

Deduplication Process in Attribute based system using cloud

Jimish Jain¹, Parth Pengoriya², Sachin Kumar³

¹⁻³ Department of Computer Engineering, NBSSOE, Ambegaon, Pune, Maharashtra, India

Abstract:- We deliver an attribute-based storage architecture with secure deduplication in a hybrid cloud environment, where private cloud management is done on the private cloud, but public cloud storage manages duplicates. Instead of referencing previous data dedupl, our methodology is more flexible and more generalised, which have some shortcomings. as an alternative to key management and to exchange encryption keys, it can be used to grant access control to data to approved users. Additionally, it falls in line with the industry-wide standards for semantic data protection but fails to achieve these levels of security by merely adhering toin the less rigorous definition. There are three steps to successfully handling the problem of ciphertext with a different access policies: first, one must handle the conversion of ciphertext that contain the same plaintext, and ciphertext using the same process; then, one must handle ciphertext with access policies that are different from the original.

Index Terms—ABE, Storage, Deduplication.

I. INTRODUCTION

AWSets or non-based (nattributed) data encryption is most often seen in cloud computing, where a data centre transfers encrypted data to a cloud service and which then disseminates it to users according to non-distributed keys (or attributes). There is a need for safer duplicate deduplacement in order to free up disc space to prevent duplicating records, whilst there is also a need for storage space expansion Although the simple ABE has proven to be effective for stability expansion, it is not supportive of deduplication.

Anyone who chooses to store data in the cloud is OK, as long as they are not share their cloud with third parties or limiting it to only people with specific permissions is done with consent. and data security of encrypted formats, since data encryption often demands mechanisms to be employed to ensure that only particular individuals have access to the data, as well as avoiding it from being made readable by someone other than its intended users (or credentials). It should also use a private key with an attribute set that can be used for control (unconditional attribute), which contains a record permissions that should be applied to the data expansion of the user in question and then encrypted data in order to fulfil this demand.

In the case of the ciphertext having the same access characteristics as the user's, then the user may obtain the decryption key using his or her own private key. the

"Stable Deduplication" method, on the other hand, is an approach to lower the storage capacity and network latency by replacing duplicate encrypted data copies. Traditionally, On the other hand, the older ABE type fails to have enough. Deduplication systems that employ attribute encryption are also use RSA keys and thus we don't know about them at this time. Many computing platforms, such as cloud platforms, would benefit from robust deduplication in ABE; a cloud storage infrastructure, which requires it, is ideal for these situations.

II. LITERATURE SURVEY

Conditional proxy re-encryption (CPRE) is a real-world implementation that allows for fine-grained delegation of decryption rights. This paper presents the ciphertext-policy-attribute-based CPRE scheme, as well as a formalisation of the primitive and a security overview. The utility of the scheme is demonstrated in a cloud implementation that allows for fine-grained data.[1].

Digital forensic examiners now face a new challenge from cloud computing. Platforms that can store vast quantities of data are increasingly becoming more common among consumers, businesses, and policymakers. Due to virtualization and a lack of information about the location, extracting digital evidence from cloud storage platforms (particularly from offshore providers) may be difficult in a digital forensic investigation.[2].

Present fuzzy identity-based encryption can be applied to information that contains personal or sensitive data in transit (FIBE). In Fuzzy IBE, identities, the question of how to accurately describe the context of a fuzzy concepts is addressed is solved by adding explicit information. Fuzzy IBEs need a private key for an integer (0), but only if the identities are also integers (in their "set") is required the output "obscularity" satisfies a relation of overlap between input and output."[3].

invested in new CAPEX and OET (with newer technologies, or with new and evolving technologies, no one needs to waste money on OPEX (operational) or CAPEX (operational expenditures). Tools are necessary, or unnecessary, the ability to work with what is already on hand or getting something that's not really needed are required. The following has been created as an SDN for this purpose, to provide the needed resources using SDN.[4].

