# ENSURING PRIVACY: EFFICIENT AND VERIFIABLE ADVANCED NETWORK TRAFFIC ANALYSIS

**1 Mr. SNVASRK PRASAD, 2 A. VISHNU VARDHAN, 3 D. ANIL VARMA**

**4 A. MAHESH, 5 B. GOPICHAND**

*1Assistant Professor, Department of CSE, Sri Indu College of Engineering and Technology-Hyderabad*

*2345Under Graduate, Department of CSE, Sri Indu College of Engineering and Technology-Hyderabad*

## ABSTRACT

In this study, we introduce a crowdsourcing-based traffic monitoring system that allows a transportation management center (TMC) to gather traffic flow data at road intersections in a secure and efficient manner. By utilizing homomorphic encryption and a super-increasing sequence, drivers can encrypt their travel direction information at T-junctions or crossroads to protect their privacy. Roadside units (RSUs) act as intermediaries between drivers and the TMC, aggregating and perturbing encrypted traffic flow to maintain driver privacy through a differential privacy mechanism. Through decryption of the perturbed data, the TMC can obtain traffic flow statistics without compromising individual driver information. Furthermore, a lightweight commitment proof ensures the integrity of the encrypted data, preventing malicious drivers from manipulating their information. Security analysis confirms that the proposed system meets all necessary security requirements, including confidentiality, verifiability, unlinkability, and traceability. Extensive simulations demonstrate the efficiency of the system in terms of computational and communication costs.

Keywords: **Cloud and Big Data, Data Security**

## INTRODUCTION

Middlebox is a network equipment that supports a wide spectrum of network functions for enterprise networks. For instance, a middlebox can provide firewall, load balancer and deep packet inspection (DPI) services . Nowadays, some of the modern middlebox services are delay sensitive. Moreover, it is also challenging to offer high efficiency facing with the explosion of traffic volume. For instance, DPI is a typical delay sensitive network function. One of its key performance metrics is the packet throughput within a certain period of time. Thus, to achieve high efficiency, the most appealing solution is outsourcing the DPI service to the cloud platform. Various benefits can be acquired with the assistance of the cloud servers. First, powerful computation and communication capabilities are provided, which makes it feasible to support efficient DPI over large-scale traffic volume. Second, for the owner of middlebox, diverse DPI functions can be customized to meet the new requirements without purchasing additional hardware. Third, the heavy burden of the daily management of DPI system is released. In addition, the advanced DPI functions, such as machine learning based malware detection , can be efficiently supported by cloud computing. Consequently, significant attentions have been paid to the outsourcing of DPI for cloud-assisted middlebox . Unfortunately, the DPI outsourcing also introduces several security and privacy concerns. In specific, the network traffic has to be redirected to the cloud for inspection. As a result, an

important privacy concern is the exposure of packet payload. For example, the personal information of enterprise employees is inevitably disclosed to the cloud server if without any protection. The cloud service provider may even attempt to analyze the private contents for economic interest. Moreover, the passing packets may contain sensitive information that relates to commercial secrets of an enterprise. If these kinds of information are leaked to the cloud or any competitor, serious losses may be caused. Another crucial issue is the confidentiality of the DPI rules. Usually, the details of the DPI rules directly reflect the security and privacy policies. If an internal or external attacker has accessed the DPI rules, it will be easier to evade the inspection. With such strong background information, the attacker can even find some loopholes of the system. Thus, both the packet payload and the DPI rules should be protected from the public cloud. A simple way to achieve this goal is using standard crypto-systems (e.g., AES, RSA) to encrypt the packet payload and the DPI rules. Unfortunately, it is usually difficult to process DPI directly over ciphertext domain . Therefore,it is challenging and urgent to design a privacy-preserving DPI scheme over cloud platform. Some approaches have been proposed to offer DPI service on the public cloud with privacy protection. The first milestone-like work Blind Box formally defined the security and privacy requirements of middleboxes. It also provided an efficient solution using symmetric encryption. Blind Box utilized garbled circuit to obfuscate the DPI rules, which could be time-consuming for large- scale connections. Yuan et al. adopted broadcast encryption . It can support the sharing of encrypted rules between different connections. Later, their subsequent work proposed an efficient method that is able to verify the inspection results. Recently, Guo et al. designed a dynamic DPI scheme to support rule update. Several public key encryption based schemes are also proposed to explore diverse functions such as malware detection and decryptable matching.

