International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 10, Issue 2, No 6, 2022. ISSN: 2348-6600
Reference ID: IJCS-449 PAGE NO: 3036-3043

A Dynamic Key Generation Scheme to Implement CP-ABE Standard Over Large Cloud Data

Vysyaraju Ashritha[#1], Uppalapati Siva Sai Pavan Karthik[*2],

Bohini Nagendra Varma[#3], Annam Reddy Dinesh Chowdary[#4]

[#1,2,3,4] *Department of Computer Science and Engineering (CSE),*
GITAM Deemed to be University,
Visakhapatnam, Andhra Pradesh, India.
[1] 121910301020@gitam.in, [2] *121910301040@gitam.in,*
[3] 121910301063@gitam.in, [4] 121910301011@gitam.in.

ABSTRACT:

Recently, the Usage of the cloud is getting bigger in range for storage of private or public data. So, there is a need for secure and integrated delivery or access to the data on the cloud. By using advanced cryptographic techniques to store data securely in an untrusted cloud platform has drawn more wide range of attention, in particular CP-ABE, QH-CPABE are promising. Here we use a Dynamic Generator of Key [DGK] function for the encryption in an advanced version of CP-ABE with QH-CPABE for users private or public data in a more secure manner. 20th century ABE models are insecure and possible of unauthorized access. Moreover, as the size of the input data grows, traditional ABE models cannot compute efficient private keys due to computation time and network overhead. To overcome these problems, a new ABE model for chaotic integrity and attribute-based key distribution and ciphertext policies is implemented for cloud data. Experimental results show that the proposed model has higher computational speed, higher memory overhead, and higher security compared to the old CP-ABE model.

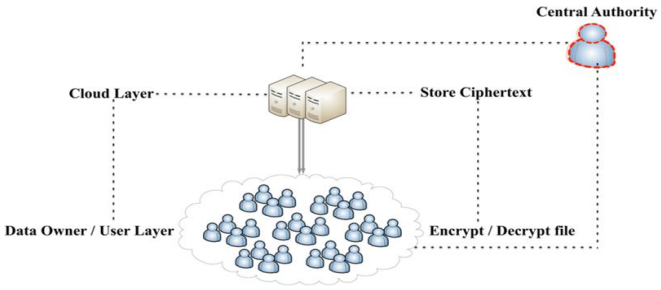


Fig1: The basic CP-ABE scheme over the cloud storage platform

I. INTRODUCTION

Cloud Computing platform offers many facilities, some of them are Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS), providing various adaptability for cloud consumers. The exponential growth for the decentralized retribution and WWW communication structures, there is a substantial need for cloud consumers′ private and confidential data management and distribution privileges provided via cloud - based platform. The third - party service - based members must use a trustworthy and persistent control supervision approach to improve the

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 10, Issue 2, No 6, 2022. ISSN: 2348-6600
Reference ID: IJCS-449 PAGE NO: 3036-3043

privacy and security aspects for cloud consumers. In Particularly, such scenarios as the big data of cloud consumers stored over the cloud - based platforms, then it leads user sensitive data such as consumers' pecuniary info, and public media info to be widely exposed over communication and simply re-installed data by 3rd party people and attackers via some malicious third - party applications. Cipher Text Policy-Attribute Based Encipherment (CP-ABE) and Attribute-based Encryption (ABE) algorithms are designed to protect consumer privacy by hiding sensitive consumer data or portions of sensitive data. Designed to Extensions to traditional encrypted IBE and ABE approaches include consumer ciphertext lookup approaches. Therefore, previous techniques are used in security maintenance applications in various domains such as banking, healthcare, respiratory, biomedical, and government storage data to achieve the same standards of integrity, privacy, security, and authorship. I can do it. It can be achieved. Computation, storage, and Internet transmission costs. Most of the modifiable CP-ABE techniques are unable to meet the diversified multi-domain media security and storage demands that are emerging. To solve the above problems, HQCP-ABE (Hybrid Quantum-based CP-ABE) technology was developed, which can securely distribute and process big data via cloud and communication.

- consumers documents are encrypted in to CP by the help of attribute encrypted methodologies.
- The policy of key here is built on the basis of tree structure and the media data are encrypted via different keys generated by the function by using cloud consumers private information.

