iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 10 **Issue:** III **Month of publication:** March 2022

DOI: https://doi.org/10.22214/ijraset.2022.40321

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue III Mar 2022- Available at www.ijraset.com

A Higher-Level Security Scheme for Key Access ON Cloud Computing

Ankit Patra[1], Saurav Verma[2], Sahil Kumar[3], Prof. S. Keerthi[4]
[1, 2, 3]*Final Year Student, Dayananda Sagar College of Engineering*
[4]*Assistant Professor, Dayananda Sagar College of Engineering*

Abstract: ***In this work, we employ a key access control management scheme which effortlessly transitions any organization-like security policy to state of the art cloud level security. Offering a very flexible, secure, and hierarchical key access mechanism for institutions that deal with mission-critical data. The scheme also minimizes concerns about moving critical data to the public cloud and ensures only the users with sufficient permission from equal or higher privileged members can access the key by the use of topological ordering of a directed graph which includes self-loop. The main overheads such as public and private storage needs are restricted to a level that is tolerable, and the derivation of key is computationally fast and efficient. From a security perspective, the proposed scheme would be resistant to collaboration attacks and would provide key in distinguishability security. Since the key isn't stored anywhere so, the problem of a data breach is eliminated.***

Keywords: Cloud platform; plagiarism check; Shamir's Secret Key, Cloud security, hierarchical, interpolation, key access, key assignment, secret sharing.

I. INTRODUCTION

With the increase in digitization of several services there are increased demands of storage systems, large-scale computations, and hosting. Our proposed scheme allows for the use of any public cloud system to be used as a secure private cloud. We consider the data owner an entity consisting of several organization units. A secure method for each user of this institution to access the public cloud from both inside and outside the company's network would be implemented. The idea of key access control scheme is based on Shamir's secret sharing algorithm and polynomial interpolation method. It is suitable for hierarchical organizational structures like that of a corporation. Since the key does not need to be held anywhere, the problem of a data breach based on key disclosure risk is also eliminated. In Cloud Computing the Higher Level Security Scheme for Key Access is owned and managed by a cloud storage provider which is located off-premise. The system can be accessed by users who have paid for the service. These requirements do not generally create an issue in the private cloud since the infrastructure which is owned and managed by the customer is located on-premise. Even though public cloud infrastructure ensures many advantages, especially in total cost, many organizations are slowing down on the overall adoption of the public cloud due to concerns about reliability, availability, data integrity, and regulatory compliance.

The adoption obstacles for public cloud are business continuity, availability, data confidentiality, and data lock-in. The proposed scheme offers additional security layers to minimize or alleviate concerns regarding transferring mission-critical data to a public cloud. The essential features of the scheme is designed for data owners desiring to access DSaaS from a public cloud is derived from the mathematical tool of Newton's interpolation. Our key access control scheme will be desirable for an organizational unit (OU) within a company that aims to accomplish a specific function in the organization. An organizational unit is one of the several vital business functions within a corporation. Despite the various methods to design the hierarchical structure of an institution, it is common for all users to not have the same access control or privileges.

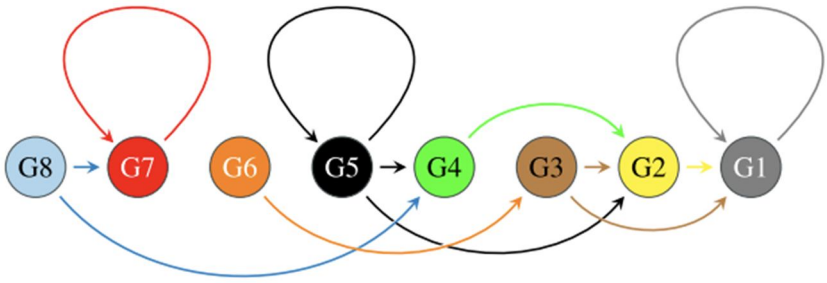


Fig. 1. A topological ordering of a directed graph including self-loop based on the security policy defined by the data owner.

Figure 1 is an example of pre-determined conditions in an organizational structure defined by any data owner. Now, each color represents distinct security clearance levels within the same Organizational Unit. G1 has the highest level, and G8 has the lowest level in the hierarchy. The tip of the arrow indicates the higher-level groups that the lower-level group members need to get permission from to derive the K of the Organizational Unit. Therefore, the users can access data only if they get enough approvals. As seen in Figure 1, G8 needs approvals from users of both G7 and G4. G7 only needs approvals from users in G7. G6 only needs enough from users in G3. G5 needs approvals from the users in G5, G4, and G2. G4 only needs enough from users in G2. G3 needs approvals both from users of G2 and G1. G2 only needs enough approvals from users in G1. G1 only needs approvals from users in G1. In this way, the data owner can flexibly determine distinct relations according to its own security policy.