Due to the using of public key crypto-system, computation overheads are inevitably increased. As a result, the time cost on packet sender side becomes higher. Meanwhile, the total packet throughput is significantly decreased. Previously proposed works have provided diverse DPI services with different levels of privacy preservation. There are still some issues not fully addressed. On one hand, larger packet throughput without compromising the privacy protection is one of the crucial design goals. On the other hand, efficient and fine-grained inspection result verification is not well supported. These issues are challenging to solve due to the natural conflicts between functionality, efficiency and privacy. To tackle these challenges, we present three observations that are not considered by existing works.

1). First, in the reality, most contents of the packet payloads are not matched (more than 99%) by any DPI rules. Therefore, these packets should be fast filtered out. Intuitively, the content filtering and exact rule matching should be conducted separately. By doing so, the whole DPI process efficiency can be boosted significantly.

2). Second, result verification may introduce extra packet delay, if the results are verified before packet forwarding. As a practical method, the verification can be executed independently.

3). Third, since most of the packets will not be matched, only verifying the final execution result is insufficient. Thus, the execution details should be proved to offer a fine-grained verification. In this paper, we propose an efficient verifiable deep packet inspection scheme (EV-DPI) with privacy protection over two non-collusion cloud servers. EV-DPI adapts fast

symmetric encryption primitives to support privacy preserving DPI. EV-DPI also achieves inspection result verification using Cuckoo hashing.

4).We propose a two-layer inspection architecture. The first layer can fast filter out the most legitimate packets using encoded Bloom filter . The second layer supports exact rule matching using carefully tailored conjunctive searchable encryption scheme. By doing so, EV-DPI achieves lower packet processing cost on sender side and larger packet throughput on middlebox side.Moreover, the intermediate and final inspection results returned by both cloud servers can all be efficiently verified.

5).EV-DPI can preserve the privacy of packet payload and the confidentiality of DPI rules against semihonest cloud servers . Moreover, to conceal the size pattern (i.e., the number of keywords) of each DPI rule, we propose a secure rule extension scheme. By doing so, the cloud server cannot distinguish two encrypted rules based on the size pattern. Thus, the confidentiality of DPI rules stored on the cloud servers is further enhanced.

6).Extensive experiments are conducted over Amazon Cloud to demonstrate the efficiency of EV-DPI. In specific, the network administrator (gateway) is simulated by a local server. The prototype of middlebox is implemented on the cloud based on the public DPI rule set.

Modern enterprise networks heavily rely on ubiquitous network middleboxes for advanced traffic processing such as deep packet inspection, traffic classification, and load balancing. Recent advances in NFV have pushed forward the paradigm of migrating in-house middleboxes to third-party providers as software-based services for reduced cost yet increased scalability. Despite its potential, this new service model also raises new security and privacy concerns, as traffic is now redirected and processed in an untrusted environment. In this article, we survey recent efforts in the direction of enabling secure outsourced middlebox functions, and identify open challenges for researchers and practitioners to further investigate solutions toward secure middlebox services.

## LITERATURE SURVEY

Enabling functionality in a modern network is achieved through the use of middleboxes. Middleboxes suffer from temporal unavailability due to various reasons, such as hardware faults. We design a backup scheme that takes advantage of network function virtualization, an emerging paradigm of implementing network functions in software, deployed on commodity servers. We utilize the agility of software-based systems, and the gap between the resource utilization of active and standby components, in order to design an optimal limited- resource backup scheme. We focus on the case where a small number of middleboxes fail simultaneously, and study the backup resources required for guaranteeing full recovery from any set of failures, of up to some limited size. Via a novel graph-based presentation, we develop a provably optimal construction of such backup schemes. Since full recovery is guaranteed, our construction does not rely on failure statistics, which are typically hard to obtain. Simulation results show that our proposed approach is applicable even for the case of larger numbers of failures.

