SECURELY ENHANCING NETWORK TRAFFIC ANALYSIS FOR PRIVACY, EFFICIENCY, AND VERIFICATION

Dr.P.Latha, Assistant Professor CSE(AI&ML), Vaagdevi College of Engineering (Autonomous), Bollikunta, Khila Warangal (Mandal), Warangal Urban – 506005(T.S)
Mr. K.Rajashekar, Assistant Professor CSE(AI&ML), Vaagdevi College of Engineering (Autonomous), Bollikunta, Khila Warangal (Mandal), Warangal Urban – 506005(T.S)
S.Prabhas Sai (20641A66C4), UG student CSE(AI&ML), Vaagdevi College of Engineering (Autonomous), Bollikunta, Khila Warangal (Mandal), Warangal Urban – 506005(T.S)
B.Udhay Kumar (21645A6603), UG student CSE(AI&ML), Vaagdevi College of Engineering (Autonomous), Bollikunta, Khila Warangal (Mandal), Warangal Urban – 506005(T.S)
S.Akash (21645A6619), UG student CSE(AI&ML), Vaagdevi College of Engineering (Autonomous), Bollikunta, Khila Warangal (Mandal), Warangal Urban – 506005(T.S)
R.Vivek (20641A66C2), UG student CSE(AI&ML), Vaagdevi College of Engineering (Autonomous), Bollikunta, Khila Warangal (Mandal), Warangal Urban – 506005(T.S)

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 andcommunication resources. However, since the traffic is redirected to the public cloud,information leakages, such as packet payload and inspection rules, arouse privacy concernsof both middlebox owner and packet senders. To address the concerns, we propose anefficient verifiable deep packet inspection (EV-DPI) scheme with strong privacy guarantees.Specifically, a two-layer architecture is designed and deployed over two non-collusion cloudservers. The first layer fast filters out most of legitimate packets and the second layersupports exact rule matching. During the inspection, the privacy of packet payload and theconfidentiality of inspection rules are well preserved. To improve the efficiency, only fastsymmetric crypto-systems, such as hash functions, are used. Moreover, the proposed schemeallows the network administrator to verify the execution results, which offers a strong controlof outsourced services. To validate the performance of the proposed EV-DPI scheme,weconduct extensive experiments on the Amazon Cloud. Large-scale dataset (millions ofpackets) is tested to obtain the key performance metrics. The experimental resultsdemonstrate that EV-DPI not only preserves the packet privacy, but also achieves high packetinspection efficiency. Analysis.

1.INTRODUCTION
Middlebox is a network equipment that supports a wide spectrum of network functions forenterprise networks. For instance, a middlebox can provide firewall, load balancer and deeppacket inspection (DPI) services . Nowadays, some of the modern middlebox services aredelay sensitive. Moreover, it is also challenging to offer high efficiency facing with theexplosion 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[1], the most appealing solution is outsourcing the DPI serviceto the cloud platform. Various benefits can be acquired with the assistance of the cloudservers. First, powerful computation and communication capabilities are provided, whichmakes it feasible to support efficient DPI over large-scale traffic volume. Second, for theowner 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 learningbased malware detection , can be efficiently supported by cloud computing. Consequently,
significant attentions have been paid to the outsourcing of DPI [2] 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[4]. 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, itwill be easier to evade the inspection. With such strong background information, the attackercan even find some loopholes of the system. Thus, both the packet payload and the DPI rulesshould be protected from the public cloud. A simple way to achieve this goal is usingstandard crypto-systems. (e.g., AES, RSA) [3] to encrypt the packet payload .

2.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 hardwarefaults. We design a backup scheme that takes advantage of network function virtualization,an emerging paradigm of implementing network functions in software, deployed oncommodity servers. We utilise the agility [2] of software-based systems, and the gap between the resource utilisation 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 failsimultaneously, and study the backup [5] resources required for guaranteeing full recovery from any set of failures, of up to some limited size. Via a novel graph-based presentation, wedevelop a provably optimal construction of such backup schemes. Since full recovery isguaranteed, our construction does not rely on failure statistics, which are typically hard toobtain. Simulation results show that our proposed approach is applicable even for the case oflarger numbers of failures.
Many network middleboxes perform deep packet inspection (DPI), a set of useful taskswhich examine packet payloads. These tasks include intrusion detection (IDS), exfiltrationdetection, and parental filtering. However, a long-standing issue is that once packets are sentover HTTPS, middleboxes can no longer accomplish their tasks because the payloads areencrypted. Hence, one is faced with the choice of only one of two desirable properties: thefunctionality of middleboxes and the privacy of encryption. We propose BlindBox, the firstsystem 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. Wedemonstrate that BlindBox enables applications such as IDS[6], 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.

Mobile edge computing is emerging as a new computing paradigm that provides enhancedexperience 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 hostsis limited, the CloudAssisted Mobile Edge (CAME) computing framework is introduced toimprove the scalabilityof the edge platform. By outsourcing mobile requests to clouds withvarious types of instances, the CAME framework can accommodate dynamic mobile requests
with diverse quality of service requirements. In order to provide guaranteed services atminimal system cost.

In this paper, we propose a framework for privacy-preserving outsourced drug discovery inthe cloud, which we refer to as POD. Specifically, POD is designed to allow the cloud tosecurely use multiple drug formula providers' drug formulas to train Support Vector Machine(SVM) provided by theanalytical model provider. In our approach, we design securecomputation protocols to allow the cloud server to perform commonly used integer andfraction computations. To securely train the SVM,[7] 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 SVMtraining and chemical compound classification without privacy leakage to unauthorised.

3.EXISTING SYSTEM

First, in reality, most contents of the packet payloads are not matched (more than 99%) byany DPI rules. Therefore, these packets should be fast filtered out. The content filtering andexact rule matching should be conducted separately. By doing so, the whole DPI [5] processefficiency can be boosted significantly. Second, result verification may introduce extra packetdelay, if the results are verified before packet forwarding. As a practical method, theverification can be executed independently.

Disadvantages:

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

4. PROPOSED SYSTEM:

Some approaches have been proposed to offer DPI service on the public cloud with privacyprotection. The first milestone-like work Blind Box formally defined the security and privacy requirements of middle boxes. It also provided an efficient solution using symmetricencryption. Blind Box utilized garbled circuit to obfuscate the DPI rules, which could betime-consuming for large-scale connections. adopted broadcast encryption . It can support thesharing of encrypted rules between different connections. Later, their subsequent workproposed an efficient method that is able to verify the inspection results. Recently, designed adynamic DPI scheme to support rule update. Several public key encryption based schemesare also proposed to explore diverse functions such as malware detection and decrypt-ablematching. Due to the using of public key crypto-system[6], computation overheads areinevitably 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

