ISSN: 2584-0495

Vol. 1, Issue 5, pp. 335- 341

IJMIT International Journal of Microsystems and IoT

International Journal of Microsystems and IoT

ISSN: (Online) Journal homepage: https://www.ijmit.org

Indian Society for VLSI Education

Methods for Storage Intrusion Mitigation with Data Transport Security Tunnels

Shankaramma, Nagaraj G S, Peter Chacko

Cite as: Shankaramma, & Nagaraj, G. S. Chacko, Peter (2023). Methods for Storage Intrusion Mitigation with Data Transport Security Tunnels. International Journal of Microsystems and IoT, 1(5), 335-341. https://doi.org/10.5281/zenodo.10254103

Published online: 23 October 2023.

CrossMark

DOI: https://doi.org/10.5281/zenodo.10254103

International Journal of Microsystems and IoT
Vol. 1, Issue 5, pp. 335-341; DOI: https://doi.org/10.5281/zenodo.10254103

Methods for Storage Intrusion Mitigation with Data Transport Security Tunnels

Shankaramma[1], Nagaraj G S[2], Peter Chacko[3]

[1,2]Department of Computer Science Engineering, R. V. College of Engineering, Bengaluru, Karnataka, India

[3]Neridio Systems Ltd, Bangalore, Karnataka, India

ABSTRACT

Securing the data is very important nowadays because a lot of data breaches are happening, every now and then. Many large and branded corporations are the huge victims of cyber security breaches. Encryption and authentication offer a good amount of security; however, these cannot be included as an integrated solutions and it does not seem to be the end goal over the data life cycle when the data is in motion. Many security tunnels are available such as Virtual Private Network (VPN), Software Defined Wide Area Network (SD-WAN), which can transfer the data from however they do not consider mitigating various types of cyber-attacks, wiretapping. Therefore, it is an extension to fill the research gap to build the global wide area tunnelling for cyber security in motion product. The present work relates to cyber-attack mitigation, information-theoretic security in motion, at rest. Methods are included for storage intrusion mitigation with content routing across an overlay network. Overlay network is built upon Data Transport Security Controllers (DTSC), System modules are operating at the control of Universal Controller (UC). Securing data at motion is provided through erasure coding and encryption. Securing data at rest is provided by storing it in safe vault, were constantly data sync from proxy system and incorporating data distributed across multiple vaults.

KEYWORDS
Wiretapping, Security Tunnels Ransom attack, Cyber Security, Storage Intrusion Mitigation, Data Transport Security Controllers, Universal Controller, Safe Vault

1. INTRODUCTION

Data is one of the major and precious strengths of an organization. Data can be of three different categories. Data in transit or movement, Data at rest and Data in use. Data is in movement pointing to data carried from one site to another. When the data is in motion, the contents are transferred from one location to another, it is essential to safeguard the data from all kinds of cyber-attacks and wiretapping. Most of the attacker's intercept and try to steal the data and modify the information contents. Attackers are becoming more intelligent while adopting new methods to exploit the vulnerabilities of the existing setup. In a way, the entire system gets hacked and compromised.

The data encryption for data in use and data at rest is mentioned in [1]. There are various ways to protect the data within the organization, and it is equally important and essential to safeguard financial records and employee data. The data encryption methods can be incorporated easily to encode the information in an unreadable format and authenticate it. It can make sure that only authorized users are able to modify and access the data. However, these methods cannot be considered as a complete solution when data protection is a major concern for data in motion. There is high time to take power over data and defend it from hacks when the data is in motion. For corporations or any organizations, if they have branch offices at different locations, it is very much required for them to have their own secure tunnel to transfer the data and protect the data from various kinds of cyber-attacks.

When numerous amounts of sensitive data are present, like financial reports, and Health records, the best method would be encrypting and transferring the data from one place to another, however, it may get disturbed by other traffic. The legitimate data traffic would need a separate channel or tunnel, a secure passage to deliver data in the most secure fashion. The established channel can be used to transfer the data securely. Security enhancements while data transfer is mentioned in [2]. The safety tunnel would also mitigate various cyber-attacks such as wiretapping, and ransom attacks. Various cyber threats are mentioned in [3] also to be mitigated when the data is in motion. The main idea is to create a secure tunnel to forward the legitimate traffic. The end-to-end communication will take place i.e., data movement from A to B through required protocols, and data conversions to suit for different interfaces. The private network moves the data or information towards a larger network or internet. The most common tunnel is the VPN tunnel used by more corporate offices which does not protect the data from cyber-attacks mentioned in [4]. Fig 1 shows how the traffic flows to and from VPN. When the user is trying to connect to VPN, immediately the user is directed to website or captive portal, where all the credentials are entered. All the user login details are captured by the attacker in a captive portal and that is how attackers get hold of all the important logging information and high chance of data breach taking place. The user who is trying to access the VPN end up giving all the important data. In a way, the user information will be accessed by the attackers and attackers steal important data information with the illegal use of credentials.

