

Research Paper

PRIVACY-PRESERVING AUTONOMOUS SYSTEM ROUTING VIA INTELLIGENT GRAPH FILTERING

D. KRISHNA VENI¹, JALA GOPIKA², SRIPATHI ESMITHA³, SAHUKAR UDAYKIRAN
YADAV⁴, SIDDANI GNANESHWARI⁵

¹Assistant Professor, Dept. of CSE, Guru Nanak Institutions Technical Campus, Ibrahimpatnam,
Telangana, India

^{2, 3, 4, 5} B.Tech, Dept. of CSE, Guru Nanak Institutions Technical Campus, Ibrahimpatnam,
Telangana, India

ABSTRACT— Traditional inter-domain routing protocols' decentralized architecture can cause a number of problems, such as misconfiguration and convergence problems. Alternative strategies that use the Software Defined Networking (SDN) paradigm to give more control over routing operations have been put forth recently in response to these issues. In this scenario, an SDN controller is assigned to handle routing duties in a multi-domain network made up of Autonomous Systems (ASs). Each controller must learn how to connect to any node outside of its domain in order to carry out inter-domain routing. Because the controllers must access sensitive, business-critical data (such link charges) across all domains, serious privacy issues arise. In order to preserve privacy,

protocols for determining the shortest path between a source and a destination a typical policy in routing tasks have recently been presented. These protocols rely on Multi-Party Computation (MPC) techniques, which limit scalability by ensuring anonymity at the expense of high computational and communication complexity. In this study, we use Data Mining (DM) approaches to eliminate nodes that have a low probability of being reached by the shortest path, thus pruning the network graph. On the pruned graph, privacy-preserving shortest path methods are then conducted at a significantly reduced complexity.

Index Terms – Inter-domain routing, Software Defined Networking (SDN), Autonomous Systems (AS), privacy-

preserving routing, shortest path computation, Multi-Party Computation (MPC), data mining, graph pruning, routing optimization, network privacy, scalable routing, secure communication.

I. INTRODUCTION

Internet traffic is delivered via an interconnection of a large number of Autonomous Systems (ASs), such as content and service providers, distributed over the whole globe. Inter-domain routing, i.e., the task of establishing paths to connect ASs across the Internet, is currently managed in a completely-distributed manner through the Border Gateway Protocol (BGP).

Along with its well-known advantages such as the possibility to implement a vast range of routing policies, BGP suffers from several issues, such as slow convergence and potential misconfigurations. Indeed, if a failure induces a change in network topology, BGP may require several minutes (up to 10 in some cases) to converge to a new routing solution, eventually resulting in the temporary unavailability of Internet services during the reconfiguration period.

As a consequence, designing alternative strategies for inter-domain routing remains a fundamental research objective. In this

regard, novel solutions that introduce a degree of centralization in current inter-domain routing protocols have been investigated. Specifically, as depicted in Figure 1, groups of ASs may form a multi-domain network where routing tasks are outsourced to a central controller that operates under the principles of the Software Defined Networking (SDN) paradigm. Within each multi-domain, routers transmit network status information to the controller, providing it with a comprehensive view of the network.

By exchanging information about their networks, the controllers converge to a common view of the overall network, thus implementing inter-domain routing policies that avoid the convergency issues of a decentralized scenario. We assume this SDN-oriented inter-domain routing model in this paper. However, this novel architecture permit a seamless integration with the existing architecture, as central controllers across various multi-domain networks may continue to employ the BGP protocol for communication.

The adoption of the above described SDN-oriented approach enhances scalability and stability in inter-domain routing, but it requires the exchange of sensitive

information about each network domain (e.g., link costs) to optimize routing strategies. In fact, the costs of inter-AS links between border routers are particularly sensitive data, as they could reveal confidential information about business relationships among ASs. Indeed, the inference of business relations between ASs has been the subject of extensive research. The adoption of the SDN-oriented architecture necessitates a high level of trust from network domain members, a requirement that can substantially impede the widespread acceptance of this approach. Therefore, solutions that ensure privacy are urgently needed.

Toward this aim, common routing operations, such as the computation of the shortest path between source and destination pairs, need to be implemented in a privacy-preserving manner, as done in for Dijkstra's algorithm. Such implementation relies on secure Multiple Party Computation (MPC) schemes, in which sensitive data are shared and processed in encrypted form to guarantee privacy.