5.SYSTEM ARCHITECTURE

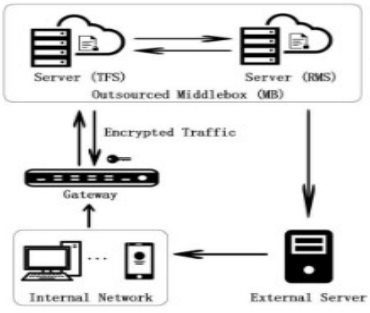


Fig-3.1 System Architecture

ISSN: 2278-4632
Vol-14, Issue-5, May: 2024

6. IMPLEMENTATION

Gateway

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

Middle Box

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

Owner

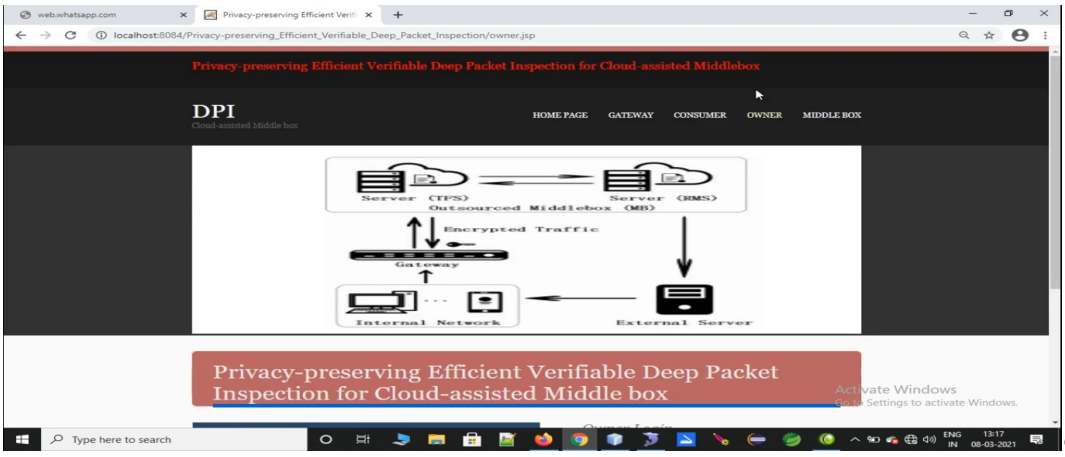
Here owner is a module, owner should register with our application and owner should log in after registrations, then he can perform some operations such as upload file and view files andlogout.

User

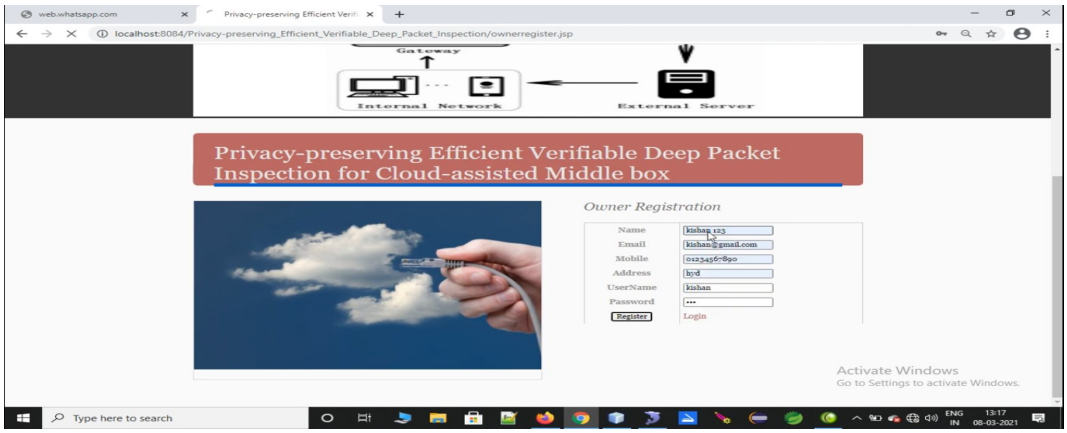
Here user is a module, user should register with our application and user should login afterregistrations, then he can perform some operations such as view files and logout.