Older methods allow access to personal data that can be indirectly observed over and over again by intruders and illegal attackers. Unauthorized persons and hackers foresee complete end-to-end access to information such as details, data and identity addresses. Except for communication through first-order quantum systems, we cannot predict the level of information in accessing data.

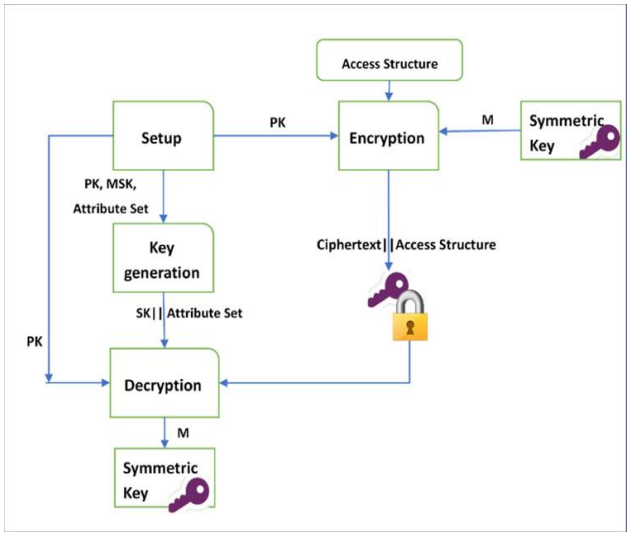


Fig2: information in accessing data.

II. RELATED WORK

Singamaneni, Kranthi Kumar, et al. [1], The authors primary goal is to increase the tendency of optimal computation overhead for key generation, encipherment, we overcome existing problems by Proposal of New Dynamic Quantum Key Distribution (QKD) Algorithm for Critical Public Infrastructure, but with 8# stages and polarization in an arbitrary way.

[2] affects the security of cloud information and hinders improvements in distributed computer management. This article proposes his own SDVC (Secure Information Erase and Confirmation) diagram from the CP-ABE perspective to achieve fine-grained secure information erasure and erasure verification of cloud information. Considering CP-ABE's access strategy, it builds a feature membership tree, performs high-quality rejection and fast re-encryption of keys, and provides fine-grained control over secure key erasure. In addition, we build standard interpretation computations

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 10, Issue 2, No 6, 2022. ISSN: 2348-6600
Reference ID: IJCS-449 PAGE NO: 3036-3043

for generating irregular blocks of information, integrate override innovations with Merkle hash trees to perform secure cryptographic deletion, and confirm the results of information deletion. Create a validator that will be used for Demonstrating the safety of the SDVC conspiracy according to the standard model, through hypothesis research and reasonable replication findings he confirms the accuracy and validity of the SDVC conspiracy. [3] Here, the authors use the input as large amounts of structured and unstructured cloud data to inspire practical results, demonstrating 92% accuracy in bit hash modification and dynamic key generation, encryption, and decryption. We validated the proposal with about 96% accuracy in the optimization time, but it makes the key generation random and predictable. [4] In this work. We propose an improved dynamic nonlinear polynomial integrity-based quantum hash code strategy using quality-based key age. Our technique involves a collection of non-straight, turbulent bends accompanied by intertwined randomized abilities. A regular function-based encryption strategy designed to manage vast amounts of sensitive customer data using a proprietary key generation system. [5] Quality-Based Encryption (ABE) is a popular innovation used to control information stored on cloud servers. Anyway, in general, an authorized decryption client may not be able to decrypt the ciphertext in time for unknown reasons. For security reasons, instead of one client, multiple proxy clients are provided to coordinate the decryption of the ciphertext. This article provides his ABE plot of a shared decryption ciphertext strategy. Authorized clients are free to restore messages. At the same time, these other clients (semi-authorized clients) can collaborate and receive messages. We are also working on a master plan for semi-regular customers to get serious about their decryption efforts. Work on plan competencies using the built-in approval tree. The new tariff is CPA-safe on the standard model. Exploratory results show that our scheme performs very well in terms of both the above computational and capacity costs.,[6] The tremendous growth of cloud information and additional storage space has made cloud security one of the more attractive research areas for distributed computer servers. Signature cryptography is a public-key cryptographic computation that allows cloud clients to retrieve sensitive data on public cloud servers. Quantum Key Distribution (QKD) is said to work for the security of communication frameworks. Quantum cryptography programs rely entirely on quantum mechanics. The essential goal of quantum key rotation is to create the keys involved in cryptography. Traditional proprietary encryption models are unstable and vulnerable to man-in-the-center key distribution attacks. Moreover, as the size of the information grew, his regular ABE model could not register a valid enigma key due to the above computation time and configuration. To solve these problems, ABE models are run against clever shape-text strategies based on turbulent erections and quantum key distribution (QKD) in cloud climates. Experimental results showed that the proposed model has high computational speed, higher capacity, and key distribution in contrast to the traditional CP-ABE, KPABE and QKD-ABE models.[7] cipher text-Strategy Property base Encryption (CP-ABE) is viewed as one of the most appropriate advances for information access control in distributed storage. Almost all current CP-ABE schemes are expected to have one expert within the framework responsible for lending to customers. Nevertheless, in many applications, various experts come together in one framework of him, and each authority is free to make loans. This article plans the access control structure of the multi-privilege framework and proposes a productive and secure multi-privilege access control for distributed storage. First, plan a competent multi-authority CP-ABE plan that does not require global authority and can maintain any LSSS