Perhaps one of the greatest technological developments of the 20th century was the Internet, which linked computers

all over the world to one another through automated networks. 4. 58% of the population is actually on the internet. the number of users on the network has to move between their devices will drive the size of the network exponentially, especially as the amount of traffic in and the system network connections both increase[5][6].

Software-defined networking was used to offer network mobility for the common network, while blockchain provided network security. Blockchain technology is particularly common, and enables information to be shared without having to be duplicated over a peer-to-peer network. problems such as confidentiality and unrestricted/expanded attack surface-area networking must be considered when building SDN security[7][8][9].

To convey the usefulness of literature is to the reader of new information and insight into recent events, and help him/her anticipate potential progress The paper deals with the emerging Software Defined Network Functions and Neural Networks, and then introduces some of the present-day Software Defined Network Functions, which is a more modern solution known as Virtual Network Virtual Network Nurturing Networks.[10]

Any of the machine learning strategies for intrusion detection device development we have discussed above have used so far have been developed to aid Software Defined Network area. In this survey, we discovered a wide range of assets that help us develop a sound detection system model for the Network Intrusion Detection System.[11].

. In light of the 5G-enabled microprocessors for sale by 5G technology suppliers and the leasing of necessary spectrums by governments, the fifth generation (5G) would quickly arrive. A highly interactive section will include the deployment of a lot of real-time response and attack systems. When data becomes more volatile and the way we handle it becomes critical, there is a need for new approaches in localised internet warfare and cyber security incidents.[12]

. Router is a multiple network network architecture allowing a device to select, regardless of its legitimacy, the best route from the source to any location. The domain separation will, however, entail new network requirements, which would require inter-domain routing to maintain the existing bandwidth available in future.[13].

Cloud computing is a fast emerging processing model that enables customers to store their data on a computer centrally and deliver services on demand. The safety and protection of information has become a fundamental

problem for distributed information storage when sensitive corporate information on a cloud server is shared more and more. In order to obtain access to the control system, the secured client preserves information.[14].

This paper discusses about security issues in 5G cell phones and network [15].

This paper discusses about virtualisation and SDN.[16]
In this paper it is discussed about SDN And DDOS[17]
This paper is regarding the applications of BLOCKCHAIN in SDN[18].The paper discuss about SDN for 5G era[19].This paper is regarding the detection of intrusion using machine learning framework[20].This paper discuss about the application of Artificial Intelligence in the 5G era.[21]
This paper discusses about the interoperability using SDN and NFV[22].The paper lines out the machine learning approach to tackle or detect intrusion[23].This paper is regarding the challenges to intelligence using AI & ML.[24].This paper is regarding the comparative analysis of DDos Mitigation[25].This paper is regarding the application of ML and AI.[26].This paper is regarding the selection of safe path and routing in OBGp and OBGp+[27].These paper are regarding the SDN in big data and cloud computing[28][29].