7.EXPECTED OUTCOMES

Home screen

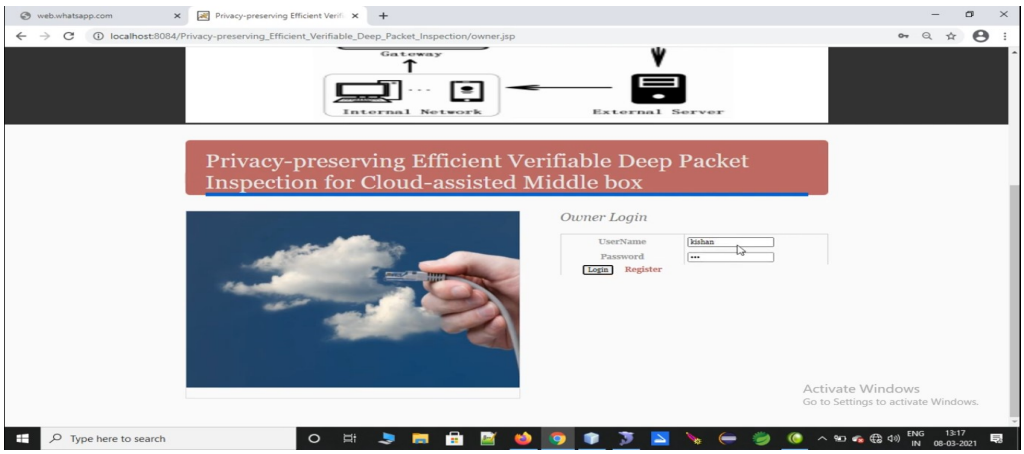


owner register

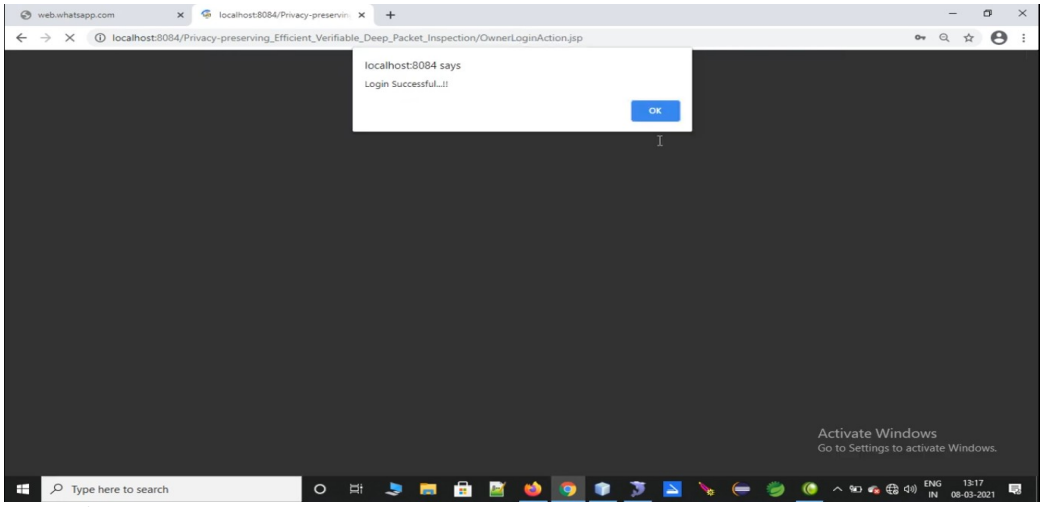


Owner login

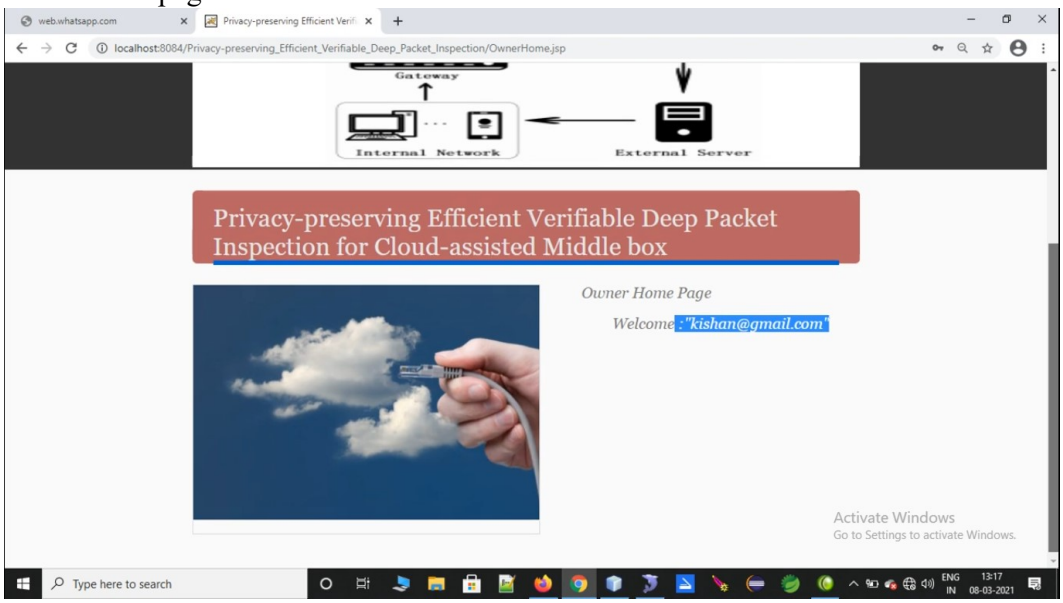
ISSN: 2278-4632
Vol-14, Issue-5, May: 2024



Login Page

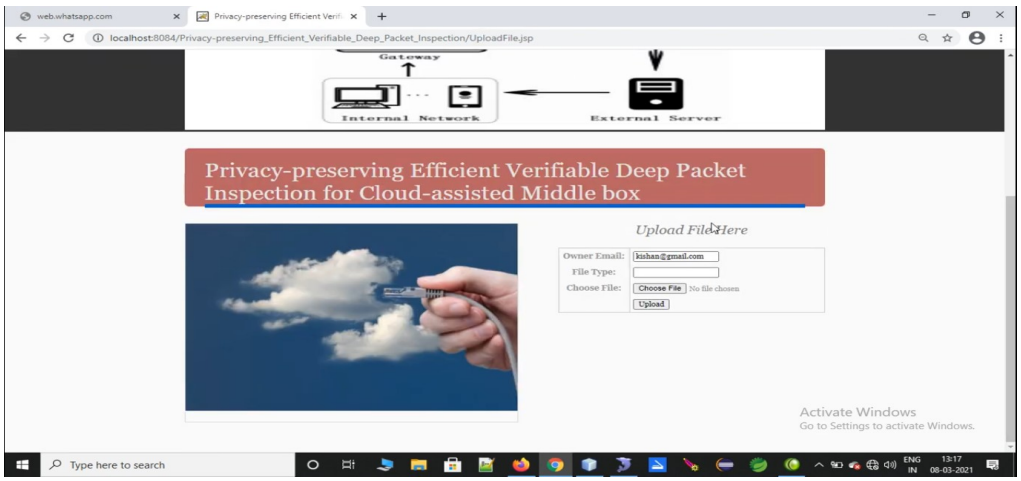


owner home page

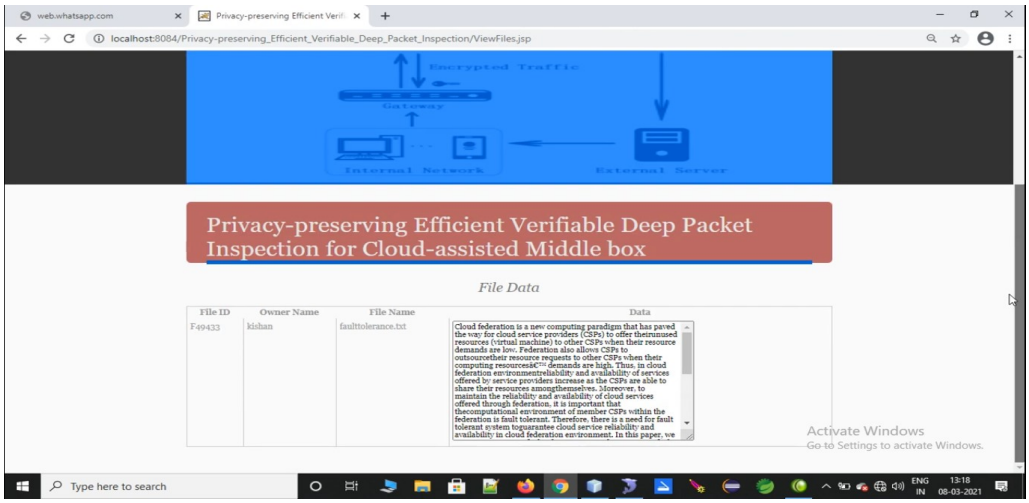


Upload files

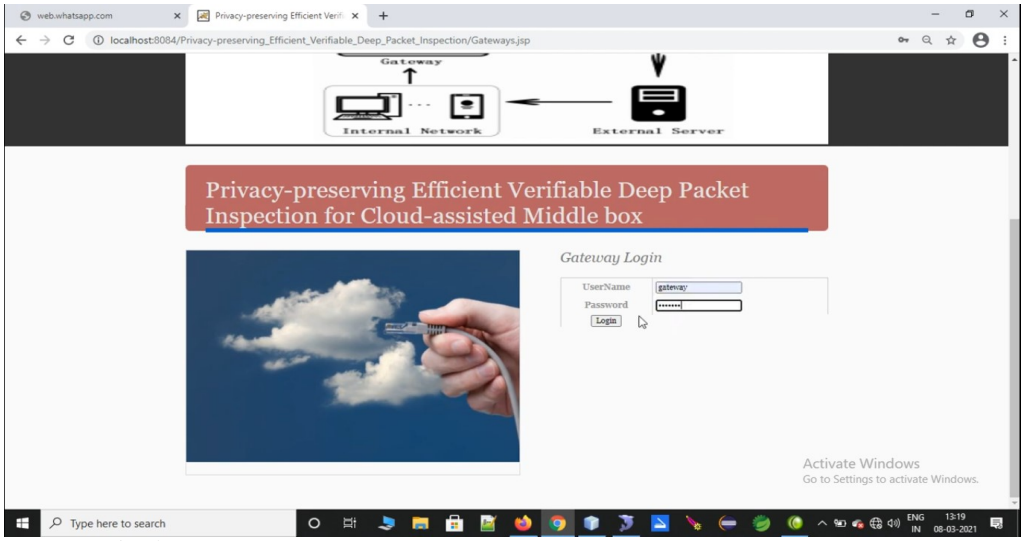
ISSN: 2278-4632
Vol-14, Issue-5, May: 2024