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 10, Issue 2, No 6, 2022. ISSN: 2348-6600
Reference ID: IJCS-449 PAGE NO: 3036-3043

access structure. Then, at this point, we show its certainty with any predictor model. We also propose another way to solve the property denial problem in the multi-agency CP-ABE framework. Research and replication results show that Multi-Authority Access Control Conspire is adaptable and productive. .[8] there is a proposal of an algorithm based on blind quantum computing for secure communication and enhanced the hierarchal attribute-based encryption based on BCQ key sharing for data access but this work is too complex to understand.[9][10][11] These are also mechanisms to secure and privacy aspects on cloud data by using quantum and QCP-ABE framework.[12] Digital image watermarking is a technique used to avoid the increasing piracies in digital images and for the effective duplication, alteration, falsifications to be made by anybody having a PC. the author describes the usage of cloud data storage is more and some have implemented the pay-per-use service [14] It's a chaotic integrity and QKD based cipher policy ABE model on cloud with the results of high computation speed, storage and secured key distribution.[14] in these two works the authors worked on the security and privacy over complex cloud data but over the secure block chain cloud environment [15] Here the authors proposed the Quantum key Allocation to overcome the different security holes however it can't completely eliminate them.

PROPOSED MODEL

The proposed DGK model (Dynamic Generation of key) is the advanced /updated model for present CP-ABE for more secure and private data access. This Model encrypts the data in using the main key and the end users and the decrypts using different private keys.

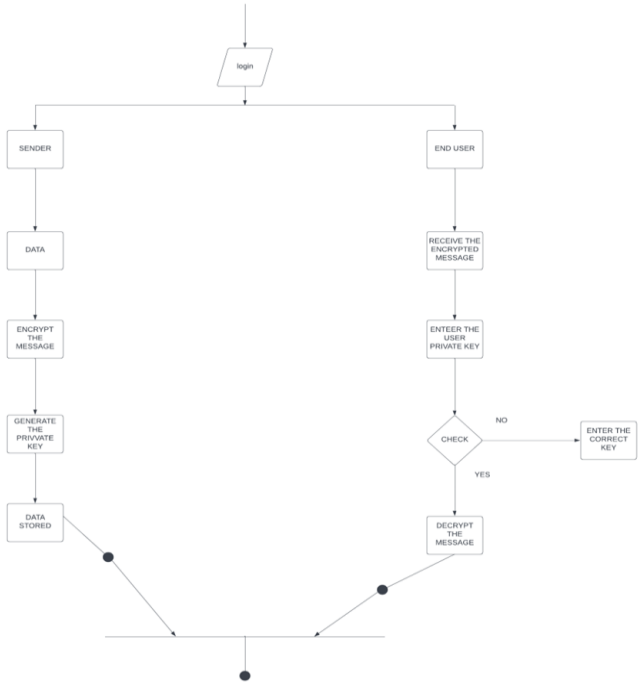


Fig-3 Activity Diagram for our proposed Model.

