuracy as the evaluation criterion. Specifically, N' represents the number of correctly classified samples, and N represents the total number of samples used for testing. Therefore, the classification accuracy is N'/N.

Analysis of Performance

As illustrated in Fig. 5, we present the results in terms of accuracy for the collaboration-enabled model and 10 independent model without any collaboration among individuals, respectively, in the form of a histogram. It can be found that whether it is *DATASET I* or *DATASET II*, collaboration can significantly improve the accuracy.

Specifically, regarding *DATASET I* (i.e., Fig. 5a), the accuracy of our proposed collaboration-enabled model reaches 93.7 percent, while the average accuracy of the other independent models is 49.34 percent. The main reason for this difference is that individuals have insufficient information, while collaboration allows information to flow and aggregate among different individuals, effectively exploiting the potential value of existing data on the basis of respecting privacy. In addition, the accuracy of 6-th individual (i.e., #6 in Fig. 5a) is only 20 percent, and it is completely incapable of dealing with unknown threats. This is because #6 has the thinnest information, which is consistent with the label categories illustrated in Table 1. In other words, resource-constrained individuals have a greater demand for our proposed collaboration-enabled intelligent Internet architecture.

Similar to *DATASET I*, *DATASET II* also illustrates that collaboration is significantly better than independence. Also, #3 in Fig. 5b, which has the most scarce information (illustrated in Table 1), also has the lowest accuracy. Comparing Fig. 5a and Fig. 5b, it can be found that the accuracy in Fig. 5b is more balanced. This is because *DATASET II* has fewer label categories and correspondingly fewer unknown threats. Therefore, collaboration-enabled intelligent Internet architecture is more suitable for dealing with unknown risks or states in the evolution.

Conclusion

In this article, we propose the collaboration-enabled intelligent Internet architecture, which is compatible with the existing Internet architecture, allowing the Internet to continuously evolve to

[5] Note that this is random and not uniform, and there can be repetitions.t

adapt to more complex scenarios. More specifically, in articulating the inherent opportunities and challenges of enabling Internet architecture to be intelligent through collaboration, we first analyze the current situation of the Internet supply and demand imbalance, the nature of network devices adopting a distributed organizational structure, and the long-standing dilemma of lacking built-in security. Subsequently, we present the collaboration-enabled intelligent Internet architecture from the perspective of software and hardware complementarity. Our heterogeneous hardware infrastructure is not only compatible with existing transmission tasks, but also provides hierarchical computing capabilities for the software service platform. While enabling efficient collaboration of intelligent algorithms, the software service platform is also conducive to fully exploiting the hierarchical capabilities of heterogeneous hardware infrastructure. In addition, the platform also integrates some flexible algorithmic modules for the proprietary requirements of Internet architecture. Finally, we separately conduct case studies on two different publicly available datasets, illustrating the positive value of collaboration for Internet architecture.

Acknowledgments

This work was in part supported by National Science Foundation for Distinguished Young Scholars of China with No. 61825204, National Natural Science Foundation of China with No. 61932016 and No. 62132011, Beijing Outstanding Young Scientist Program with No. BJJWZYJH01201910003011, China Postdoctoral Science Foundation with No. 2021M701894, China National Postdoctoral Program for Innovative Talents, and Shuimu Tsinghua Scholar Program. We also thank our editors and anonymous reviewers for their comments and guidance.