Many network middleboxes perform deep packet inspection (DPI), a set of useful tasks which examine packet payloads. These tasks include intrusion detection (IDS), exfiltration detection, and parental filtering. However, a long-standing issue is that once packets are sent over HTTPS, middleboxes can no longer accomplish their tasks because the payloads are encrypted. Hence,

one is faced with the choice of only one of two desirable properties: the functionality of middleboxes and the privacy of encryption. We propose Blind Box, the first system that simultaneously provides {\em both} of these properties. The approach of Blind Box is to perform the deep-packet inspection {\em directly on the encrypted traffic. Blind Box realizes this approach through a new protocol and new encryption schemes.

We demonstrate that BlindBox enables applications such as IDS, exfiltration detection and parental filtering, and supports real rulesets from both open-source and industrial DPI systems. We implemented BlindBox and showed that it is practical for settings with long-lived HTTPS connections. Moreover, its core encryption scheme is 3-6 orders of magnitude faster than existing relevant cryptographic schemes.

## SYSTEM ANALYSIS

### EXISTING SYSTEM

Existing works First, in the reality, most contents of the packet payloads are not matched (more than 99%) by any DPI rules. Therefore, these packets should be fast filtered out. Intuitively, the content filtering and exact rule matching should be conducted separately. By doing so, the whole DPI process efficiency can be boosted significantly. Second, result verification may introduce extra packet delay, if the results are verified before packet forwarding. As a practical method, the verification can be executed independently.

### DISADVANTAGES

- Security Risks: Without proper implementation, sensitive data could be at risk of exposure, leading to potential security breaches and unauthorized access to confidential information.
- Lack of Trust: Users may lose trust in the system or organization if their privacy is not adequately protected, impacting the reputation and credibility of the project

### PROPOSED SYSTEM

Some approaches have been proposed to offer DPI service on the public cloud with privacy protection. The first milestone-like work Blind Box formally defined the security and privacy requirements of middleboxes. It also provided an efficient solution using symmetric encryption. Blind Box utilized garbled circuit to obfuscate the DPI rules, which could be time-consuming for large-scale connections. adopted broadcast encryption. It can support the sharing of encrypted rules between different connections. Later, their subsequent work proposed an efficient method that is able to verify the inspection results.

### ADVANTAGES

Ensuring privacy, efficiency, and verifiability in advanced network traffic analysis is crucial for maintaining security, compliance, trust, accurate analysis, and overall system performance.

# IMPLEMENTATION

## MODULES

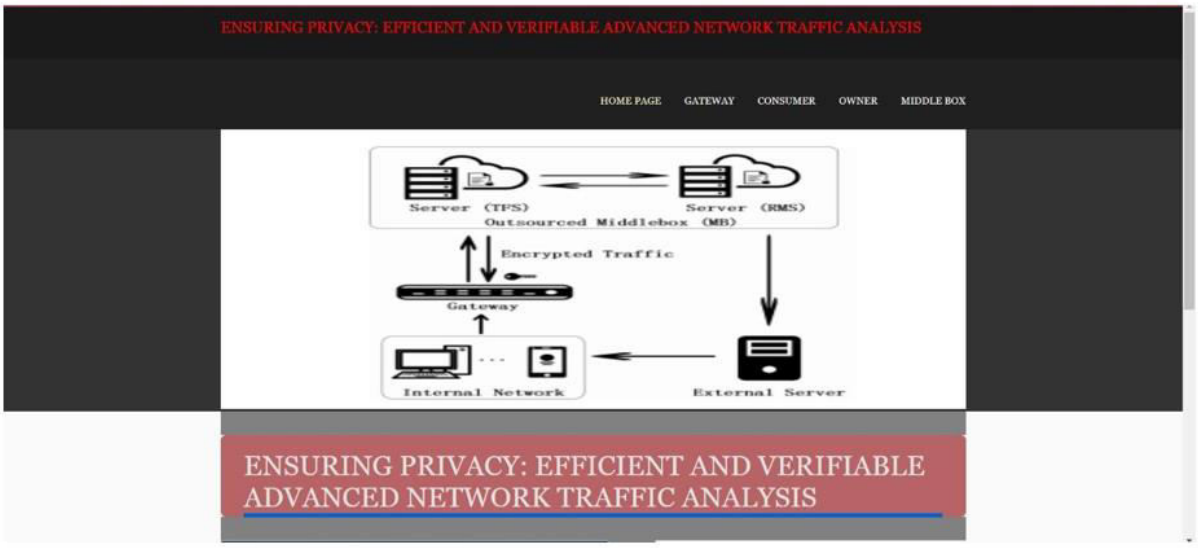
- Gate Way
- Consumer
- Owner
- Middle Box