The attribute-based ciphertext policy encryption scheme consists of four bases.

DGK algorithms: setup, key generation, encryption and decryption.

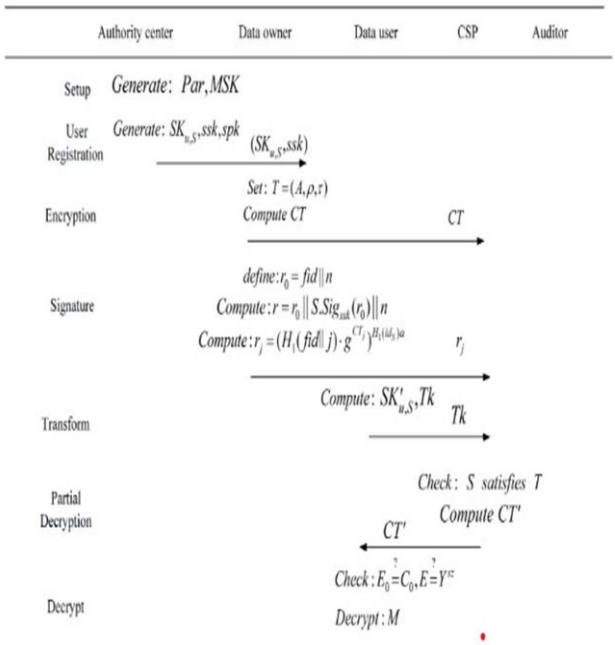
Setup: The setup algorithm requires no input other than implicit security parameters. Prints public parameter PK and master key MK.

Key Generation (MK, S): The key generation algorithm takes as input a master key MK and a set of attributes S that describe the key. He issues a private key SK.

Encryption (PK, A, M): The encryption algorithm takes as input the public parameter PK, the message M, and the access structure A to the universe of attributes. This algorithm encrypts M and produces a ciphertext CT such that only users possessing a set of attributes that satisfy the access structure can decrypt the message.

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 10, Issue 2, No 6, 2022. ISSN: 2348-6600
Reference ID: IJCS-449 PAGE NO: 3036-3043

Decryption (PK, CT, SK): The decryption algorithm takes as input the public parameter PK, the ciphertext CT containing the access policy A, and the private key SK. A set S of attributes. If the attribute set S satisfies the access structure A, the algorithm decrypts the ciphertext and returns the message M.



COMPARISONS AND RESULT

TABLE I
FONT SIZES FOR PAPERS

	Info size (kb)	Hash Period (m/s)	Enciphered Period (m/s)	Deciphered Period (m/s)
CPABE+ MD- 5	≅3200	4657	7760	5937
KPABE+SHA- 256	≅3454	5844	5957	5565
FHABE+SHA- 512	≅3210	6384	7679	7428
MUH- ABE	≅3790	2965	3948	3825
CIH- ABE	≅4600	2353	3017	3635
Hybrid QHCP- ABE	≅6080	1969	2763	2769
DGK CP-ABE	=2800	1606	2500	2743

Table 1: Analysis of different Hash - based Encryption Techniques.

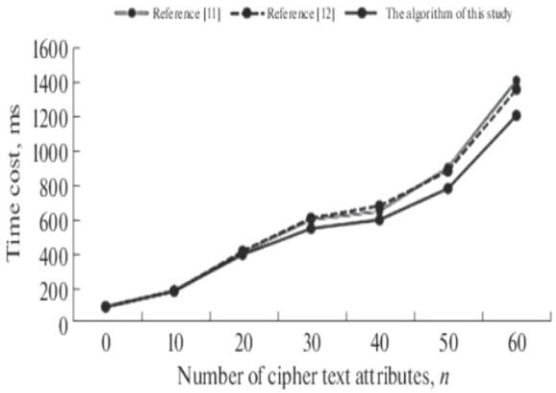
Standard	Info Volume (KB)	Cloud Info Space (KB)
CPABE	5000	5287
KPABE	5000	5142
FHABE	5000	4278
MUHABE	5000	3729
Hybrid QCPABE	5000	2547
DGK CP-ABE	4450	2540

