International journal of basic and applied research
www.pragatipublication.com
ISSN 2249-3352 (P) 2278-0505 (E)
Cosmos Impact Factor-5.86

CONFIDENTIAL DEEP PACKET INSPECTION: ENSURING PRIVACY, EFFICIENCY, AND VERIFIABILITY FOR CLOUD

Dr.K.Swaroopa Rani[1] , Nandini[2], Shravani[3], Sahithi[4]

[1]Professor, Department of CSE, Malla Reddy Engineering College for Women, Hyderabad, kantaswaruparani@gmail.com

[2,3,4]UG Students, Department of CSE, Malla Reddy Engineering College for Women, Hyderabad, TS, India.

ABSTRACT

With the increasing traffic volume, enterprises choose to outsource their middlebox services, such as deep packet inspection, to the cloud to acquire rich computational and communication resources. However, since the traffic is redirected to the public cloud, information leakages, such as packet payload and inspection rules, arouse privacy concerns of both middlebox owner and packet senders. To address the concerns, we propose an efficient verifiable deep packet inspection (EV-DPI) scheme with strong privacy guarantees. Specifically, a two-layer architecture is designed and deployed over two non-collusion cloud servers. The first layer fast filters out most of legitimate packets and the second layer supports exact rule matching. During the inspection, the privacy of packet payload and the confidentiality of inspection rules are well preserved. To improve the efficiency, only fast symmetric crypto-systems, such as hash functions, are used. Moreover, the proposed scheme allows the network administrator to verify the execution results, which offers a strong control of outsourced services. To validate the performance of the proposed EV-DPI scheme, we conduct extensive experiments on the Amazon Cloud. Large-scale dataset (millions of packets) is tested to obtain the key performance metrics. The experimental results demonstrate that EV-DPI not only preserves the packet privacy, but also achieves high packet inspection efficiency

I. INTRODUCTION

International journal of basic and applied research
www.pragatipublication.com
ISSN 2249-3352 (P) 2278-0505 (E)
Cosmos Impact Factor-5.86

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 [5]. 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 [5]. 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 BlindBox [2] formally defined the security and privacy requirements of middleboxes. It also provided an efficient solution using symmetric encryption. BlindBox [2] utilized garbled circuit [9] to obfuscate the DPI rules, which could be time-consuming for large-scale connections. Yuan et al. [10] adopted broadcast encryption [11]. It can support the sharing of encrypted rules between different connections. Later, their subsequent work [12] proposed an efficient method that is able to verify the inspection results. Recently, Guo et al. [13] designed a dynamic DPI scheme to support rule update. Several public key encryption based schemes [8], [14], [15] 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

International journal of basic and applied research
www.pragatipublication.com
ISSN 2249-3352 (P) 2278-0505 (E)
Cosmos Impact Factor-5.86

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 [16] to support privacypreserving DPI. EV-DPI also achieves inspection result verification using Cuckoo hashing [17], [18]. The verification and DPI can be processed independently. This design guarantees the high performance in terms of network latency. The main contributions of this paper are summarized as follows. • We propose a two-layer inspection architecture. The first layer can fast filter out the most legitimate packets using encoded Bloom filter [19]. The second layer supports exact rule matching using carefully tailored conjunctive searchable encryption scheme [16]. 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. • EV-DPI can preserve the privacy of packet payload and the confidentiality of DPI rules against semihonest cloud servers [20]. 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. • Extensive experiments are conducted over Amazon Cloud [21] 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 [22]. Without compromising the privacy, EV-DPI is more efficient in terms of packet latency and packet throughput. The remainder of this paper is organized as follows. In Section 2, the system and threat models are described. Based on the models, the design goals are presented. At last, the building blocks are reviewed. In Section 3, we show the design details of EV-DPI. The security analysis and the performance evaluation are provided in Section 4 and Section 5, respectively. In Section 6, closely related works are reviewed. Section 7 concludes the paper.