References

[1] S. Yan *et al.*, "ACC: Automatic ECN Tuning for High-Speed Datacenter Networks," *Proc. ACM SIGCOMM*, 2021, pp. 384–97.
[2] C. Fu *et al.*, "Realtime Robust Malicious Traffic Detection via Frequency Domain Analysis," *Proc. ACM CCS*, 2021, pp. 3431–46.
[3] S. Wang *et al.*, "Adaptive Federated Learning in Resource Constrained Edge Computing Systems," *IEEE JSAC*, vol. 37, no. 6, 2019, pp. 1205–21.
[4] Y. Zhao *et al.*, "Stability-Based Analysis and Defense against Backdoor Attacks on Edge Computing Services," *IEEE Network*, vol. 35, no. 1, 2021, pp. 163–69.
[5] L. Chen *et al.*, "AuTO: Scaling Deep Reinforcement Learning for Datacenter-Scale Automatic Traffic Optimization," *Proc. ACM SIGCOMM,* 2018, pp. 191–205.
[6] Y. Mirsky *et al.*, "Kitsune: An Ensemble of Autoencoders for Online Network Intrusion Detection," *Proc. NDSS*, 2018.
[7] D. Wang *et al.*, "Federated Analytics: Opportunities and Challenges," *IEEE Network*, vol. 36, no. 1, 2022, pp. 151–58.
[8] C. Hu, R. Lu, and D. Wang, "FEVA: A Federated Video Analytics Architecture for Networked Smart Cameras," *IEEE Network*, vol. 35, no. 6, 2021, pp. 163–70.
[9] M. Salehi and E. Hossain, "Federated Learning in Unreliable and Resource-Constrained Cellular Wireless Networks," *IEEE Trans. Commun.*, vol. 69, no. 8, 2021, pp. 5136–51.
[10] T. Li *et al.*, "Ditto: Fair and Robust Federated Learning Through Personalization," *Proc. ICML*, 2021, pp. 6357–68.
[11] Y. Zhao *et al.*, "Intelligent Networking in Adversarial Environment: Challenges and Opportunities," *SCIENCE CHINA Information Sciences*, vol. 65, no. 7, 2022, pp. 170 301:1–11.
[12] F. Yang *et al.*, "I Know If the Journey Changes: Flexible Source and Path Validation," *Proc. IEEE/ACM IWQoS,* 2020, pp. 1–6.
[13] S. Fu *et al.*, "MASK: Practical Source and Path Verification based on Multi-AS-Key," *Proc. IEEE/ACM IWQoS*, 2021, pp. 1–10.
[14] S. Bhatia *et al.*, "MStream: Fast Anomaly Detection in Multi-Aspect Streams," *Proc. ACM WWW*, 2021, pp. 3371–82.
[15] R. Sheatsley *et al.*, "On the Robustness of Domain Constraints," *Proc. ACM CCS*, 2021, pp. 495–515.

Biographies

Yi Zhao [S'19, M'21] received the B. Eng. degree from the School of Software and Microelectronics, Northwestern Polytechnical University, Xi'an, China, in 2016, and the Ph.D. degree from the Department of Computer Science and Technology, Tsinghua University, Beijing, China, in 2021. Currently, he is an assistant researcher and postdoctoral fellow at the Department of Computer Science and Technology, Tsinghua University. And he is a recipient of the Shuimu Tsinghua Scholar Program. His research interests include next-generation Internet, deep learning robustness, machine learning, and game theory. He is a member of ACM.

Ke Xu [M'02, SM'09] received his Ph.D. from the Department of Computer Science and Technology of Tsinghua University, Beijing, China, where he serves as a full professor. He has published more than 200 technical papers and holds 11 US patents in the research areas of next-generation Internet, Blockchain systems, Internet of Things, and network security. He is a member of ACM. He has guest-edited several special issues in IEEE and Springer Journals. He is an editor of IEEE IoT Journal. He was Steering Committee Chair of IEEE/ACM IWQoS.

Jiahui Chen received the B. Eng. degree from the School of Computer Science & Technology, Huazhong University of Science and Technology, Wuhan, China, in 2022. Currently, he is pursuing a Ph.D. degree in the Department of Computer Science and Technology at Tsinghua University, Beijing, China. His research interests include federated learning, network security, and privacy.

Qi Tan received the master degree from the Department of Computer Science and Technology, Tsinghua University, Beijing, China, in 2019. Currently, he is a Ph.D candidate in the Department of Computer Science and Technology at Tsinghua University, Beijing, China. His research interests include network security, machine learning, and privacy.