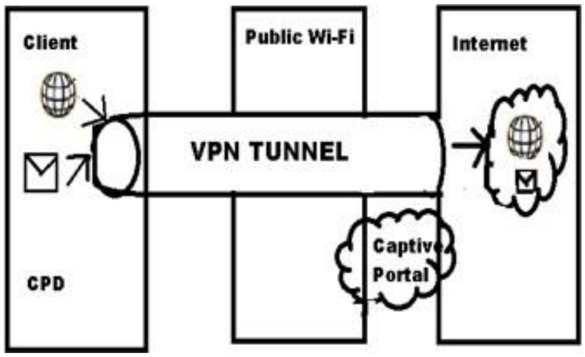


Fig. 1 Data Traffic Movement to and from VPN [4]

It is also equally important that when data is at rest or in use, continuously monitoring must be incorporated to check whether attacker has modified any binary, increased number of processes. Then certain action to be taken such as stopping the migration of data and booting the client machine migration of data and booting the client machine.

2. BACKGROUND

Traditional Storage systems have been built with initial goals of performance of a storage system, scalability, and reliability aspects. It was always considered that data can be stored inside a secure and safe perimeter of a corporation and hence network security systems would protect data from external attacks. Such storage systems added security on an extra feature approach rather than security is a part of approach by design. Encryption, authentication, and identity management offer good amount of security but not built as an integrated solution and does not look at end to end perspective over data lifecycle when data is in transit. Traditional storage systems do not address end-to-end data-centric security in motion in the context of wiretapping and cyber-attacks on encrypted data streams. In the present work, a list of methods, System, and architecture to detect intrusions to storage systems, mitigating it and securing data during motion with information theory, secure content forwarding across an overlay network and system security techniques are implemented. The data at rest should be also protected by storing in multi-node vault systems as more data theft happens when data is at rest.

3. LITERATURE SURVEY

The Data Transport Security Tunnels belongs to various domains like cyber security, cloud security, computer networking, Information security etc. A lot of research has been done on this topic and several researchers have written scientific articles and research papers on various security tunnels and data transmission through the tunnels. The summary of the same is mentioned below, in the literature survey.

Automation of VPN Tunnel Deployment between Trusted Users is described in [5]. The work incorporates REST API to perform client to server communication. Once the tunnel is deployed the configuration update is carried out from server to client. The work depicts a method of deploying VPN in Linux. It also provides higher security and safety; the user can securely connect through the tunnel, transmit the data securely and evaluate the performance.

Open V Proxy: Low-Cost Squid Proxy Based Teleworking Environment with OpenVPN Encrypted Tunnels to Provide Confidentiality, Integrity and Availability is proposed in [6], a solution is being proposed for the existing network environments with spending too much money, utilizing the capability of deploying open VPN to work remotely in secure fashion along with maintaining confidentiality, integrity, and availability. The proposed solution will be varying for single and multiple organizations. With the use of Open Proxy at time around 250 clients can work securely and simultaneously.

Reinforcing Protection against Chosen-plaintext Attack using Ciphertext Fragmentation in Multi-cloud Environments is described in [7]. The proposal here is to modify SFD (Secure Fragmentation and Dispersal) to be more resistant and secure towards chosen plain text attack, making it very difficult for the adversary to get hold of all the fragments. The proposed method includes the separation of the halves of cipher block, instead of separating the continuous blocks of ciphertext, and performance is analysed and compared with initial SFD.

Improving Security and Privacy Attribute Based Data Sharing in Cloud Computing is proposed in [8]. CP-ABE (Ciphertext-Policy, Attribute Based Encryption) technique privacy preserving model is incorporated as a solution. The depiction of how user privacy and confidentiality is achieved without adding a greater number of computations in decryption algorithm is also present here.

Cyber KPI for Return on Security Investment is proposed in [9]. In this paper a solution is proposed by referring to various metrics like foiled attacks, vulnerabilities, and threats etc and by considering Key performance indicators, since there are no fixed metrics used by any organization, return on investment is measured.

An Empirical Analysis of Plugin-Based Tor Traffic over SSH Tunnel is proposed in [10]. The issue of validating the traffic and normal SSH traffic and tor traffic are compared with different plugins such obfs3 and obfs4 is addressed here. Various Upstream and Downstream flows are checked against metrics such as accuracy rate and false positive rate.

On Deep Reinforcement Learning for Traffic Engineering in SD-WAN is mentioned in [11]. Here, it is being suggested that establishing WAN is more efficient as compared to MPLS. Different Traffic Engineering are incorporated to sustain the solutions of services of WAN. The reward function is extended to include increasing performance with respect to SD-WAN at the customer premises equipment.

Social SDN: Design and Implementation of a Secure Internet Protocol Tunnel between Social Connections is included in [12]. The proposed solution here is the building tool, which resolves the issues with respect to E2EE network services. Social SDN (Software Defined Network) Need to support ad-hoc Wi-Fi so that secure peer-to-peer connections can be made without the need for any third-party infrastructure.