The SDN-oriented architecture constitutes a favorable substrate for the adoption of MPC-based route computation algorithms, which can be executed by the controllers of the

multi-domain networks. The main drawback is that this secure processing comes at the cost of significant computational and communication overheads, which increase super-linearly with i) the number of involved MPC nodes and ii) the size of the network.

II. RELATED WORK

A. Taming the Transient While Reconfiguring BGP

In modern Internet infrastructure, Border Gateway Protocol (BGP) plays a critical role in enabling communication between multiple Autonomous Systems across large-scale networks. However, during routing reconfiguration processes such as policy updates, topology modifications, or link failures, transient routing issues can occur, causing packet loss, forwarding loops, congestion, and temporary service interruptions. Traditional BGP reconfiguration methods often fail to guarantee stable and disruption-free routing updates, especially in highly dynamic network environments. This project focuses on developing a reliable framework to control and minimize transient routing problems while reconfiguring BGP networks. The proposed system introduces intelligent routing coordination mechanisms that analyze routing dependencies and safely

schedule network updates without violating forwarding consistency. The framework uses graph-based analysis, Software Defined Networking (SDN) concepts, and automated verification techniques to predict unsafe routing transitions before deployment. It also incorporates optimized update sequencing methods to reduce convergence delays and improve overall routing stability. Additionally, the system supports scalable deployment across large multi-domain networks with heterogeneous routing policies and complex interconnections. The project evaluates routing performance using real-world and simulated BGP topologies to measure packet loss reduction, convergence speed, network availability, and transient disruption rates. Furthermore, adaptive recovery strategies and policy-aware reconfiguration techniques are integrated to improve fault tolerance and operational efficiency. By enabling safe and efficient BGP reconfiguration, the proposed framework provides a scalable and dependable solution for enhancing Internet routing reliability, service continuity, and next-generation communication network stability.

B. Vertical Split Learning-Based Identification and Explainable Deep

Learning-Based Localization of Failures in Multi-Domain NFV Systems

Modern Network Function Virtualization (NFV) systems operate across multiple domains and cloud infrastructures, making fault detection and localization highly challenging due to distributed resources and complex service dependencies. Traditional failure management techniques often struggle to provide accurate and privacy-preserving analysis in multi-domain environments. This project focuses on developing an intelligent framework for identifying and localizing failures in NFV systems using vertical split learning and explainable deep learning techniques. The proposed system allows multiple domains to collaboratively train deep learning models without directly sharing sensitive operational data, thereby preserving privacy and security. Vertical split learning divides the model training process across domains while enabling efficient knowledge sharing for accurate fault identification. Additionally, explainable AI mechanisms are integrated to provide transparent insights into the root causes and locations of failures within virtualized network services. The framework supports real-time monitoring, anomaly detection, and efficient troubleshooting across distributed NFV infrastructures. The

system is evaluated using network performance metrics such as detection accuracy, localization precision, response time, and scalability under dynamic network conditions. By combining privacy-preserving collaborative learning with explainable deep learning, the project provides a secure, scalable, and intelligent solution for improving reliability and fault management in next-generation NFV and SDN-enabled communication networks.

C. Privacy-Preserving Shortest Distance Query for Dynamic Large-Scale Road Network

Modern intelligent transportation systems and location-based services rely heavily on shortest distance queries to provide efficient navigation and traffic management across large-scale road networks. However, traditional shortest path computation methods often require users to reveal sensitive location information to centralized servers, leading to serious privacy and security concerns. This project focuses on developing a privacy-preserving framework for shortest distance query processing in dynamic large-scale road networks. The proposed system enables users to compute shortest travel distances without exposing their exact locations, travel patterns, or query information to untrusted entities. The

framework integrates secure computation techniques, encrypted query processing, and privacy-preserving routing mechanisms to protect sensitive data during route computation. Additionally, the system is designed to efficiently handle dynamic road conditions such as traffic congestion, accidents, and topology updates in real time. Advanced optimization strategies are incorporated to reduce computational overhead and improve query response time for large-scale networks. The project also supports scalable deployment in smart transportation infrastructures and cloud-based navigation systems. Performance evaluation is conducted using metrics such as query efficiency, privacy protection level, computation cost, communication overhead, and routing accuracy. By combining secure shortest distance computation with dynamic traffic adaptability, the proposed framework provides a scalable, efficient, and privacy-aware solution for next-generation intelligent transportation and navigation systems.