Table 2. Memory occupancy efficacy of proposed standard Vs. conventional ABE standards

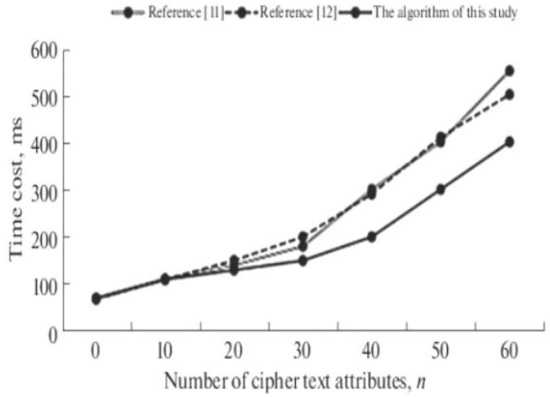
International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 10, Issue 2, No 6, 2022. ISSN: 2348-6600
Reference ID: IJCS-449 PAGE NO: 3036-3043

CPABE (m/s)	KPABE (m/s)	DUPHA (m/s)	FHABE (m/s)	QKD/ CPABE (m/s)	DGK CP-ABE	Proposed Standard (m/s)
845.54	761.66	571.51	629.56	356.55	301.22	294.34
837.35	752.73	622.39	786.37	338.34	310.24	302.13
972.33	884.30	545.47	719.98	329.21	315.5	295.54
859.44	734.54	432.23	727.27	359.29	302.15	275.64
836.59	708.12	411.32	892.09	345.95	321.22	302.34
830.65	700.13	623.12	786.62	329.6	280.23	244.63

Table 3. Relative Findings of Trusted DGK CPABE Planned with Conventional Cryptographic Standards on Execution Time as parameter



[13]. From the comparisons given by the author are compared and the DGK algorithm has less time complexity. This comparison is about Encryption time.



[11,12] This the comparison is all about the time complexity of decryption process for this study and other references.

CONCLUSIONS

In the standard ABE models, several of the models throughout their input user attributes are text-based info and used fixed values for key production, client text encipherment and decryption method to overcome and maintain the current situation, we have a tendency to planned a new trilinear Tinkerbelle chaotic map-centric hash technique applied to reinforce. The cloud client security of the projected DGK – CP-ABE customary. In the planned customary, consumer's attributes are any kind, and people are protected with the help of the trilinear Tinkerbelle chaotic operate for key setup, cloud client text encipherment, and coding procedure. Investigational findings conclude that the projected model is functioning well to realize huge cloud consumers′ sensitive knowledge integrity and privacy with less enciphered, deciphered, and key production time as compared with the conventional ABE models. Our projected model used each structured and unstructured big cloud clinical knowledge as input in order that the simulated experimental results conclude that the proposal has precise, leading to around ninety-

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 10, Issue 2, No 6, 2022. ISSN: 2348-6600
Reference ID: IJCS-449 PAGE NO: 3036-3043

two correctness of bit hash change and around ninety-six correctness of chaotic dynamic key production, enciphered and deciphered time as compared with typical standards from the literature. In the future, posts of this analysis will be published on other domains such as suburban blockchain apps and IOT...

REFERENCES

[1] Singamaneni, Kranthi Kumar, et al. "A Novel QKD Approach to Enhance IIOT Privacy and Computational Knacks." Sensors 22.18 (2022): 6741.

[2] Ma, Jun, et al. "Cp-Abe-based secure and verifiable data deletion in cloud." Security and Communication Networks 2021 (2021).

[3] Singamaneni, Kranthi Kumar, et al. "An Efficient Hybrid QHCP-ABE Model to Improve Cloud Data Integrity and Confidentiality." Electronics 11.21 (2022): 3510.

[4] Kranthi Kumar Singamaneni, Abhinav Juneja, Mohammed Abd-Elnaby, Kamal Gulati, Ketan Kotecha, A. P. Senthil Kumar, "An Enhanced Dynamic Nonlinear Polynomial Integrity-Based QHCP-ABE Framework for Big Data Privacy and Security", Security and Communication Networks, vol. 2022, Article ID 4206000, 13 pages, 2022. https://doi.org/10.1155/2022/4206000

[5] Chen, Ningyu, et al. "Efficient CP-ABE scheme with shared decryption in cloud storage." IEEE Transactions on Computers 71.1 (2020): 175-184.