View files

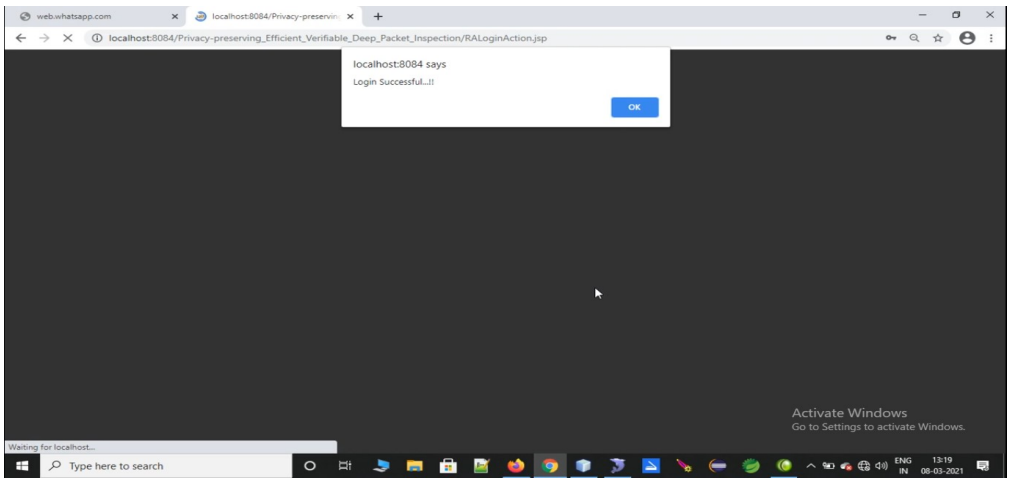


gateway login

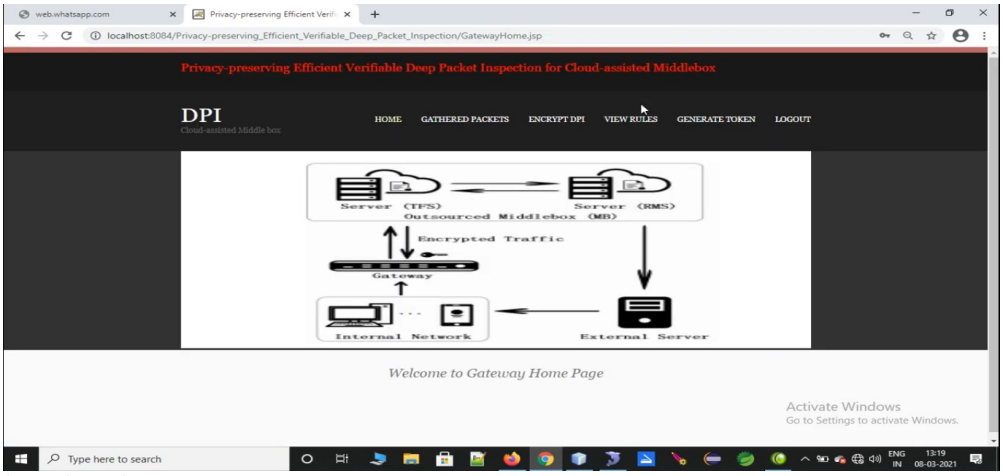


Gateway login status

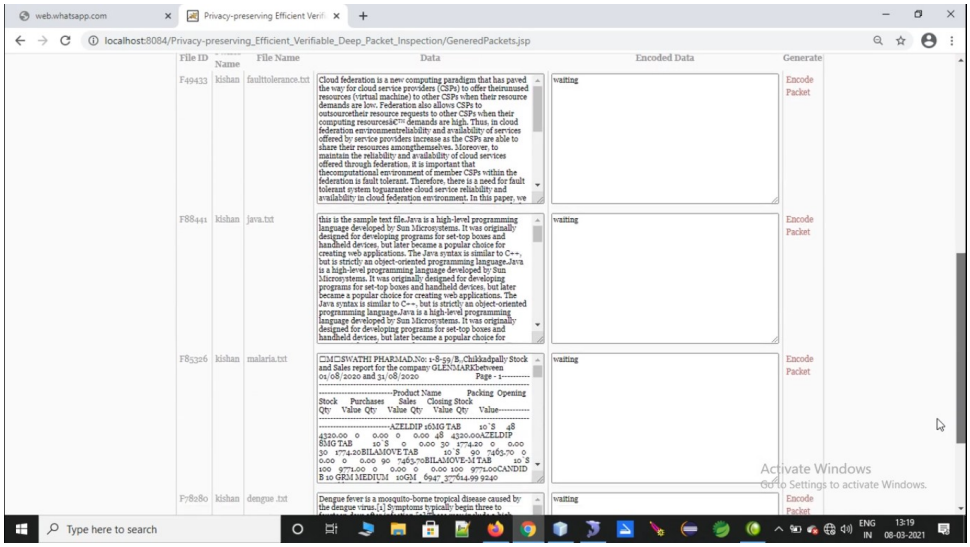
ISSN: 2278-4632
Vol-14, Issue-5, May: 2024