D. Homomorphic Routing: Private Data Forwarding in the Internet

Modern Internet communication systems require efficient routing mechanisms to forward data packets across multiple networks and domains. However, traditional routing protocols expose sensitive routing

information and packet forwarding details to intermediate nodes, creating serious privacy and security concerns. This project focuses on developing a privacy-preserving routing framework using homomorphic encryption techniques for secure data forwarding in the Internet. The proposed system enables routers and network devices to process routing information directly on encrypted data without decrypting the original content. By leveraging homomorphic routing methods, the framework protects sensitive user information, routing paths, and forwarding policies from unauthorized access and traffic analysis attacks. The system is designed to support secure packet forwarding while maintaining routing efficiency and scalability in large-scale Internet infrastructures. Additionally, optimized cryptographic operations are incorporated to reduce computational overhead and communication latency during encrypted routing operations. The framework also addresses challenges such as secure path computation, privacy-preserving traffic engineering, and compatibility with existing Internet routing architectures. Experimental evaluation is performed using different network topologies to analyze encryption overhead, forwarding efficiency, scalability, and privacy protection levels.

III. PROPOSED METHODOLOGY

This paper, we propose a new approach based on Data mining methodologies. Specifically, we develop an DM-based system that prunes the inter-AS network graph in such a way that the obtained sub-graph contains only the nodes that more likely belong to the shortest path between a source/destination pair. More specifically, our system is based on a DM algorithm trained to compute the likelihood that each node belongs to the shortest path between a source and a destination and, if its likelihood is below a certain threshold, that node is pruned from the network. More details are provided in. The privacy-preserving shortest path computation is then executed on the pruned network. Such implementation relies on secure Multiple Party Computation (MPC) schemes, in which sensitive data are shared and processed in encrypted form to guarantee privacy.

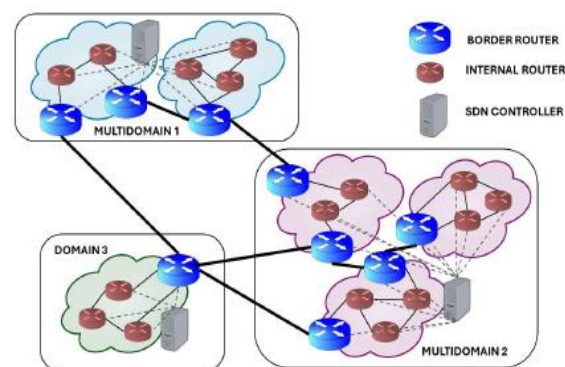
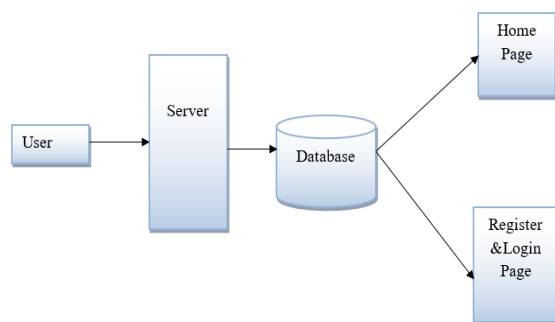


Fig. 1: System Overview

3.1 User Interface Design

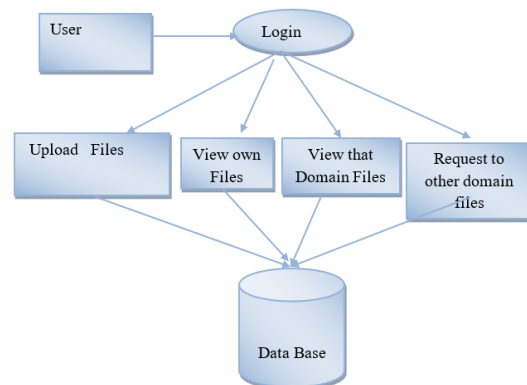
To connect with server user must give their email and password then only they can able to connect the server. If the user already exists directly can login into the server else user must register their details such as username, password, Email id, City and Country into the server. Database will create the account for the entire user to maintain upload and download rate. Name will be set as user id. Logging in is usually used to enter a specific page. It will search the query and display the query.