The rest of the paper is as follows. It is devoted to related works on hierarchical key access control schemes in the literature survey. The researchers also talk about the architecture of the proposed scheme and explain all components in detail including the implementation of Higher-Level Security Scheme for Key Access in Cloud Computing results, security and performance analysis of the scheme and present a concluding remark.

II. LITERATURE SURVEY

Several new features have been added over the years to cloud computing and storage. Some of the features are real-time access of data, secure hierarchical key access, secret one-time access, huge storage of data for lesser cost, higher computing power than a home laptop, data recovery system, data backup system, encrypted data storage system, etc. Among them the most useful features are efficient storage and fast retrieval of data, tracking the data flow in real time, automatic generation of graphs and charts explaining data inflow and outflow, and automatic generation of data hierarchical trees in a corporate structure after the addition of a new leaf(or employee).

The previous papers mainly analyze the problems relating to cryptographic key access to data and then we go on to see papers by Google on cloud enumerating the possibility of data storage on cloud. Later we witnessed the global decrease in data storage prices which led to the wider adaptability to storing data on cloud. This called for the need of improvement of the existing cloud computing systems. Most of this improvement as we would would be focused on the security and access-control than on the improvement of other services since that is the scope of improvement of our papers. The first few studies focused on the cryptographic key assignment scheme for access control in hierarchical structure like that in a corporation. In this study it was proposed that we employ a time-bound cryptographic key assignment scheme in which the cryptographic keys of a class are different for each time period but, this system is with its own flaws. So, in further studies we propose a key derivation that is constrained by both the class relation and time period rather than just time. This greatly improves computation; performance and reduces the cost of implementation.

Further down the road we saw the need for a hierarchical key assignment scheme which protects the sensitive higher class information from the access from the child classes. Later practical application scenarios were considered and were used to illustrate how trust systems can work with cryptographic-role based access control and can be used to reduce risks and enhance the quality of decision making by cloud data administrators and assign the roles of cloud storage service. As per reports, due to cloud computing's rapid growth it is anticipated that cloud computing will be a crucial and challenging issue in the IT industry. The last significant development in security was SECO where a two-level hierarchical identity based encryption (HIBE) to guarantee data confidentiality against untrusted cloud. Yet there is scope of improvement in terms of security, data confidentiality and automation of processes.

III.PROPOSED SOLUTION

A. Implementation of Shamir's secret sharing algorithm to eliminate the security and efficiency issues existing in a public cloud system.

B. A Key Establishment Unit is set up on the data owner's side that executes secret key splitting, computation of operations, sharing of generations, and also performs the approval and key derivation mechanisms according to the input received from LDAP queries and Security Level Policy.

C. The Credential Generator is responsible for construction of the secret key by using the key components received and sends the secret key to Cloud Management Client.

D. The Network Control Policy checks if the request is received inside or outside the network. Integrity Controller is responsible for checking if the data in the public cloud has been compromised at any point of time.

E. The data owner would be able to install a Cloud Management Client. An application would be managed for each user inside the cloud and outside the cloud network.

F. The final application would provide secure communication with a standalone workstation inside the network and performs encryption of data before uploading and decryption of data after downloading data.