## MODULE DESCRIPTION

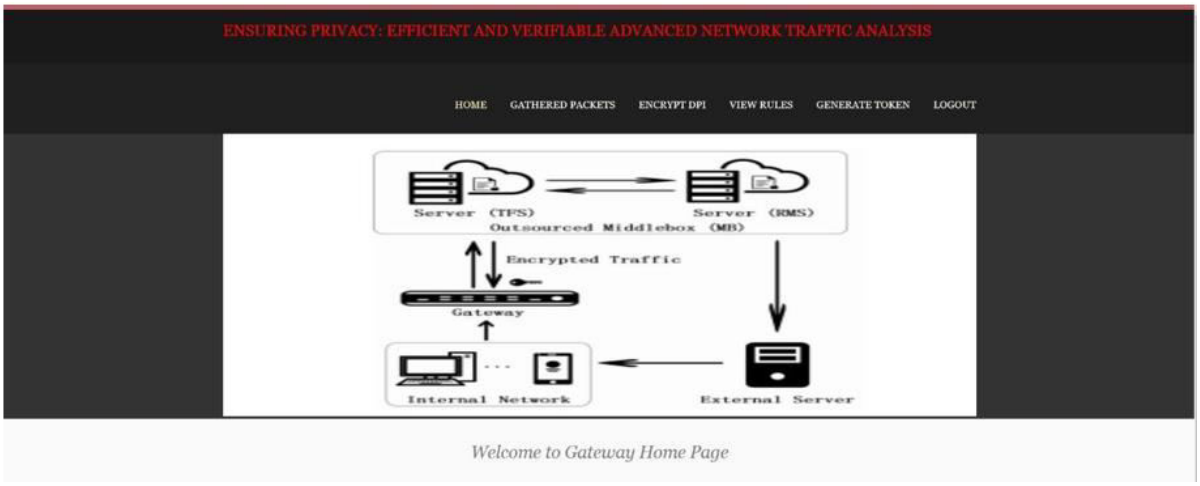
The major modules of the project are

- Gate Way : This Module Transmits the data between network and the server.
- Consumer : this module register into the application first and then login into the application and performs operations in it various networks.
- Owner : the server may owns different networks.
- Middle Box