3.2 User

The User Module is designed to manage all user related operations within the SDN based file sharing system. In this module, users can register by providing their personal details and securely log in using their username and password. After successful authentication, users are allowed to upload files into their respective domains for secure storage and sharing. The module enables users to view their uploaded files as well as access files available in other domains based on system

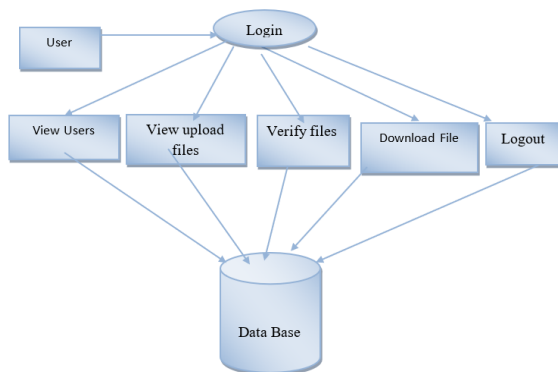
permissions. Users can request file downloads from other domains through the shortest path communication mechanism supported by the SDN environment. The system identifies the optimal routing path to reduce transmission delay and improve download efficiency. Once the request is approved, users can securely download the required files. The module ensures secure communication, proper access control, and efficient file sharing across multiple domains. Overall, the User Module improves collaboration, accessibility, and reliable data transfer in the network.



3.3 Router

The Router Module is responsible for managing routing operations and file verification processes within the network environment. In this module, routers securely log into the system and monitor communication activities between different domains. The router can view registered

users, domain related files, and uploaded data shared across the network. One of the major responsibilities of this module is verifying uploaded files before they are allowed for further processing or sharing. The verification process helps in identifying invalid, corrupted, or unauthorized files to maintain network security and data integrity. Routers also support shortest path routing by analyzing available network paths for efficient data transmission. This module ensures smooth communication between users and domains while minimizing congestion and delay. The Router Module plays an important role in maintaining reliable routing and secure file management within the SDN architecture.

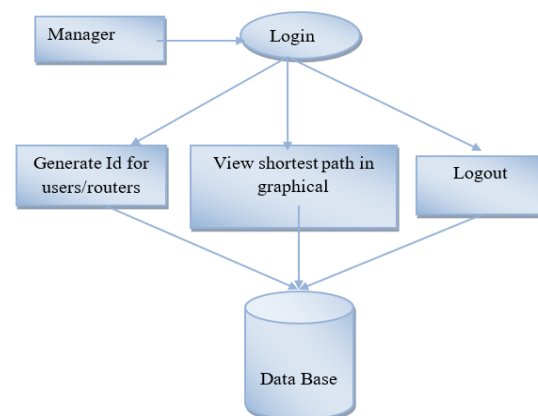


3.4 Manager

The Manager Module acts as the central administrative management system for controlling users, routers, and file routing operations. In this module, the manager

securely logs into the system and supervises overall network activities.

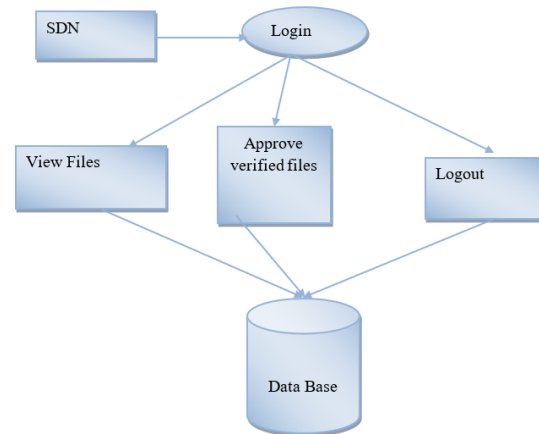
The manager generates unique IDs for users and routers to maintain proper identification and secure communication within the network. This module also monitors file download requests and visualizes the shortest path routing process in graphical format for better analysis and monitoring. The graphical representation helps in understanding network communication flow, routing efficiency, and transmission performance between domains. The manager maintains records of file transfers, user activities, and routing operations to improve system management. Additionally, the module helps in coordinating between routers and the SDN controller for secure file verification and access approval. Overall, the Manager Module provides centralized monitoring, routing management, and efficient control over the entire SDN based system.