Taxonomy of Challenges in Cloud Security [13]. The

Fundamentals of cloud computing and security concerns, various risks and solutions in cloud are highlighted here. Various open research questions about cloud protection are analysed. This is mainly since cloud protection poses the largest issue for data owners. Open-ended data protection problems will continue to affect clouds. However, this paper does not cover all aspects of cloud security.

Enabling Cyber Security Data Sharing for Large-scale Enterprises Using Managed Security Services is mentioned in [14]. When using the MSS (Managed security services) platform, attempts to keep combining and keep confidentiality when sharing data are made. Sharing the data within managed security service platforms daily would be difficult. The MSS environment is complex, and the different components are integrated in a complicated manner. This paper also underlines the challenges of data sharing MSS platform.

4. PROPOSED WORK

The proposed work relates to a set of methods and architectures for implementing cyber risk mitigation and information security services for data in motion and data at rest.

Securing Data in Motion

To secure data in motion, the overlay tunnel is built on number of Data Transport Security Controller nodes, which is centrally controlled by Universal Controller. The node failure, adopting a new route to transmit the data from source to destination across security tunnels details are specified in this section. Figure 2 shows system architecture of data transport security tunnels.

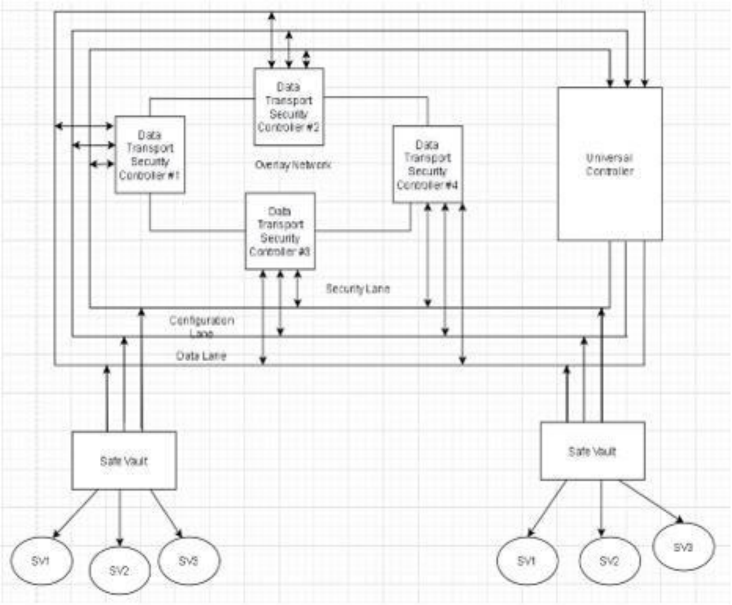

Data Transport Security Controller #2
Data Transport Security Controller #1
Overlay Network
Data Transport Security Controller #4
Universal Controller
Data Transport Security Controller #3
Security Lane
Configuration Lane
Data Lane
Safe Vault
Safe Vault
SV1
SV2
SV3
SV1
SV2
SV3

Fig. 2 System Architecture of data transport security tunnels

The major components are Data Transport Security Controller, Universal Controller, Safe vault. DTSC is the heart of the Architecture. Which constantly sync various security data and interstate data graph with Universal Controller. Universal Controller has various modules integrated for metadata, security contexts, telemetry data captured from different systems. Safe Vault is the static end, connecting other parts to storage at-rest. The present disclosure shows end to end security and guarantees the data during motion.

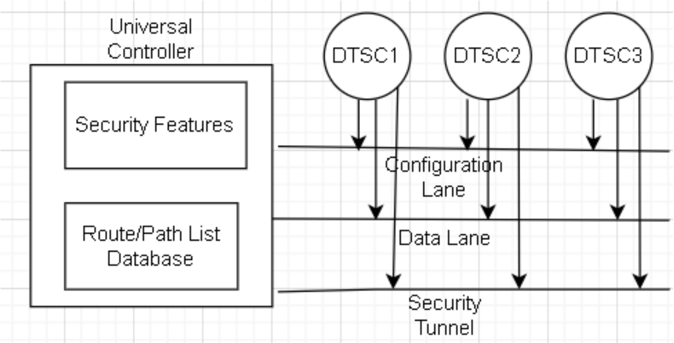


Fig. 3. Data Transport Security Controller Overlay Tunnel

Data Transport Security Controller uses separate channels for control or configuration of traffic, Data Traffic, and security traffic. There are 3 lanes mentioned such as Control &Config Lane, Data Lane, and Security Lane. UC contains Security features Database and Route/Path Database list. Security lane will carry traffic for Data Transport Security Controller List Database which is depicted in figure 3.