International journal of basic and applied research
www.pragatipublication.com
ISSN 2249-3352 (P) 2278-0505 (E)
Cosmos Impact Factor-5.86

II.LITERATURE SURVEY

1. Designing optimal middlebox recovery schemes with performance guarantees ,Y. Kanizo, O. Rottenstreich, I. Segall, and J. Yallouz, 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.

2.BlindBox: Deep packet inspection over encrypted traffic, J. Sherry, C. Lan, R. A. Popa, and S. Ratnasamy, 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 BlindBox, the first system that simultaneously provides {\em both} of these properties. The approach of BlindBox is to perform the deep-packet inspection {\em directly on the encrypted traffic. BlindBox 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.

3. Cost-efficient resource provisioning for dynamic requests in cloud assisted mobile edge computing, X. Ma, S. Wang, S. Zhang, P. Yang, C. Lin, and X. Shen, Mobile edge computing is emerging as a new computing paradigm that provides enhanced experience to mobile users via low latency connections and augmented computation capacity. As the amount of user requests is time-varying, while the computation capacity of edge hosts is limited, the Cloud Assisted Mobile Edge (CAME) computing framework is introduced to improve the scalability of the edge platform. By outsourcing mobile requests to clouds with various types of instances, the CAME framework can accommodate dynamic mobile requests with diverse quality of service requirements. In order to provide guaranteed services at minimal system cost, the edge resource provisioning and cloud outsourcing of the CAME framework should be carefully designed in a cost-efficient manner. Specifically, two fundamental problems should be answered: (1) What is the optimal edge computation capacity configuration? (2) What types of cloud instances should be tenanted and what is the amount of each type? To solve these issues, we formulate the resource provisioning in CAME framework as an optimization problem. By exploiting the piecewise convex property of this problem, the Optimal Resource Provisioning (ORP) algorithms with different instances are developed, so as to optimize the computation capacity of edge hosts and meanwhile dynamically adjust the cloud tenancy strategy. The proposed algorithms are proved to be with polynomial computational complexity. To evaluate the performance of the ORP algorithms, extensive simulations and experiments are conducted based on both widely-used traffic models and Google cluster usage tracelogs, respectively. It is shown that the proposed ORP algorithms outperform the local-first and cloud-first benchmark algorithms in system flexibility and cost-efficiency.

4.Privacy-Preserving Outsourced Support Vector Machine Design for Secure Drug Discovery, X. Liu, R. Deng, K. R. Choo, and Y. Yang, In this paper, we propose a framework for privacy-preserving outsourced drug discovery in the cloud, which we refer to as POD. Specifically, POD is designed to allow the cloud to securely use multiple drug formula providers' drug formulas to train Support Vector Machine (SVM) provided by the analytical model provider. In our approach, we design secure computation protocols to allow the cloud server to perform commonly used integer and fraction computations. To securely train the SVM, we design a secure SVM parameter selection protocol to select two SVM parameters and construct a secure sequential minimal optimization protocol to privately refresh both selected SVM parameters. The trained SVM classifier can be used to determine whether a drug chemical compound is active or not in a privacy-preserving way. Lastly, we prove that the proposed POD achieves the goal of SVM training and chemical compound classification without privacy leakage to unauthorized parties, as well as demonstrating its utility and efficiency using three real-world drug datasets.

5. Toward secure outsourced middlebox services: Practices, challenges, and beyond, C. Wang, X. Yuan, Y. Cui, and K. Ren, ,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.

III. 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

International journal of basic and applied research
www.pragatipublication.com
ISSN 2249-3352 (P) 2278-0505 (E)
Cosmos Impact Factor-5.86

filtered out. 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. 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 new cloud server, and finally upload the data to the new server this process is very inefficient and tedious.