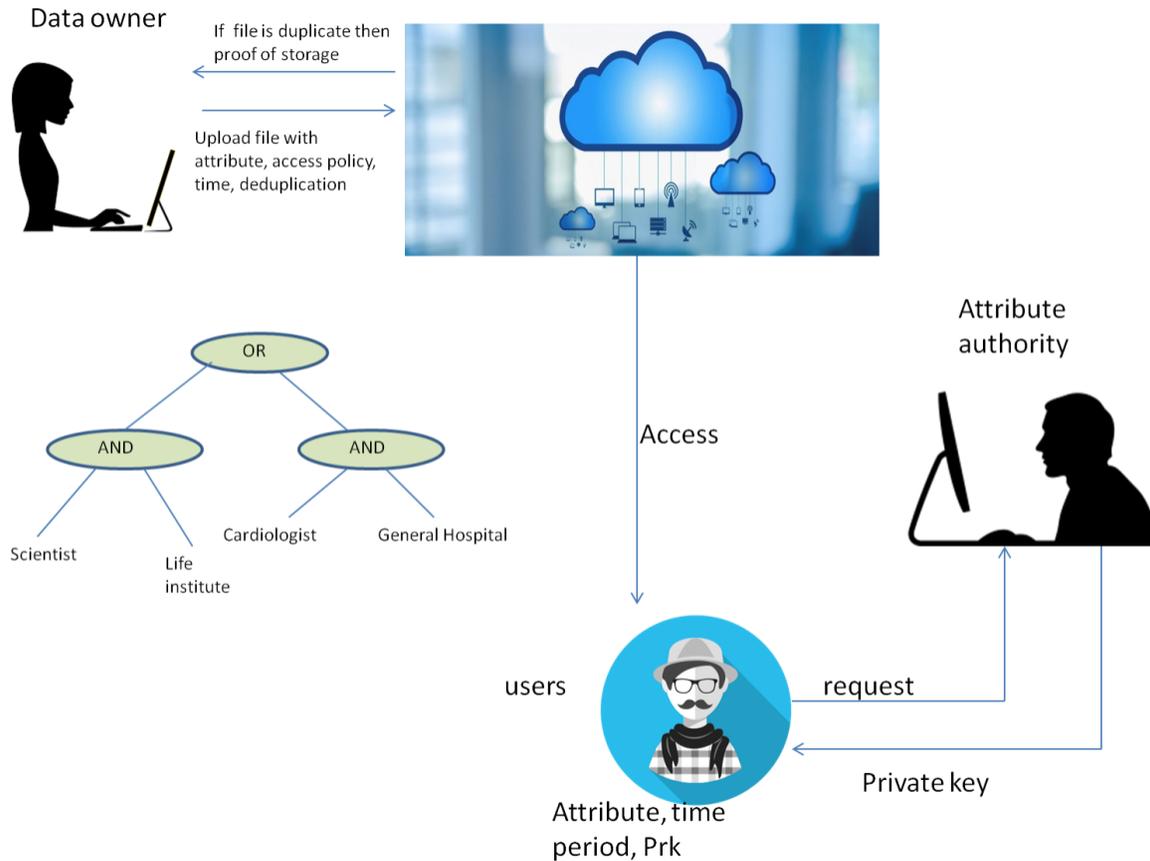
PROPOSED SYSTEM

In contrast to dictionary storage deduplication, an attribute-based storage scheme may accomplish deduplication. The cloud of publicly-accessible part of a company's infrastructure is controlled by a public cloud providers, while the company's privately-internal part is exclusively owned and managed by the company (or attributes). Another acronym for this approach is named for shortening, on the other hand, EADM, but it uses deduplication and can reduce the amount of disc space and bandwidth use, thus saving copies. Expanding a data storage processing such as tag checking in a hybrid cloud is a challenge in a simplified form. Our database is based on a hybrid cloud model, where the data is stored in a private cloud and retrieval is handled by a public cloud. If a trapdoor key is used for another ciphertext, the private cloud can always pass it even if it does not understand the plaintext, because the operation is different under both policies.

A) PROBLEM DEFINATION

Once data has been secured in a data centre, a stable deduplication cloud structure receives the data, then examines it to find any duplicates before passing it to a public cloud for storage.

B) SYSTEM ARCHITECTURE



III. CONCLUSION

Application-based password recovery, also known as attribute-based encryption (ABE), has become popular because of cloud storage. This permits services to transfer protected data to the cloud, where users have specific credentials, which enables the users to receive copies of their encrypted data with new attribute-generated keys in case their passwords become compromised. While redundant file storage capacity elimination is useful for disc space and network capacity savings, it has the potential to result in duplicate entries that can be safely deleted with the Expand feature.

IV. REFERENCES

[1] D. Kreutz, F. M. Ramos, P. E. Verissimo, C. E. Rothenberg, S. Azodolmolky, and S. Uhlig, "Software-defined networking: A comprehensive survey," *Proceedings of the IEEE*, vol. 103, no. 1, pp. 14–76, Jan. 2015.

[2] S. Lal, et al., "NFV: Security Threats and Best Practices", *IEEE Communications Magazine*, 55(8), 2017, pp. 211–217.