The DTSC route information and configure information is updated through the plane control. The Rx receiver module receives the traffic from any of the connected DTSC nodes. Then Tx module will further forward the data to upstream nodes. The originator module will further forward the content to upstream DTSC nodes. According to the hello message response update, the Data Transport Security Tunnel overlay tunnel route would be updated.

Conventional neighbor reachability and link state graph building method of underlay, packet level routing cannot be applied here, as all Data Transport Security Controller nodes are not L2/L3devices but operate at application level.

In overlay network routing, at application layer, all the end-to-end delivery of data fragments will be handled by University Controller-Data Transport Security Controller pair. The details of the data fragments created mentioned in the next session. UC also has various metadata for storage security management and security state and system state of various connected parts which are recently stored.

The data will be transmitted to receiver from sender through overlay network, in terms of data fragments. In this work Reed Solomon on erasure coding is incorporated to split the data contents into secret and not intelligible partitions or groups.

With reed Solomon algorithm combination is available, if a content of data is split into N pieces, only M pieces needed for fully recovery, only M pieces of the content will be sent to M distinct list Data Transport Security Controllers in a overlay network. As shown below figure before erasure coding, the data content can be redacted with blocks of data removed as gap blocks [27].

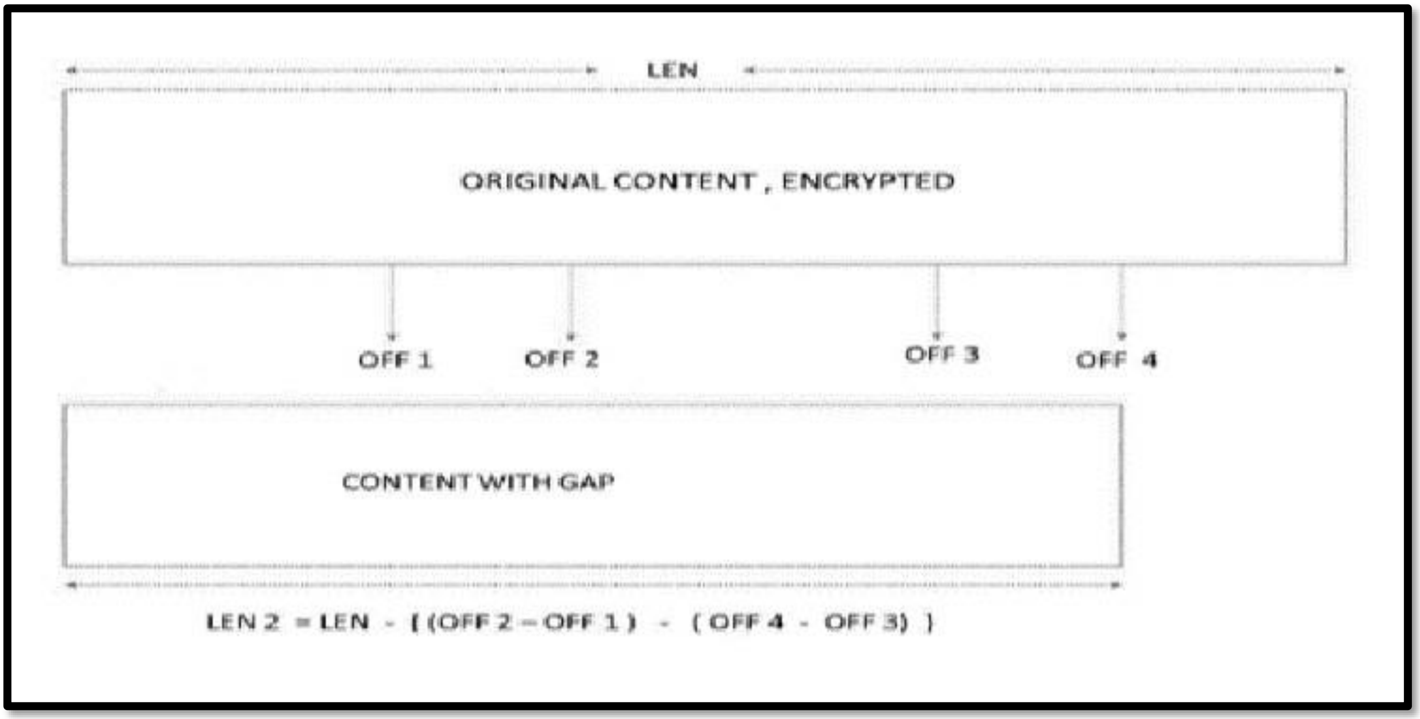

LEN
ORIGINAL CONTENT , ENCRYPTED
OFF 1
OFF 2
OFF 3
OFF 4
CONTENT WITH GAP
LEN 2 = LEN - [(OFF 2 – OFF 1) - (OFF 4 - OFF 3)]

Fig. 4 Fragment Creation from the data

The file or customer uploaded data can be split into either 3 fragments using reed solo man erasure coding. Once the minimal number of partitions or fragments are received in the data communication of erasure coding, the encryption key is left with the data before making the secret split, and those fragments are transmitted to the destination node. With reed Solomon erasure coding, if three fragments are made, then out of which two of the fragments are sent to different routes or paths to the destination. At the destination, the file will be recovered from those fragments. Out of 3, only two partitions are required for data recovery i.e., only m pieces are needed.