Disadvantages

1. Most of the packed are not matched.
2. This process is very inefficient and tedious.

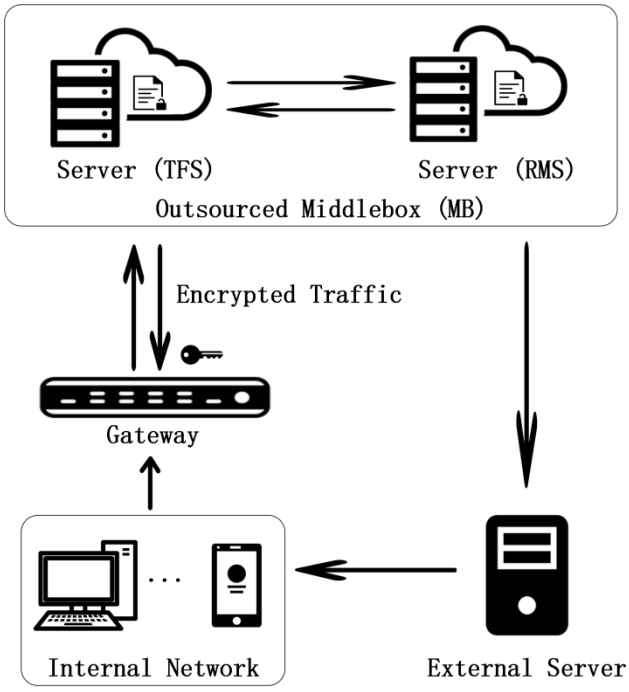
IV. PROPOSED SYSTEM:

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 middle boxes. 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. Recently, 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 decrypt-able 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.

Advantages

1. Efficient matching
2. Can handle large data

International journal of basic and applied research
www.pragatipublication.com
ISSN 2249-3352 (P) 2278-0505 (E)
Cosmos Impact Factor-5.86



V. IMPLEMENTAION

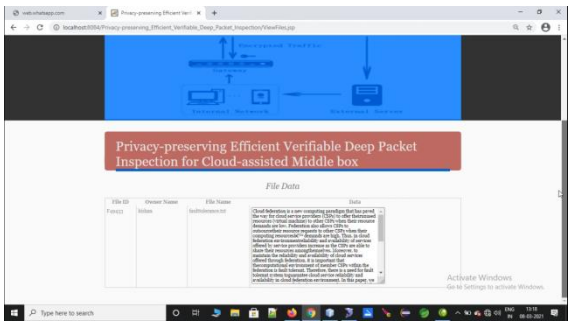
MODULE

1. Gateway
2. Middle box
3. Owner
4. Consumer

MODULE DESCRIPTION

GATEWAY

In this application gateway is a module, here it should login directly with our application and after successful login he can perform some operations such as gathered packets and encrypt dpi and view rules and generated tokens and logout



International journal of basic and applied research
www.pragatipublication.com
ISSN 2249-3352 (P) 2278-0505 (E)
Cosmos Impact Factor-5.86

Fig: Gateway login

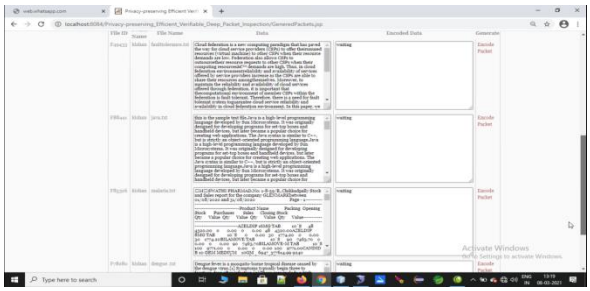


Fig:Encode packets

MIDDLE BOX

In this application middle box is a module, here it should login directly with our application and after successful login he can perform some operations such as token filtering and rules matching and logout.