Gateway home page

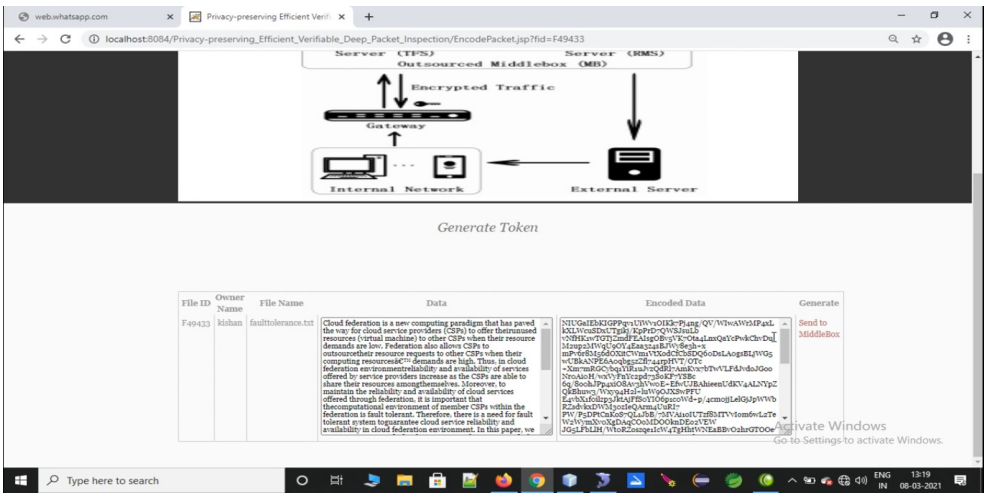


Gathered packets

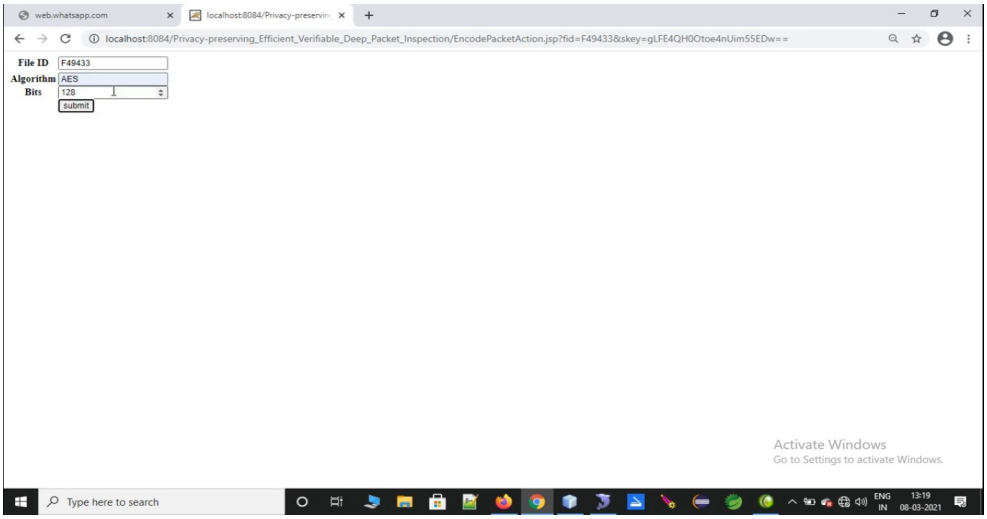


Encode packets

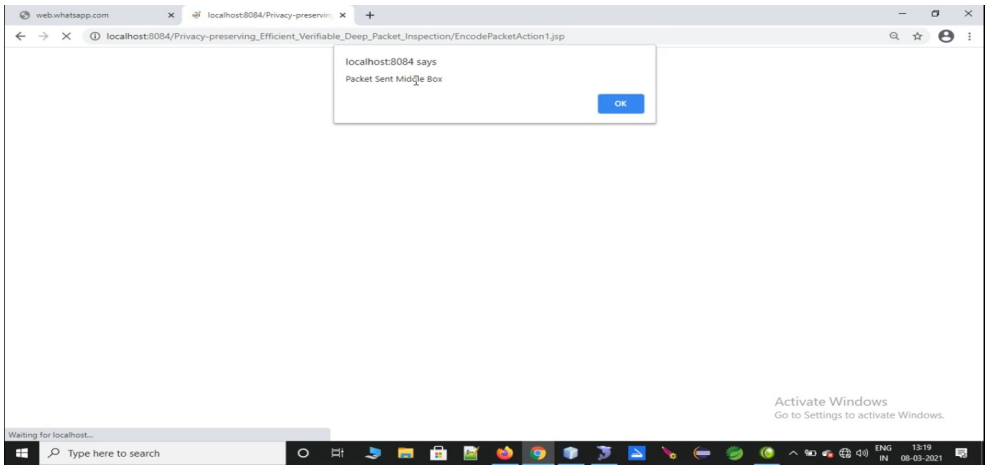
ISSN: 2278-4632
Vol-14, Issue-5, May: 2024