Once the fragments are created, every DTSC node is to look up the next hop listed in the routing list created at the first DTSC node. Every different fragment of data is referred to as a fragment set. Each member of the minimal fragment set receives a unique set of path lists, embedded in the fragment, and transmitted by the first DTSC node. Then every next node, simply look at the list, and update the next node and this process repeats until the fragment reaches the last Data Transport Controller node. As each fragment goes through an exclusive list of routes are referred to as an Exclusive path routing.

Securing data at rest

When data is stored in any public cloud storage based on some form of object storage is referred to as a Data vault. Data Vaults run in a generalized manner and have open ports for receiving connections. In connection with this, Safe Vault referred to Figure 2 is the enabling component to implement security at the rest part of the specification. It is very common to store file-level data in the file systems or in object storage systems.

5. EXPERIMENTAL FRAMEWORK

5.1 SECURING DATA IN MOTION

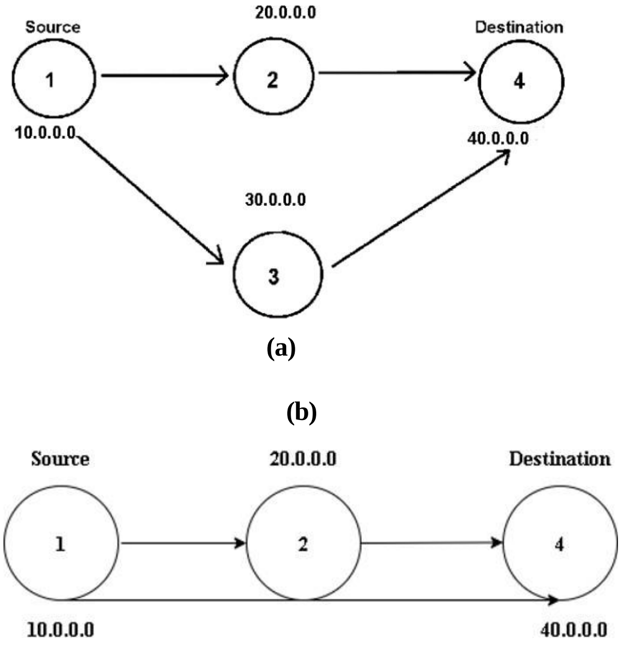
The test was performed by using 4 nodes in a virtual machine. The sender node has the IP address say 10.0.0.0, and the node is configured with the required binary and library. The sender script was initiated through GUI mode, then the sender script will add the source and destination address and by using RAID binary, 3 fragments will be made which was mentioned in erasure coding. The sender node will send a Hello message to all the intermediate nodes, based on the Hello message response, the fragments will be sent to a particular intermediate node.

```
sudo ssh root@10.0.0.0
sh senderscrpipt.sh
```

Root access to the system, then invoke the sender script, once the sender script is invoked, fragments will be sent to intermediate nodes. The fragments created will be stored at the following path. By specifying the IP address and port number, created fragments would be sent to the intermediate node’s lane buffer. Further, through all intermediate nodes, it reaches to receiver node.

```
tree /home/frag/Ramp/1/
sudo /ath/bin/Client $nodeIP2 30006 $i inramp/lane_1/$i
```

The receiver script is executed, and acknowledgment will be sent to the sender. Once sender gets the ack of data, then sender machine will remove the sent files. Based on the Rx is up and running in each node, the sender transfers the data to corresponding node. Fig 5 a) shows if two intermediate nodes are up and running, then fragments from source to destination will reach passing along intermediate nodes. The fig 5 b) depicts if one of the intermediate nodes, is down say node 3 is down, then fragment will be sent directly to destination from source. So, it indicates that if any of the fragments are lost, still we can recover the file.



(a)

(b)

Fig. 5 Experimental Framework

In this way, we are creating a virtual path tunnel with number of Data Transfer Security Controller nodes, Data Fragments would be sent to receiver across intermediate nodes. Each node maintains routing list before traversing, static routing is carried out. Wiretapping and other cyber-attacks are mitigated.

Securing Data at Rest

There will be a proxy and vault in secure vault. Proxy is the system that contains the files that need to be sent to the vault. The vault is the object storage where all the files are being stored. So, in multi node, we have proxy in one system and vaults in other systems. So, in total, we have three systems for vault storage such as (SV1, SV2, SV3). The Universal Controller controls the proxy and stores the data files in proxy. From there, we are sending the files to different vaults. Referring to the UC component from figure 2, which is the main component of overlay network. UC takes care of Rx status (Receiver status of each Data Transport Security Controller node is up or down), Binary Modification, Process surge (Increase in number of processes). Binary Modification means, any system can be tampered, and any binary can be replaced by a malicious adversary. UC component interacts with Safe Vault through proxy system.