[3] V. Deepa, K. M. Sudar and P. Deepalakshmi, "Detection of DDoS Attack on SDN Control plane using Hybrid Machine Learning Techniques," 2018 International Conference on Smart Systems and Inventive Technology (ICSSIT), Tirunelveli, India, 2018, pp. 299-303.

[4] C. Buragohain and N. Medhi, "FlowTrApp: An SDN based architecture for DDoS attack detection and mitigation in data centers," 2016 3rd International Conference on Signal Processing and Integrated Networks (SPIN), Noida, 2016, pp. 519-524.

[5] Anteneh A. Gebremariam, Muhammad Usman, Marwa Qaraq, Applications of Artificial Intelligence and Machine Learning in the Area of SDN and NFV: A Survey, 2019 16th International Multi-Conference on Systems, Signals & Devices (SSD'19)

[6] L. Zhu, X. Tang, M. Shen, X. Du, and M. Guizani, "Privacypreserving DDoS attack detection using cross-domain traffic in Software Defined Networks," *IEEE J. Sel. Area Comm.*, vol.36, no.3, pp. 628-643, 2018

- [7] YuhuaXu, Zhe Sun, Zhixin Sun, "SDN- Based Architecture for Big Data Network ",International Conference on Cyber- Enabled Distributed Computing and Knowledge Discovery,2017.
- [8]https://www.researchgate.net/publication/335108911_Utilizing_Blockchain_to_Overcome_Cyber_Security_Concerns_in_the_Internet_of_Things_A_Review
- [9] A. Rahman *et al.*, "DistB-Condo: Distributed Blockchain-Based IoT-SDN Model for Smart Condominium," in *IEEE Access*, vol. 8, pp. 209594-209609, 2020, doi: 10.1109/ACCESS.2020.3039113.
- [10] Pei, Jianing & Hong, Peilin & Li, Defang. (2018). Virtual Network Function Selection and Chaining Based on Deep Learning in SDN and NFV-Enabled Networks. 1-6. 10.1109/ICCW.2018.8403657.
- [11] A. Yazdinejad, R. M. Parizi, A. Dehghantanha, Q. Zhang and K. R. Choo, "An Energy-efficient SDN Controller Architecture for IoT Networks with Blockchain-based Security," in *IEEE Transactions on Services Computing*.
- [12] Guan Z., Lyu H., Zheng H., Li D., Liu J. (2019) Distributed Audit System of SDN Controller Based on Blockchain. In: Qiu M. (eds) Smart Blockchain. SmartBlock 2019. Lecture Notes in Computer Science, vol 11911. Springer, Cham
- [13]. Anteneh Beshir, Marcelo Yannuzzi, Fernando Kuipers, "Inter-domain Routing in Optical Networks with Wavelength Converters", IEEE Communications Society, 2010
- [14]. Keke Gai, Meikang Qiu, Lixin Tao and Yongxin Zhu, "Intrusion detection techniques for mobile cloud computing in heterogeneous 5G", John Wiley & Sons, Ltd., SECURITY AND COMMUNICATION NETWORKS research article.
- [15] Shailesh P Bendale, Jayashree R Prasad , " Security Threats and Challenges in Future Mobile Wireless Networks", - 2018 IEEE Global Conference on Wireless Computing Network(GCWCN), 2018.
- [16] A S Patil, P S Jain, R G Ram, V N Vayachal, S P Bendale," Detection of Distributed Denial-of-Service (DDoS) Attack on Software Defined Network (SDN)",- IRJET 2018
- [17] A S Patil, P S Jain, R G Ram, V N Vayachal, S P Bendale,"Software Defined Network: DDoS Attack Detection", — IRJET 2019
- [18] Praneeta Dumbre, Shailesh P. Bendale, "Application of Blockchain in Software Defined Network", International Journal of Future Generation Communication and Networking, Vol. 13, No. 3s, (2020), pp. 1587–1593 <http://www.sersc.org/journals/index.php/IJFGCN/article/view/29394/16354>
- [19] Ruchira Borkar, Shailesh Bendale, Software Defined Network (SDN) for 5G era an emerging Mega-trend, International Journal of Future Generation Communication and Networking Vol. 13, No. 3s, (2020), pp. 1579–1586 <http://www.sersc.org/journals/index.php/IJFGCN/article/view/29393>
- [20] Tiwari, S., Pandita, V., Sharma, S., Dhande, V. and Bendale, S., 2019. SURVEY ON SDN BASED NETWORK INTRUSION DETECTION SYSTEM USING MACHINE LEARNING FRAMEWORK.
- [21] S. Shah and S. Pramod Bendale, "An Intuitive Study: Intrusion Detection Systems and Anomalies, How AI can be used as a tool to enable the majority, in 5G era," 2019 5th International Conference On Computing, Communication, Control And Automation (ICCUBEA), Pune, India, 2019, pp. 1-8, doi: 10.1109/ICCUBEA47591.2019.9128786.
- [22] Prasad J.R., Bendale S.P., Prasad R.S. (2021) Semantic Internet of Things (IoT) Interoperability Using Software Defined Network (SDN) and Network Function Virtualization (NFV). In: Pandey R., Paprzycki M., Srivastava N., Bhalla S., Wasielewska-Michniewska K. (eds) Semantic IoT: Theory and Applications. Studies in Computational Intelligence, vol 941. Springer, Cham. https://doi.org/10.1007/978-3-030-64619-6_18
- [23] Shivam Tiwari, Vanshika Pandita, Samarth Sharma, Vishal Dhande, Shailesh Bendale AN INITIATIVE WORK ON SDN BASED NETWORK INTRUSION DETECTION SYSTEM USING MACHINE LEARNING., Volume 7, Issue 04, Pages 1229-1233 <https://www.irjet.net/archives/V7/i4/IRJET-V7I4229.pdf>
- [24] Shailesh Pramod Bendale, Jayashree Rajesh Prasad. (2020). Security Challenges to provide Intelligence in SDN with the help of Machine Learning or Deep Learning. International Journal of Advanced Science and Technology, 29(05), 356 - 363. Retrieved from