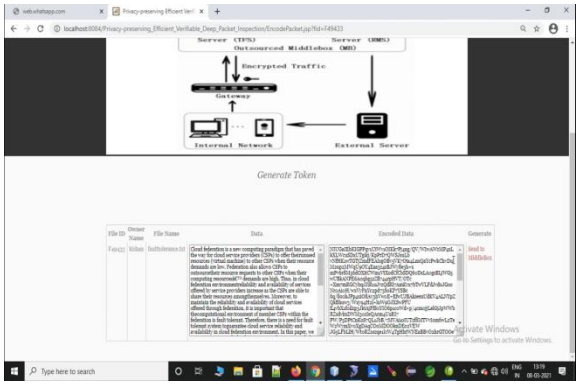


Fig: Send to middle box

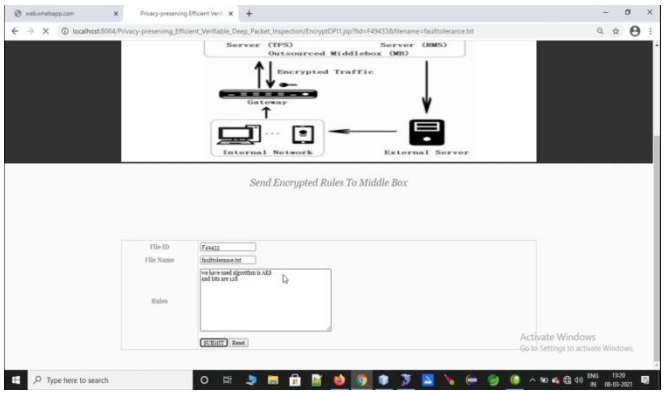


Fig: Encrypted rules sent status

OWNER

International journal of basic and applied research
www.pragatipublication.com
ISSN 2249-3352 (P) 2278-0505 (E)
Cosmos Impact Factor-5.86

Here owner is a module, owner should register with our application and owner should login after registrations, then he can perform some operations such as upload file and view files and logout

Fig2:Owner register

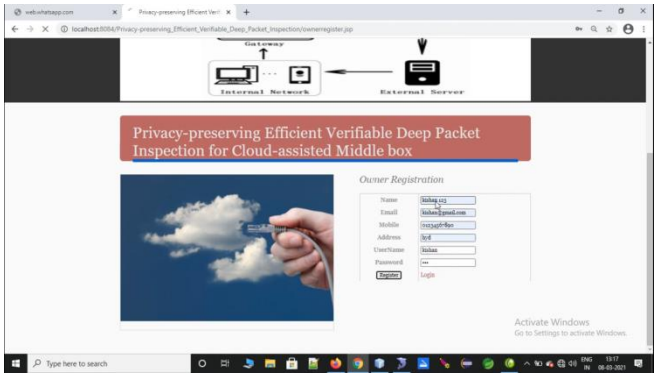


Fig: Owner login

USER

Here user is a module, user should register with our application and user should login after registrations, then he can perform some operations such as view files and logout

International journal of basic and applied research
www.pragatipublication.com
ISSN 2249-3352 (P) 2278-0505 (E)
Cosmos Impact Factor-5.86

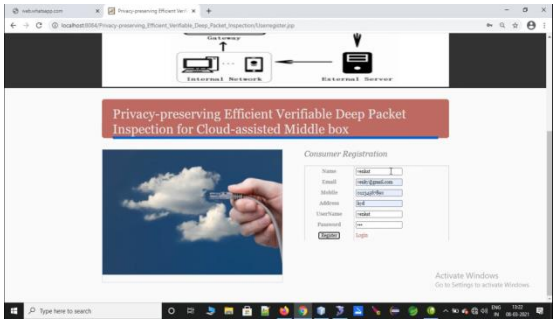


Fig: Consumer login

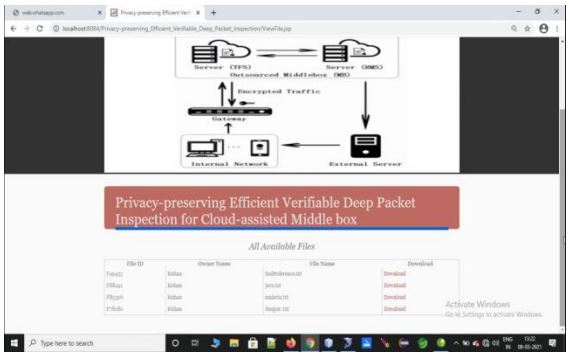


Fig: view files and download

VI. 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.

VI.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.