3.5 SDN Controller

The SDN Controller Module is responsible for controlling and managing the Software Defined Network operations within the file sharing environment. This module acts as the intelligent decision making component that supervises communication between users, routers, and domains. After routers verify uploaded files, the SDN controller analyzes the verification status and provides approval for secure file sharing and downloading. The controller manages traffic flow, routing policies, and access permissions dynamically to improve network efficiency and reduce communication delay. It supports shortest path routing by selecting optimized transmission paths for faster and reliable file transfer. The SDN Controller continuously monitors network conditions and coordinates with routers to ensure secure and stable communication.

It also prevents unauthorized file access and maintains centralized network control. Overall, the SDN Controller Module enhances network performance, security, and intelligent routing management in the SDN based multi domain file sharing system.



IV. EXPERIMENTAL RESULTS AND ANALYSIS

The experimental results show that the proposed method improves privacy-preserving inter-domain routing by reducing the size of the network graph before shortest path computation. The use of data mining-based graph filtering lowers computational and communication complexity compared to traditional MPC-based approaches. At the same time, it protects sensitive routing information across domains. Overall, the framework offers a more scalable and efficient solution for secure SDN-based routing.



Fig. 2: Home Page

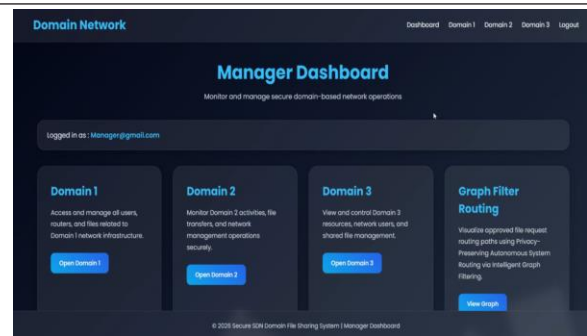


Fig. 6: Manager Dashboard

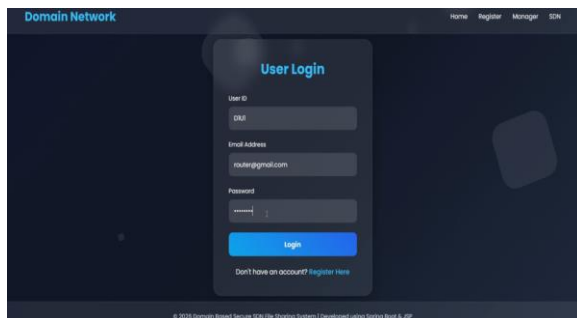


Fig. 3: Registration



Fig. 6: Results

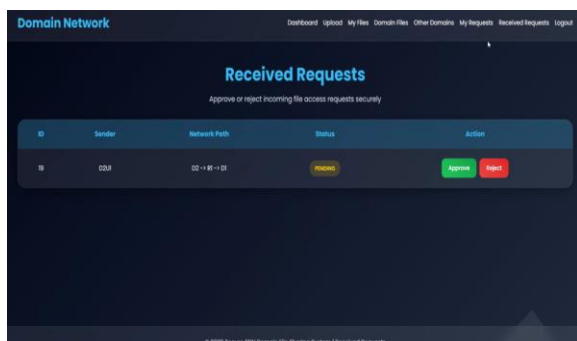


Fig. 4: Received Request

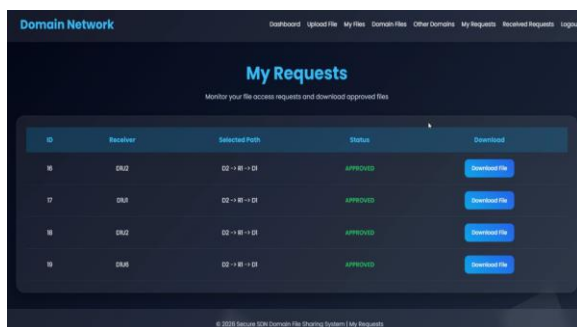


Fig. 5: View Request

V. CONCLUSION

The proposed SDN based multi domain secure file sharing system provides an efficient and privacy preserving solution for inter domain communication and routing management. The system successfully integrates Software Defined Networking concepts with secure shortest path computation to improve file sharing, routing efficiency, and network performance across multiple domains. By using Multiple Party Computation (MPC) techniques, the proposed model protects sensitive routing information and maintains data privacy during shortest path calculation. The

integration of Data Mining based graph pruning further reduces computational complexity and communication overhead, resulting in faster and more scalable routing operations.