<http://sersc.org/journals/index.php/IJAST/article/view/8983>

[25] Chinmay Dharmadhikari, Salil Kulkarni, Swarali Temkar, Shailesh Bendale , Comparative Analysis of DDoS Mitigation Algorithms in SDN, International Journal of Future Generation Communication and Networking Vol. 13, No.2s, (2020), pp. 1700-1707
<http://www.sersc.org/journals/index.php/IJFGCN/article/view/29228/16286>

[26] Mr. Shailesh P. Bendale, M. A. R. S. (2020). Implications and Application of Artificial Intelligence and Machine Learning Concepts on Software Defined Network and Its Future Prospects. International Journal of Advanced Science and Technology, 29(4s), 1142 - 1152. Retrieved from <http://sersc.org/journals/index.php/IJAST/article/view/6666>

[27] S. P. Bendale and G. V. Chowdhary, "Stable path selection and safe backup routing for Optical Border Gateway Protocol (OBGP) and Extended Optical Border Gateway Protocol (OBGP+)," 2012 International Conference on Communication, Information & Computing Technology (ICCICT), Mumbai, India, 2012, pp. 1-6, doi: 10.1109/ICCICT.2012.6398201.

[28] Tejeshwari Chouhan , Shailesh Pramod Bendale , Software Defined Network systems embedded with big data, international Journal of Future Generation Communication and Networking Vol. 13, No.2s, (2020), pp. 1591-1596
<http://www.sersc.org/journals/index.php/IJFGCN/article/view/29210/16269>

[29] Kshitij Chaudhari, Prof. Shailesh P. Bendale, An Initiative Study on Software Defined Cloud Computing, International Journal of Future Generation Communication and Networking Vol. 13, No.2s, (2020), pp. 1727-1732
<https://sersc.org/journals/index.php/IJFGCN/article/view/29233>