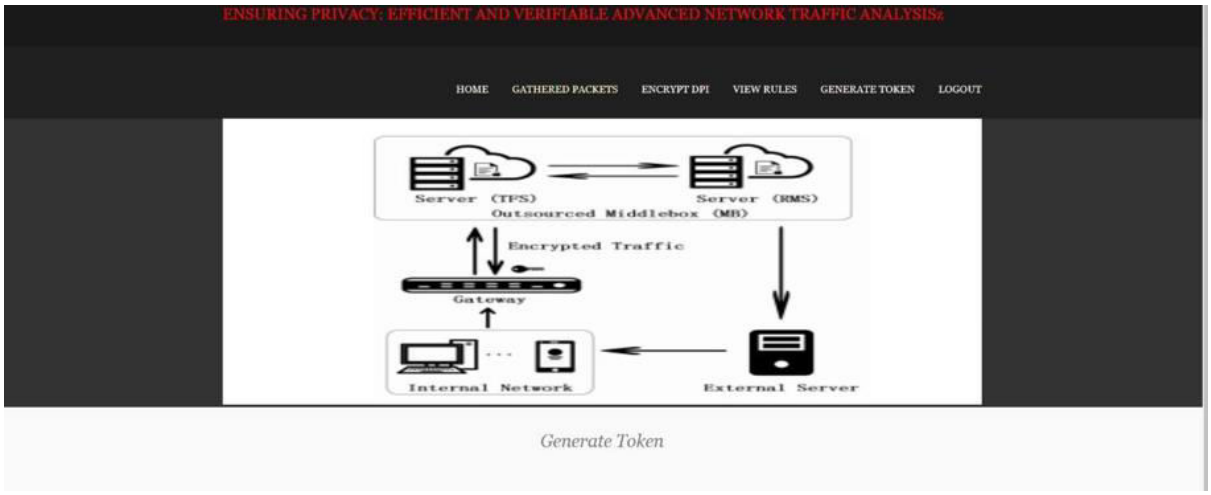
# RESULTS




**HOME SCREEN**




**GATEWAY HOMEPAGE**




**GENERATE TOKEN**


**MIDDLEBOX LOGIN**

## CONCLUSION

In this paper, we have proposed an efficient verifiable deep packet inspection (EV- DPI) scheme with privacy preservation. EV-DPI can well support the verification over final and intermediate inspection results. Both inspection and verification protocols are able to preserve the privacy of packet payload and confidentiality of DPI rules. We have demonstrated the high performance of EV-DPI through extensive experiments and compared the results with the existing scheme. In the future, we will explore the blockchain techniques and learning-based approach to secure diverse outsourced middlebox services.

### FUTURE SCOPE

In this paper, we have considered crowdsourcing-based traffic flow statistics at road intersections and proposed a novel verifiable and privacy-preserving traffic flow statistics (VPTS) scheme for advanced traffic management systems. VPTS can provide strong protection of drivers' privacy, verify the correctness of drivers' data, and guarantee high efficiency for the traffic management system. We have also provided detailed analysis and extensive simulations to demonstrate its correctness, security, and efficiency. For the future work, we will investigate the fairness of the crowdsourcing-based traffic monitoring scenario, by applying the blockchain technology.

## REFERENCES

[1]Y. Kanizo, O. Rottenstreich, I. Segall, and J. Yallouz, "Designing optimal middlebox recovery schemes with performance guarantees," IEEE JSAC, vol. 36, no. 10, pp. 2373–2383, 2018.

[2]J. Sherry, C. Lan, R. A. Popa, and S. Ratnasamy, "BlindBox: Deep packet inspection over encrypted traffic," in Proc. of ACM SIGCOMM, 2015, pp. 213–226.

[3]X. Ma, S. Wang, S. Zhang, P. Yang, C. Lin, and X. Shen, "Cost-efficient resource provisioning for dynamic requests in cloud assisted mobile edge computing," IEEE TCC, 2019, doi:10.1109/TCC.2019.2903240.

[4]X. Liu, R. Deng, K. R. Choo, and Y. Yang, "Privacy-preserving outsourced support vector machine design for secure drug discovery," IEEE TCC, 2018, doi:10.1109/TCC.2018.2799219.

[5]C. Wang, X. Yuan, Y. Cui, and K. Ren, "Toward secure outsourced middlebox services: Practices, challenges, and beyond," IEEE Network, vol. 32, no. 1, pp. 166–171, 2018.

[6]N. Cheng, F. Lyu, W. Quan, C. Zhou, H. He, W. Shi, and X. Shen, "Space/Aerial-assisted computing offloading for IoT applications: A learning-based approach," IEEE JSAC, vol. 37, no. 5, pp. 1117– 1129, 2019.

[7]M. Hao, H. Li, X. Luo, G. Xu, H. Yang, and S. Liu, "Efficient and privacy-enhanced federated learning for industrial artificial intelligence," IEEE TII, 2019, doi:10.1109/TII.2019.2945367.

[8]J. Fan, C. Guan, K. Ren, Y. Cui, and C. Qiao, “SPABox: Safeguarding privacy during deep packet inspection at a middlebox,” IEEE/ACM ToN, vol. 25, no. 6, pp. 3753–3766, 2017.

[9]E. M. Songhori, S. U. Hussain, A. Sadeghi, T. Schneider, and F. Koushanfar, “TinyGarble: Highly compressed and scalable sequential garbled circuits,” in Proc. of IEEE S&P, May 2015, pp. 411–428.

[10]X. Yuan, X. Wang, J. Lin, and C. Wang, “Privacy-preserving deep packet inspection in outsourced middleboxes,” in Proc. of IEEE INFOCOM, 2016, pp. 1–9.