[11] T. V. X. Phuong, G. Yang, W. Susilo, and X. Chen, "Attribute based broadcast encryption with short ciphertext and decryption key," in Proc. of ESORICS, 2015, pp. 252–269.

[12] X. Yuan, H. Duan, and C. Wang, "Bringing execution assurances of pattern matching in outsourced middleboxes," in Proc. of IEEE ICNP, 2016, pp. 1–10.

[13] Y. Guo, C. Wang, and X. Jia, "Enabling secure and dynamic deep packet inspection in outsourced middleboxes," in Proc. of ACM SCC, 2018, pp. 49–55. [14] S. Canard, A. Diop, N. Kheir, M. Paindavoine, and M. Sabt, "BlindIDS: Market-compliant and privacy-friendly intrusion detection system over encrypted traffic," in Proc. of ACM AsiaCCS, 2017, pp. 561–574.

[15] H. Li, H. Ren, D. Liu, and X. Shen, "Privacy-enhanced deep packet inspection at outsourced middlebox," in Proc. of WCSP, 2018, pp. 1–6.

[16] S. Lai, S. Patranabis, A. Sakzad, J. K. Liu, D. Mukhopadhyay, R. Steinfeld, S.-F. Sun, D. Liu, and C. Zuo, "Result pattern hiding searchable encryption for conjunctive queries," in Proc. of ACM CCS, 2018, pp. 745–762.

[17] G. Levy, S. Pontarelli, and P. Reviriego, "Flexible packet matching with single double cuckoo hash," IEEE Communications Magazine, vol. 55, no. 6, pp. 212–217, 2017.

[18] W. Ogata and K. Kurosawa, "Efficient no-dictionary verifiable searchable symmetric encryption," in Proc. of IFCA FC, 2017, pp. 498–516.

[19] B. H. Bloom, "Space/time trade-offs in hash coding with allowable errors," Communications of the ACM, vol. 13, no. 7, pp. 422–426, 1970.

[20] Y. Zhang, C. Xu, X. Lin, and X. Shen, "Blockchain-based public integrity verification for cloud storage against procrastinating auditors," IEEE TCC, 2019, doi:10.1109/TCC.2019.2908400. [21] "Amazon cloud," https://aws.amazon.com/cn/, 2019, [Online, accessed 27-March-2019].

[22] "Snort rules," https://www.snort.org/, 2019, [Online, accessed 07-March-2019].

[23] L. Melis, H. J. Asghar, E. De Cristofaro, and M. A. Kaafar, "Private processing of outsourced network functions: Feasibility and constructions," in Proc. of ACM SDN-NFV Security, 2016, pp. 39–44.

[24] Y. Zhang, C. Xu, H. Li, K. Yang, J. Zhou, and X. Lin, "Healthdep: An efficient and secure deduplication scheme for cloud-assisted ehealth systems," IEEE TII, vol. 14, no. 9, pp. 4101–4112, 2018.

[25] H. Ren, H. Li, Y. Dai, K. Yang, and X. Lin, "Querying in Internet of Things with privacy preserving: Challenges, solutions and opportunities," IEEE Network, no. 99,

pp. 1–8, 2018. [26] D. Cash, S. Jarecki, C. Jutla, H. Krawczyk, M.-C. Ros¸u, and M. Steiner, "Highly-scalable searchable symmetric encryption with support for boolean queries," in Proc. of CRYPTO, 2013, pp. 353–373. [27] D. Cash, P. Grubbs, J. Perry, and T. Ristenpart, "Leakage-abuse attacks against searchable encryption," in Proc. of ACM CCS, 2015, pp. 668–679. [28] Y. Zhang, J. Katz, and C. Papamanthou, "All your queries are belong to us: The power of file-injection attacks on searchable encryption," in Proc. USENIX Security, 2016, pp. 707–720. [29] X. Yuan, H. Duan, and C. Wang, "Assuring string pattern matching in outsourced middleboxes," IEEE/ACM ToN, 2018. [30] H. Li, D. Liu, Y. Dai, T. Luan, and S. Yu, "Personalized search over encrypted data with efficient and secure updates in mobile clouds," IEEE TETC, vol. 6, pp. 97–109, 2015.