Send to middle box

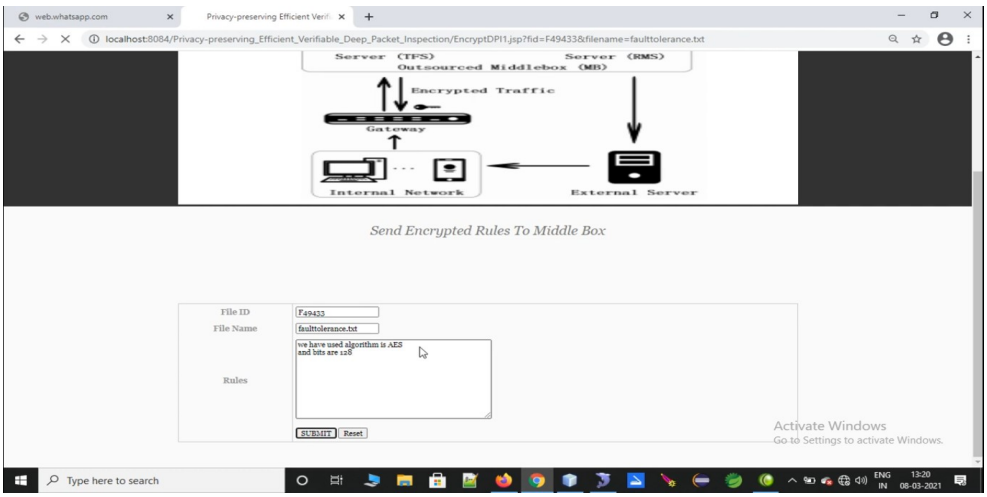


Packet sent to middle box

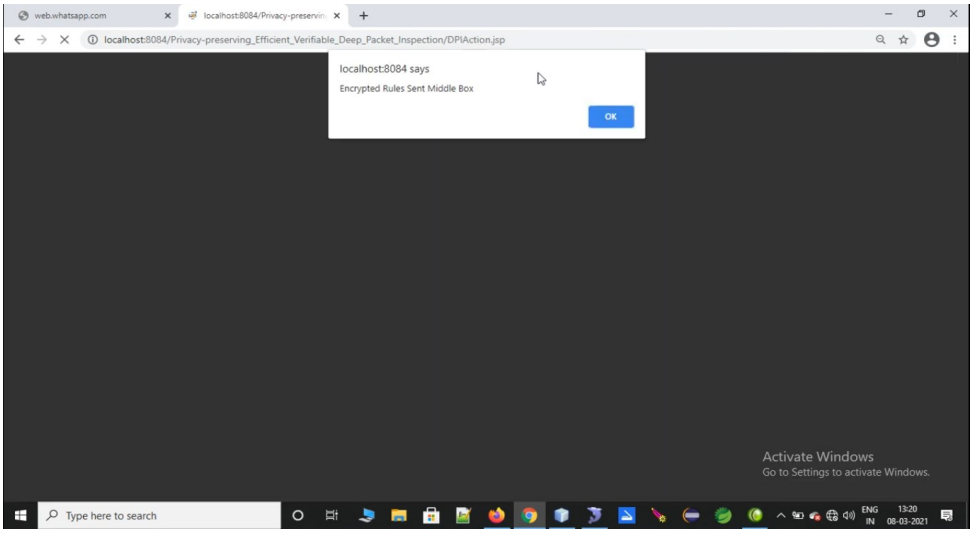


Encrypted rules sent to middle box

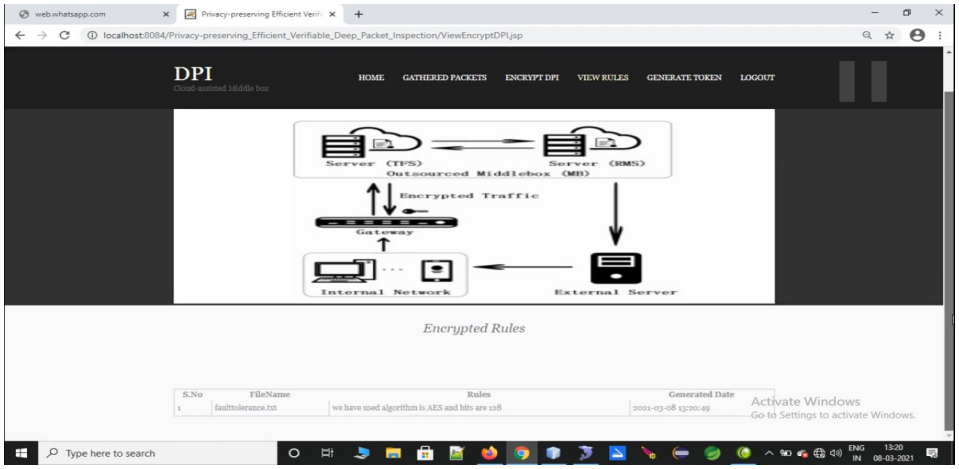
ISSN: 2278-4632
Vol-14, Issue-5, May: 2024



Encrypted rules sent status

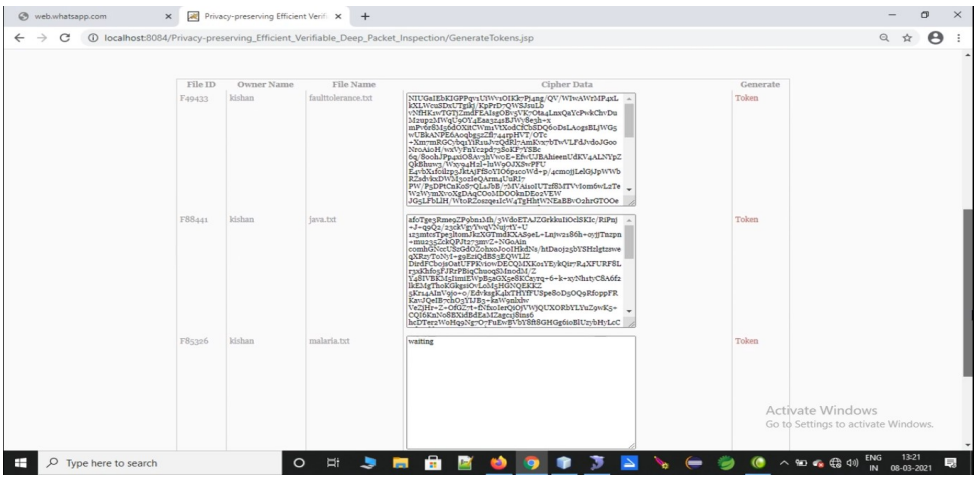


View rules

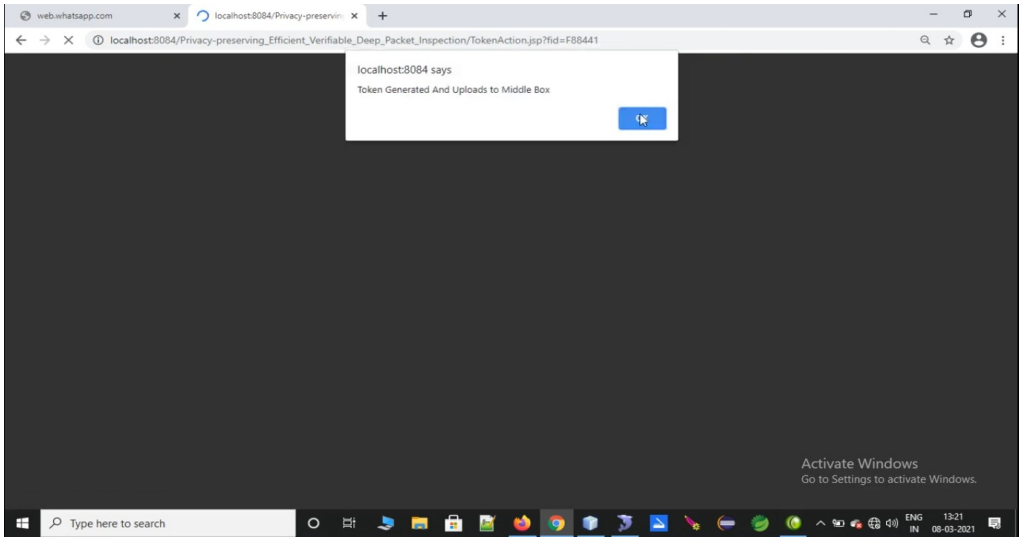


Generate token

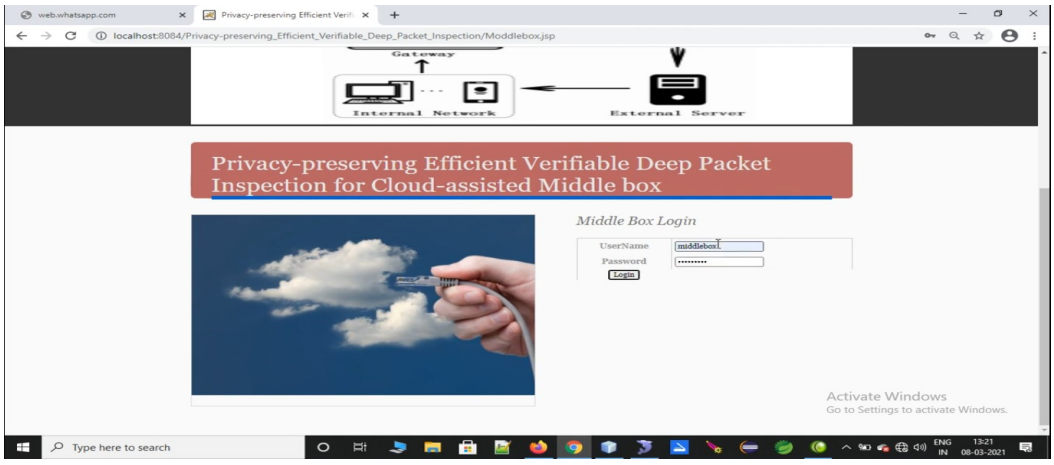
ISSN: 2278-4632
Vol-14, Issue-5, May: 2024