Considering the experimental set up given in Fig 6, Node 1 is the server (UC), which sends the object files to proxy system. In turn, the files will be retrieved by the vaults. In proxy, we need to configure server ip and customer id. Then in vault mention the vault id, customer id and proxy system ip address. Then start the service of ddserver in proxy system and ddclient in vault systems.

```
vim /ath/data/proxy/config/config.xml
```

and

```
vim /ath/data/cloudapi/config/cong.xml
```

```
cloudpushpvt <file_name> <customer-id> <vaulted>
```

where the filename is the name of the file that wants to be sent, customer ID is given while installing, here we have considered as 1. Vault id is given as the ip address of the vaults, which is mentioned in the experimental framework fig 6. After successful execution of cloudpushpvt (pvt-means private), files will be sent to proxy (as temporary storage) then it will be pulled to vault. Similarly, reverse process is carried out to pull the data from vaults.

Safe Vault provides further cyber-attack protection, if one vault failed or is compromised, data can be retrieved from other vault nodes with no data loss.

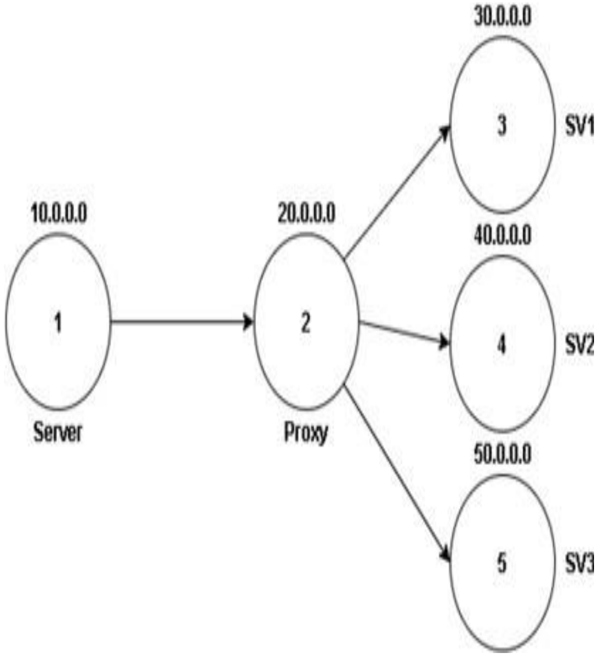


Fig. 6 Experimental Framework

6. COMPARATIVE ANALYSIS

The comparative study of Data Transport Security Tunnels with VPN (Virtual Path Network), MPLS (Multiprotocol Label Switching) and SD-WAN (Software-defined Wide Area Network) is shown in Table 1

The comparative study table shows how research gaps about security and various attacks such as Wiretapping and Ransomware attack can be addressed by data security tunnels, it can be provided as a SAAS product for the customer. The customer can register and login to send the data securely by using this SAAS product to their family and friends.

Table. 1 Comparative Study Table

Parameters	VPN	MPLS	SD-WAN	Proposed Data Transport Security Tunnels
Open Connectivity	At the close of VPN tunnel establishment, the system permits networking capabilities to all other applications and services [4]	Multi-protocol Label switching uses the dedicated links, permits only required services to pass on.	Increasing the ability of WAN services to make sure, the networking capabilities are forwarded [11].	Once the data transfer security tunnel established, then networking capabilities are not easily permitted to other services.
Cost	The cost of VPN is relatively low compared other security tunnels	Due to the longer installation of MPLS, it is very costly.	SDWAN is cost effective.	Data Transport Security Tunnels is cost effective.
Wiretapping	Wiretapping is possible	Wiretapping is possible	Wiretapping is possible	Wiretapping is avoided
Ransom Attack	Ransom attack not detected	MPLS does not check whether there is any modification in the data size	The attack not detected at the customer premises	Ransom attack is easily detected and alert message will be sent to customer machine
Improved Operational Efficiency	NO	NO	YES, 50% operational efficiency is improved compared to MPLS.	YES, there is a 60 to 70% improvement in operational efficiency.
Scalable	VPN is not scalable; it is very difficult to manage as more and more sites are added to WAN.	Easily scalable and reliable compared to VPN.	SD-WAN is scalable and grants flexibility	Data transport Security Tunnel can be scalable easily by adding several intermediate nodes to transfer the data securely across the route from sender to receiver.

7. CONCLUSION

Methods for Storage Intrusion Mitigation with Data Transport Security Tunnels, implement the overlay network and to be able to transfer the data through the secure tunnel from sender to receiver. And, how protection of data is provided at rest. Various cyber-attacks are mitigated when data is stored in safe storage, Even if one of the storage vaults is compromised the attacker will not be able to get the complete data as multiple nodes hold the complete data. Similarly, the tunnel is created on an overlay network to transmit the data securely through DTSC nodes controlled by UC and avoids wiretapping and other cyber-attacks. The detailed comparative analysis of Data Transport Security Tunnels with other security tunnels is analysed for various parameters. The dynamic routing is to be incorporated for routing packets through different nodes and maintaining the adaptive nature of accessing any data transport security controller node in case of failure of node and occurring of cyber-attack is to be considered as a future enhancement of present work.