[31] I. Ghosh Ray, Y. Rahulamathava, and M. Rajarajan, "A new lightweight symmetric searchable encryption scheme for string identification," IEEE TCC, 2018, doi:10.1109/TCC.2018.2820014.

[32] S. Kamara and T. Moataz, "Boolean searchable symmetric encryption with worst-case sub-linear complexity," in Proc. of EUROCRYPT, 2017, pp. 94–124.

[33] C. Lan, J. Sherry, R. A. Popa, S. Ratnasamy, and Z. Liu, "Embark: Securely outsourcing middleboxes to the cloud," in Proc. of USENIX NSDI, 2016, pp. 255–273.

[34] G. Xu, H. Li, S. Liu, K. Yang, and X. Lin, "Verifynet: Secure and verifiable federated learning," IEEE TIFS, vol. 15, no. 7, pp. 911– 926, 2020, doi:10.1109/TIFS.2019.2929409.

[35] "DARPA traffic," https://www.ll.mit.edu/r-d/datasets, 2019, [Online, accessed 07-March-2019].

[36] J. Sherry, S. Hasan, C. Scott, A. Krishnamurthy, S. Ratnasamy, and V. Sekar, "Making middleboxes someone else's problem: network processing as a cloud service," in Proc. of ACM SIGCOMM, 2012, pp. 13–24.

[37] Y. Guo, C. Wang, X. Yuan, and X. Jia, "Enabling privacy-preserving header matching for outsourced middleboxes," in Proc. of IWQoS, 2018.

[38] D. Song, D. Wagner, and A. Perrig, "Practical techniques for searches on encrypted data," in Proc. of IEEE S&P, 2000, pp. 44–55. [39] M. Huang, W. Liang, Y. Ma, and

S. Guo, "Maximizing throughput of delay-sensitive nfv-enabled request admissions via virtualized network function placement," IEEE TCC, 2019, doi:10.1109/TCC.2019.2915835.

[40] D. Boneh, E.-J. Goh, and K. Nissim, "Evaluating 2-dnf formulas on ciphertexts," in Proc. of IACR TCC, J. Kilian, Ed., 2005, pp. 325–341.

[41] T. Fuhr and P. Paillier, "Decryptable searchable encryption," in Proc. of ProvSec, 2007.

[42] G. Xu, H. Li, Y. Dai, K. Yang, and X. Lin, "Enabling efficient and geometric range query with access control over encrypted spatial data," IEEE TIFS, vol. 14, no. 4, pp. 870–885, 2019.

[43] J. Liang, Z. Qin, S. Xiao, J. Zhang, H. Yin, and K. Li, "Privacypreserving range query over multi-source electronic health records in public clouds," Elsevier JPDC, vol. 135, no. 7, pp. 127–139, 2020.

[44] K. Lewi and D. J. Wu, "Order-revealing encryption: New constructions, applications, and lower bounds," in Proc. of ACM CCS, 2016, pp. 1167–1178.

[45] Y. Yang, X. Liu, X. Zheng, C. Rong, and W. Guo, "Efficient traceable authorization search system for secure cloud storage," IEEE TCC, 2018, doi:10.1109/TCC.2018.2820714.

[46] J. Liang, Z. Qin, S. Xiao, L. Ou, and X. Lin, "Efficient and secure decision tree classification for cloud-assisted online diagnosis services," IEEE TDSC, 2019, doi:10.1109/TDSC.2019.2922958.