[6] Singamaneni, Kranthi Kumar, and P. Sanyasi Naidu. "An efficient quantum hash-based CP-ABE framework on cloud storage data." International Journal of Advanced Intelligence Paradigms 22.3-4 (2022): 336-347.

[7] Yang, Kan, and Xiaohua Jia. "Attributed-based access control for multi-authority systems in cloud storage." 2012 IEEE 32nd International Conference on Distributed Computing Systems. IEEE, 2012.

[8] Singamaneni, Kranthi Kumar, and Pasala Sanyasi Naidu. "IBLIND Quantum Computing and HASBE for Secure Cloud Data Storage and Accessing." Rev. d'Intelligence Artif. 33.1 (2019): 33-37.

[9] Singamaneni, Kranthi Kumar, Pasala Sanyasi Naidu, and Pasupuleti Venkata Siva Kumar. "Efficient quantum cryptography technique for key distribution." Journal Europeen des Systemes Automatises 51.4-6 (2018): 283.

[10] Singamaneni, Kranthi, Abdullah Shawan Alotaibi, and Purnendu Shekhar Pandey. "The Performance Analysis and Security Aspects of Manet." ECS Transactions 107.1 (2022): 10945.

[11] Singamaneni, Kranthi Kumar, and Sanyasi Naidu Pasala. "An improved dynamic polynomial integrity based QCP-ABE framework on large cloud data security." International Journal of Knowledge-based and Intelligent Engineering Systems 24.2 (2020): 145-156.

[12] Kumar, Singamaneni Kranthi, et al. "Image transformation technique using steganography methods using LWT technique." Traitement du Signal vol 36 (2019): 233-237.

[13] Xue, Shumin, and Chengjuan Ren. "Security protection of system sharing data with improved CP-ABE encryption algorithm under cloud computing environment." Automatic Control and Computer Sciences 53.4 (2019): 342-350.

[14] Kranthi Kumar, S., Ramana, K., Dhiman, G., Singh, S., & Yoon, B. (2021). A Novel Blockchain and Bi-Linear Polynomial-Based QCP-ABE Framework for Privacy and Security over the Complex Cloud Data. Sensors, 21(21), 7300.

[15] Singamaneni, Kranthi Kumar, and Pasala Naidu. "Secure key management in cloud environment using quantum cryptography." Ingénierie des Systèmes d'Information 23.5 (2018).

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 10, Issue 2, No 6, 2022. ISSN: 2348-6600
Reference ID: IJCS-449 PAGE NO: 3036-3043

[16] https://lucid.app/lucidchart/cb6377b4-252b-4201-87a0-c19a194a4570/edit?view_items=PYv8ZK7KQsXV%2C6Tv8iO06oysA%2ChSv8cpV9mqEa%2ClYv8cb7tM7Xk%2CsZv8fY1OdPrf%2CjZv8sS5WhSbW%2C_Zv8_Y1e1V_x%2C3Zv8RZpBzyH5%2C49v8rulEJ6ag%2CT0v8LJ2y46_F%2CC1v8MAgKcfKp%2CE0v8NeB0AXLO%2Ci-v8SRlT3GPj%2CQ7v8P2DV6I~y%2CI4v8q7ra6.lX%2Cf2v8AVNYw.E2%2Cs0v8X_6hWpKW%2CI1v8HXGQJnAz%2C70v83SJohTLm%2CY5v8dtAQhbqA%2CO7v8EnlF0aRC%2CH5v8YW6OEKaO%2CP6v8nphSVOaB%2Ck6v8_Vejdj.y%2C73v86N0PVR_-%2Cr_v8LyrNSAJR%2C3Yv8I-fXMRWo%2CMXv8~D_kXz4z%2CBXv8fk-xF7Ks%2CjTv8rCBj-IAn%2C_Yv8wLJWEb6C%2CNZv8EU6X~aln%2CWZv8pJ_Y58B2%2Ce0v8BgMR1c5o&invitationId=inv_5f9f7578-1881-4921-9541-3d323a8e69df