Compared with VPN, MPLS and SD-WAN, Data Intrusion, mitigation, and data security tunnel provide security of data when it is in motion. It is easily scalable and does not require many settings.

The proposed work of Methods of storage intrusion mitigation with data security tunnel secures the data against Ransomware and Wiretapping attacks and transfer the data securely through tunnel by dividing the data into various fragments. This is a unique capability, which is not present in previous works.

ACKNOWLEDGMENT

I would like to express my sincere gratitude to Mr. Peter Chacko, Founder of Neridio Systems Pvt Ltd, Bangalore, for offering me the internship and for his invaluable support and guidance throughout my work.

REFERENCES

1. V. Sidorov and W. K. Ng, (2015) Transparent Data Encryption for Data-in-Use and Data-at-Rest in a Cloud-Based Database-as-a-Service Solution, IEEE World Congress on Services, 221-228 doi: 10.1109/SERVICES.2015.40.
2. K. Singh, S. G. Samaddar and A. K. Misra. (2012). Enhancing VPN security through security policy management. 1st International Conference on Recent Advances in Information Technology (RAIT) 137-142, doi: 10.1109/RAIT.2012.6194494.
3. K. Thakur, M. Qiu, K. Gai and M. L. Ali. (2015) An Investigation on Cyber Security Threats and Security Models. IEEE 2nd International Conference on Cyber Security and Cloud Computing, 307-311, doi: 10.1109/CSCloud.2015.71.
4. C. Burkert, J. A. McDougall, H. Federrath and M. Fischer. (2021) Analyzing Leakage during VPN Establishment in Public Wi-Fi Networks, ICC IEEE International Conference on Communications. 1-6, doi: 10.1109/ICC42927.2021.9500375.
5. Y. Khramov, N. S. Ivanov, E. F. Smirnov, I. V. Latypov and A. V. Gumirov. (2021) Automation of VPN Tunnel Deployment between Trusted Users. IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (ElConRus) 449-453. doi: 10.1109/ElConRus51938.2021.9396669
6. J. E. Cruz de la Cruz, C. A. Romero Goyzueta and C. D. Cahuana (2020) Open VProxy: Low-Cost Squid Proxy Based Teleworking Environment with OpenVPN Encrypted Tunnels to Provide Confidentiality, Integrity and Availability IEEE Engineering International Research Conference (EIRCON) 1-4. doi: 10.1109/EIRCON51178.2020.9253767.
7. K. Kapusta, H. Qiu and G. Memmi (2019) Reinforcing Protection Against Chosen-Plaintext Attack Using Ciphertext Fragmentation in Multi-cloud Environments. 6th IEEE International Conference on Cyber Security and Cloud Computing (CSCloud)/ 5th IEEE International Conference on Edge Computing and Scalable Cloud (EdgeCom) 7-9, doi: 10.1109/CSCloud/EdgeCom.2019.00011.
8. L. Zhang, Y. Cui and Y. Mu (2020) Improving Security and Privacy Attribute-Based Data Sharing in Cloud Computing, in IEEE Systems Journal, vol. 14, no. 1 387-397 doi: 10.1109/JSYST.2019.2911391.
9. Onwubiko and A. Onwubiko (2019) Cyber KPI for Return on Security Investment. International Conference on Cyber Situational Awareness,

Data Analytics and Assessment (Cyber SA) 1-8, doi: 10.1109/CyberSA.2019.8899375.

10. Z. Guan, G. Gou, Y. Guan and B. Wang (2019) An Empirical Analysis of Plugin-Based Tor Traffic over SSH Tunnel. MILCOM IEEE Military Communications Conference (MILCOM). 616-621, doi: 10.1109/MILCOM47813.2019.9020938.

11. S. Troia, F. Sapienza, L. Varé and G. Maier (2021). On Deep Reinforcement Learning for Traffic Engineering in SD-WAN. in IEEE Journal on Selected Areas in Communications, vol. 39, no. 7 2198-2212, July 2021, doi: 10.1109/JSAC.2020.3041385.

12. M. Lescisin and Q. H. Mahmoud (2021) SocialSDN: Design and Implementation of a Secure Internet Protocol Tunnel Between Social Connections. IEEE International Systems Conference (SysCon). 1-8, doi: 10.1109/SysCon48628.2021.9447117.