Generated status

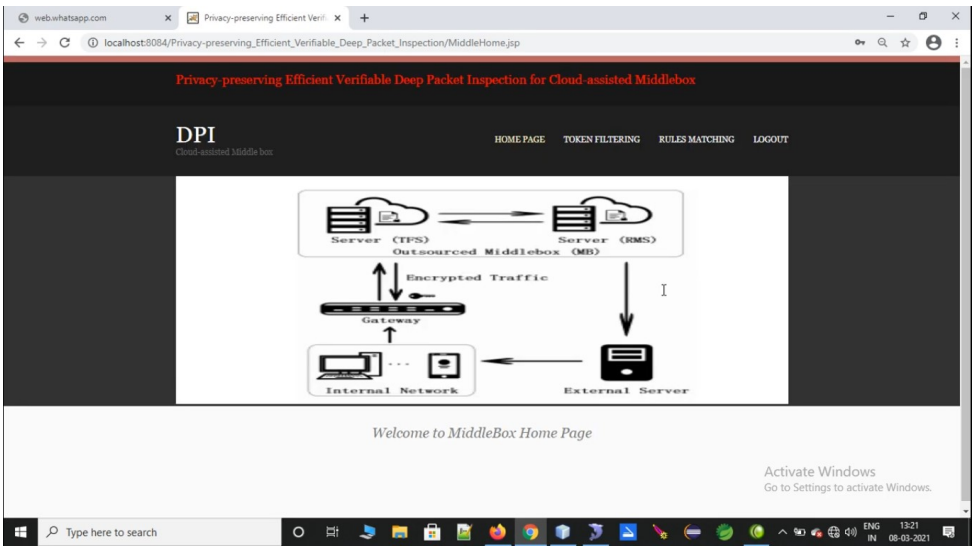


Middle box login

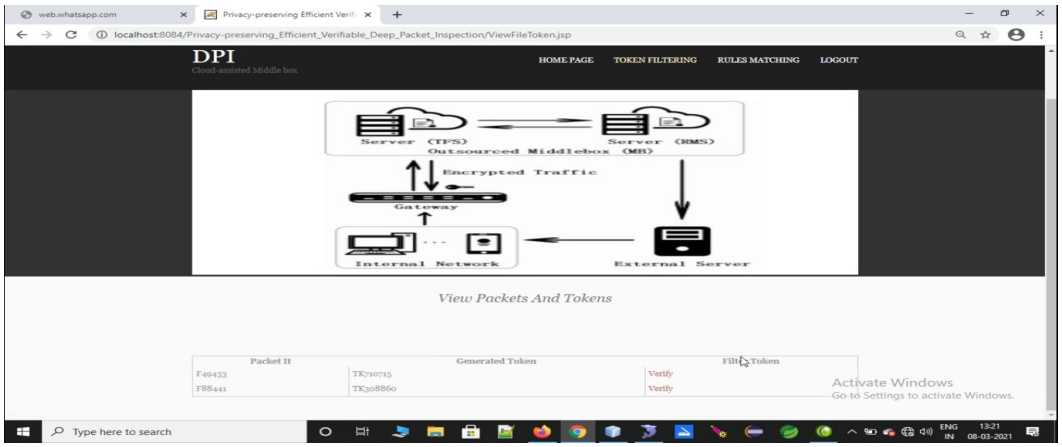


Home page

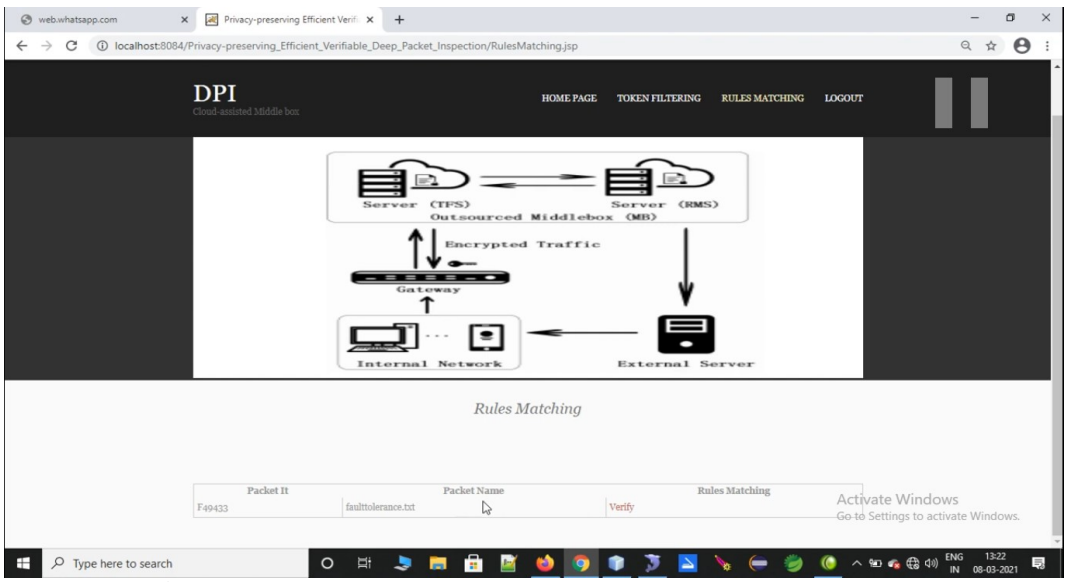
ISSN: 2278-4632
Vol-14, Issue-5, May: 2024