The User, Router, Manager, and SDN Controller modules work together to ensure secure authentication, file verification, optimized routing, and controlled file access. Overall, the system achieves reliable communication, improved security, reduced delay, and efficient resource utilization, making it suitable for future large scale SDN enabled network environments.

REFERENCES

- [1] Y. Rekhter, T. Li, and S. Hares, “A border gateway protocol 4 (bgp-4),” Internet Eng. Task Force (IETF), Tech. Rep. RFC 4271, 2006.
- [2] A. Narayanan, “A survey on BGP issues and solutions,” 2009, arXiv:0907.4815.
- [3] T. Schneider, R. Schmid, S. Vissicchio, and L. Vanbever, “Taming the transient while reconfiguring BGP,” in Proc. ACM SIGCOMM Conf., Sep. 2023, pp. 77–93.
- [4] H. Zang, J. P. Jue, and B. Mukherjee, “A review of routing and wavelength assignment approaches for wavelength-routed optical WDM networks,” Opt. Netw. Mag., vol. 1, no. 1, pp. 47–60, 2000.
- [5] Q. Chen, S. Shi, X. Li, C. Qian, and S. Zhong, “SDN-based privacy preserving cross domain routing,” IEEE Trans. Dependable Secure Comput., vol. 16, no. 6, pp. 930–943, Nov. 2019.
- [6] K. Phemius, M. Bouet, and J. Leguay, “DISCO: Distributed multi domain SDN controllers,” in Proc. IEEE Netw. Operations Manage. Symp. (NOMS), May 2014, pp. 1–4.
- [7] S. Goldberg, “Why is it taking so long to secure Internet routing?” Commun. ACM, vol. 57, no. 10, pp. 56–63, Sep. 2014.
- [8] A. Mitseva, A. Panchenko, and T. Engel, “The state of affairs in BGP security: A survey of attacks and defenses,” Comput. Commun., vol. 124, pp. 45–60, Jun. 2018.
- [9] X. Dimitropoulos, D. Krioukov, M. Fomenkov, B. Huffaker, Y. Hyun, K. Claffy, and G. Riley, “AS relationships: Inference and validation,” ACM SIGCOMM Comput. Commun. Rev., vol. 37, no. 1, pp. 29–40, Jan. 2007, doi: 10.1145/1198255.1198259.
- [10] L. Gao, “On inferring autonomous system relationships in the Internet,”

IEEE/ACM Trans. Netw., vol. 9, no. 6,
pp. 733–745, Dec. 2001.

Nanak Institutions Technical Campus
affiliated to JNTUH in 2022-2026.

AUTHORS Profile



Mrs. D. Krishna Veni
has received her B.Tech
from JNTUH,
Hyderabad in 2011,
M.Tech degree in

Computer science from JNTUH, Hyderabad
in 2021 and Pursuing Ph.D degree in
Computer Science from Guru Naanak
university, Ibrahim patnam. She is dedicated
to teaching field from the last 8 years. Her
research area Machine Learning. At present
She is working as Assistant Professor in CSE
Department at Guru Nanak Institutions
Technical Campus, Ibrahimpatnam,
Telangana, India.



**Mr. SAHUKAR UDA-
YKIRAN YADAV**

pursuing B.Tech degree
in Computer Science and
Engineering at Guru
Nanak Institutions Technical Campus
affiliated to JNTUH in 2022-2026.



**Ms. SIDDANI
GNANESHWARI**

pursuing B.Tech degree
in Computer Science
and Engineering at
Guru Nanak Institutions
Technical Campus affiliated to JNTUH in
2022-2026.



Ms. JALA GOPIKA
pursuing B.Tech degree
in Computer Science and
Engineering at Guru
Nanak Institutions

Technical Campus affiliated to JNTUH in
2022-2026.



**Ms. SRIPATHI
ESMITHA** pursuing
B.Tech degree in
Computer Science and
Engineering at Guru