13. T. Eltaeib and N. Islam (2021) Taxonomy of Challenges in Cloud Security. 8th IEEE International Conference on Cyber Security and Cloud Computing (CSCloud)/ 7th IEEE International Conference on Edge Computing and Scalable Cloud (EdgeCom). 42-46, doi: 10.1109/CSCloud- EdgeCom52276.2021.00018

14. X. Wang, I. Herwono, F. D. Cerbo, P. Kearney and M. Shackleton, (2018) Enabling Cyber Security Data Sharing for Large-scale Enterprises Using Managed Security Services. IEEE Conference on Communications and Network Security (CNS) 1-7, doi: 10.1109/CNS.2018.8433212.

15. Z. Yu-Tong (2017) Research of Computer Network Data Transmission Routing Method *International Conference on Smart City and Systems Engineering (ICSCSE).* 167-171, doi: 10.1109/ICSCSE.2017.49

16. Gubbi J, Buyya R, Marusic S, (2012) Internet of things (IoT). A Vision, Architectural Elements, and Future Directions[J]. Future Generation Computer Systems. 29(7):1645-1660.

17. Miorandi D, Sicari S, Pellegrini F D (2012) Internet of things: Vision, applications and research challenges[J]. Ad Hoc Networks. 10(7):1497-1516.

18. Petros Wallden, Elham Kashefi (2019) Cyber Security in the Quantum Era Communications of the ACM. Vol. 62 No. 4, Page 120 10.1145/3241037

19. S. Kamble and B. R. Chandavarkar (2019) A Survey on Wired, Wireless, and Internet of Things Routing Protocols *10th International Conference on Computing, Communication and Networking Technologies (ICCCNT)* 1-7, doi: 10.1109/ICCCNT45670.2019.8944834.

20. Deep Medhi and Karthik Ramasamy (2018). Chapter 5 IP routing and distance vector protocol family. In Deep Medhi and Karthik Ramasamy, editors, Network Routing (Second Edition), The Morgan Kaufmann Series in Networking, pages 160 – 182. Morgan Kaufmann, Boston, second edition.

21. Coonjah, P. C. Catherine and K. M. S. Soyjaudah (2015). Performance evaluation and analysis of layer 3 tunnelling between OpenSSH and OpenVPN in a wide area network environment. International Conference on Computing, Communication and Security (ICCCS). 1-4, doi: 10.1109/CCCS.2015.7374130.

22. Hamsha K., Nagaraja G.S. (2019) Threshold Cryptography Based Light Weight Key Management Technique for Hierarchical WSNs. In: Kumar N., Venkatesha Prasad R. (eds) Ubiquitous Communications and Network Computing. UBICNET. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, vol 276. Springer, Cham. https://doi.org/10.1007/978-3-030-20615-4_1

23. G. S. Nagaraja, A. B. Soppimath, T. Soumya and A. Abhinith (2019), IoT Based Smart Agriculture Management System. 4th International Conference on Computational Systems and Information Technology for Sustainable Solution (CSITSS). 1-5, doi: 10.1109/CSITSS47250.2019.9031025.

24. Kalyur S., Nagaraja G.S. (2019) A Taxonomy of Methods and Models Used in Program Transformation and Parallelization. In: Kumar N., Venkatesha Prasad R. (eds) Ubiquitous Communications and Network Computing. UBICNET. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, vol 276. Springer, Cham. https://doi.org/10.1007/978-3-030-20615-4_18

25. Sowmyarani C. N. & Veena Gadad & Dayananda P(2021). (p+, α, t)-Anonymity Technique Against Privacy Attacks. International Journal of Information Security and Privacy (IJISP), IGI Global, vol. 15(2), pages 68- 86, April.

26. Sandhya, S., and N. K. Cauvery (2019). Dynamic Load Balancing Based on Genetic Algorithm. International Journal of Innovative Technology and Exploring Engineering 8.11 (2019): 176-179.

27. L. Barukang (2010).Reed-Solomon codes for uncompressed IP header protection. *International Conference on Computer Applications and Industrial Electronics*. 29-33, doi: 10.1109/ICCAIE.2010.5735041

AUTHORS:

Shankaramma received her BE degree in computer science and engineering from BEC, Bellary, Karnataka, India. And an MTech degree in Computer Network Engineering from RV Engineering College, Bangalore, India. She is currently pursuing PhD at the Department of Computer Science and Engineering, RV College of Engineering, Bangalore. Her area of interest includes cyber security, computer networking, and cloud computing.

E-mail: shankaramma.scn20@rvce.edu.in

Dr. Nagaraj G S is working as a professor and Associate Dean at the Department of Computer Science and Engineering, Rashtriya Vidyalaya College of Engineering, Bengaluru, Karnataka.

E-mail: nagarajags@rvce.edu.in

Mr. Peter Chacko has a bachelor's in physics from Mahatma Gandhi University and Masters in Computer Science from the University of Madras. He is the Founder, CEO of Neridio Systems Ltd and has 25+ Years of experience in Networking, Storage and Security. He owns multiple US Patents including US12206686 and US 1218 4667 related to his pioneering inventions on storage intrusion mitigation tunnelling.

Email: peter@neridio.com