Token filter

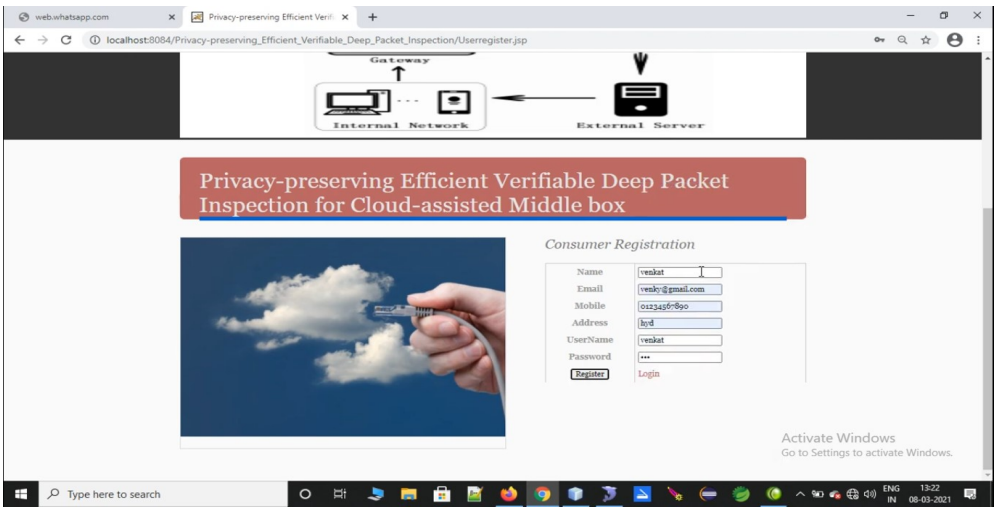


rules matching

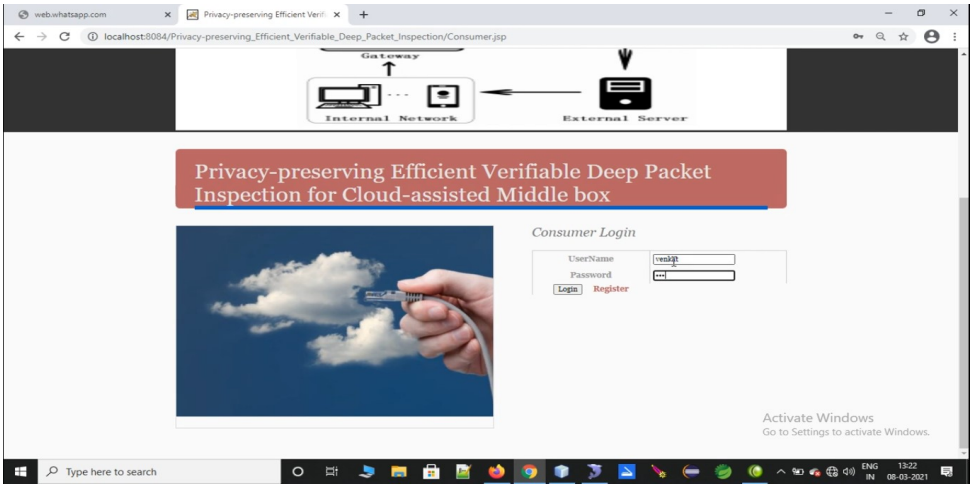


consumer register

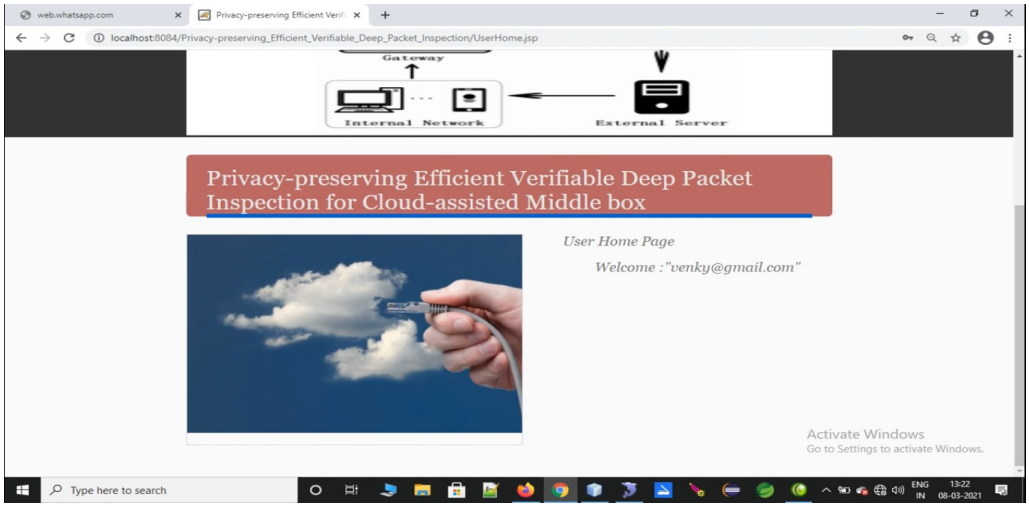
ISSN: 2278-4632
Vol-14, Issue-5, May: 2024



Consumer login

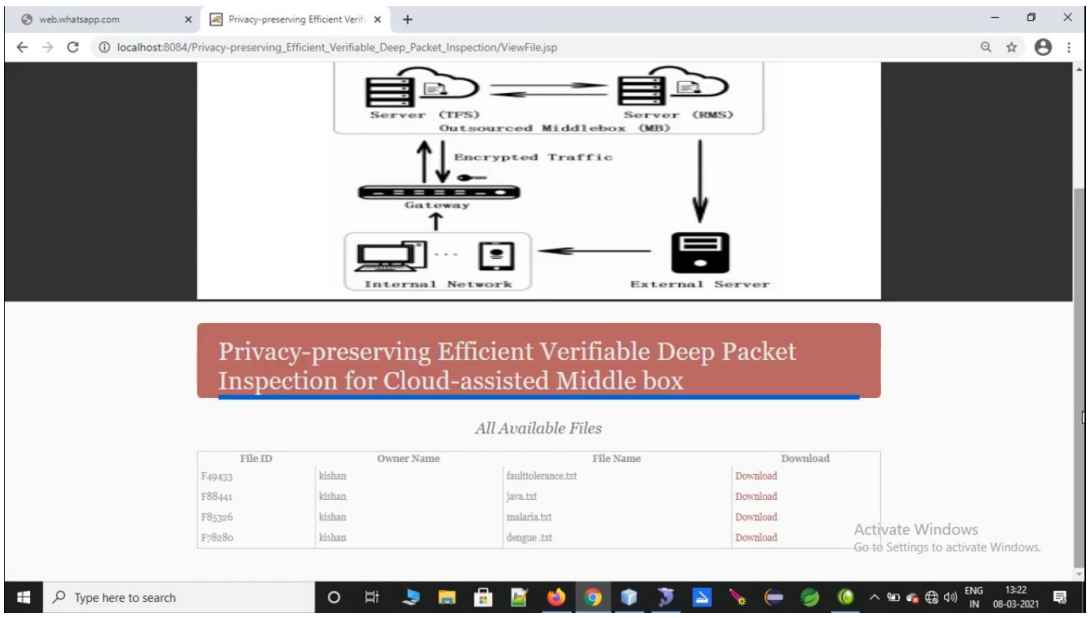


Consumer home page



view files and download

ISSN: 2278-4632
Vol-14, Issue-5, May: 2024



8.FUTURE SCOPE

The future scope for the proposed Efficient Verifiable Deep Packet Inspection (EV-DPI) scheme with strong privacy guarantees holds promise for several advancements and applications:

1. **Integration with Emerging Technologies**: As technology evolves, EV-DPI can integrate with emerging technologies such as edge computing and 5G networks. Edge computing can reduce latency by processing data closer to the source, while 5G networks can provide higher bandwidth and lower latency, enabling more efficient packet inspection and faster response times.

2. **Enhanced Security Measures**: With the constant evolution of cybersecurity threats, the EV-DPI scheme can be further enhanced to detect and mitigate advanced threats such as zero-day attacks, polymorphic malware, and insider threats. This can involve the incorporation of machine learning and artificial intelligence techniques to improve threat detection capabilities.

3. **Scalability and Flexibility**: As the volume of network traffic continues to grow exponentially, there will be a need for EV-DPI solutions that are highly scalable and flexible. Future research can focus on developing techniques to efficiently handle large-scale network traffic and adapt to dynamic network environments.

4. **Interoperability and Standardization**: To facilitate widespread adoption, future efforts can focus on ensuring interoperability and standardization of EV-DPI solutions across different cloud platforms and network infrastructures. This can involve collaboration with industry stakeholders and standardization bodies to develop common protocols and interfaces.

5. **Regulatory Compliance and Privacy Protection**: With increasing concerns around data privacy and regulatory compliance, future research can focus on enhancing the privacy-preserving capabilities of EV-DPI solutions to comply with regulations such as

ISSN: 2278-4632
Vol-14, Issue-5, May: 2024

GDPR (General Data Protection Regulation) and CCPA (California Consumer Privacy Act). This can involve the development of techniques for anonymizing sensitive data and providing users with greater control over their personal information.

9.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 andintermediate inspection results. Both inspection and verification protocols are able to preserve the privacy of packet payload and confidentiality of DPI rules. We havedemonstrated 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.

10. 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