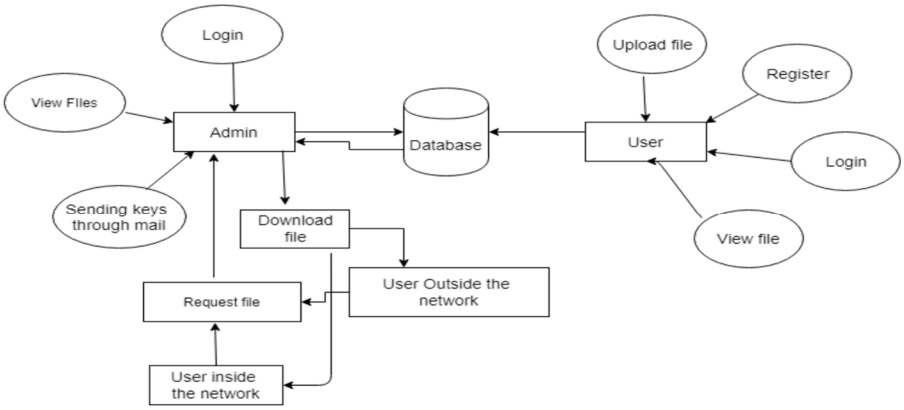


Fig. 1 Block diagram of the proposed solution

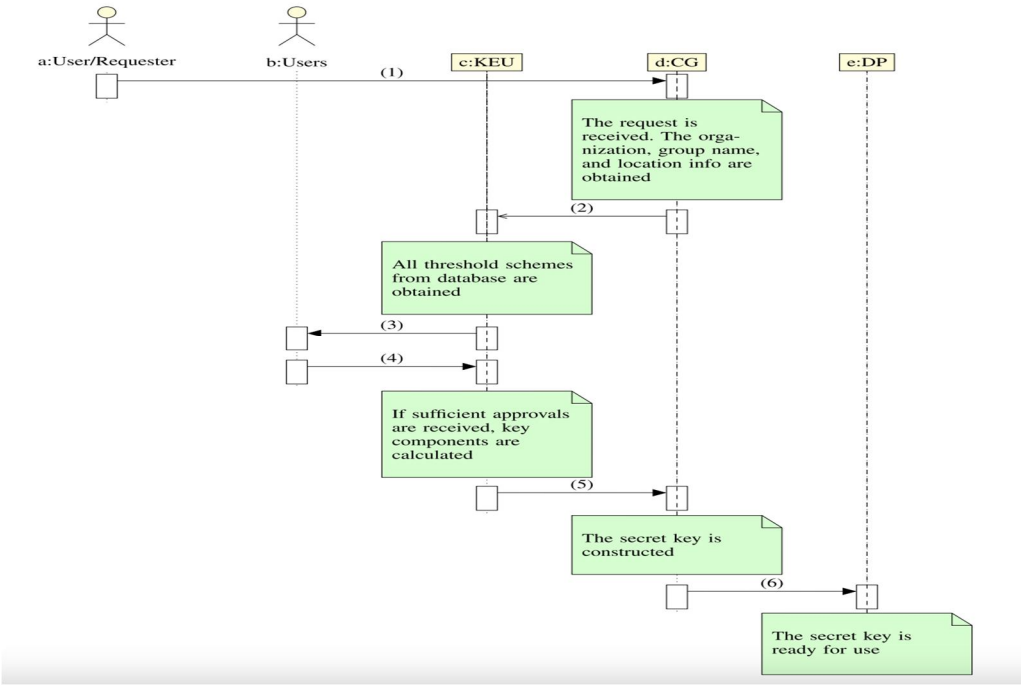


Fig. 2 Algorithm of the proposed solution

IV. CONCLUSIONS

We work with Shamir's secret sharing scheme and Newton's interpolation method. We have exploited this to construct a flexible hierarchical key access control mechanism that can be employed in cloud infrastructures. Private and Public needs of storage are the main overheads for data owners. This scheme has reduced the concern for security of data. And established an access policy based on a hierarchical structure. Our proposed key access control scheme provides us with a computationally efficient method for derivation of key. This scheme is collusion resistant. The scheme would provide the private cloud security and the functionality, accessibility, and cost savings of a public cloud. Other advantages are the reliability of the public cloud, the minimum maintenance and management requirements.

V. ACKNOWLEDGMENT

I would like to express my gratitude and appreciation to all those who gave us the possibility to carry on and complete this paper. Special thanks to our Head of the Department, Guide and other faculty members whose help, supervision, suggestions, and encouragement has helped us in all time of the fabrication process and in writing this paper. I also sincerely thank my teammates for the time spent researching, proofreading, and correcting any errors.

I would also like to acknowledge with much appreciation the crucial role of our college "Dayananda Sagar College of Engineering" for giving us permission to use the infrastructure and research labs to procure necessary papers and other tools.

REFERENCES

[1] L. Zhou, V. Varadharajan, and M. Hitchens, ''Achieving secure role-based access control on encrypted data in cloud storage,'' IEEE Trans. Inf. Forensics Security, vol. 8, no. 12, pp. 1947–1960, Dec. 2013.

[2] L. Zhou, V. Varadharajan, and M. Hitchens, ''Trust enhanced cryptographic role-based access control for secure cloud data storage,'' IEEE Trans. Inf. Forensics Security, vol. 10, no. 11, pp. 2381–2395, Nov. 2015.

[3] W.-G. Tzeng, ''A time-bound cryptographic key assignment scheme for access control in a hierarchy,'' IEEE Trans. Knowl. Data Eng., vol. 14, no. 1, pp. 182–188, Aug. 2002.

[4] H. M. Sun, K. H. Wang, and C. M. Chen, ''On the security of an efficient time-bound hierarchical key management scheme,'' IEEE Trans. Dependable Secure Comput., vol. 6, no. 2, pp. 159–160, Apr. 2009.

[5] S. Tang, X. Li, X. Huang, Y. Xiang, and L. Xu, ''Achieving simple, secure and efficient hierarchical access control in cloud computing,'' IEEE Trans. Comput., vol. 65, no. 7, pp. 2325–2331, Jul. 2016.

[6] A. K. Das, N. R. Paul, and L. Tripathy, ''Cryptanalysis and improvement of an access control in user hierarchy based on elliptic curve cryptosystem,'' Inf. Sci., vol. 209, pp. 80–92, Nov. 2012.

[7] Y.-L. Lin and C.-L. Hsu, ''Secure key management scheme for dynamic hierarchical access control based on ECC,'' J. Syst. Softw., vol. 84, no. 4, pp. 679–685, 2011.

[8] A. De Santis, A. L. Ferrara, and B. Masucci, ''Efficient provably-secure hierarchical key assignment schemes,'' Theor. Comput. Sci., vol. 412, no. 41, pp. 5684–5699, 2011.

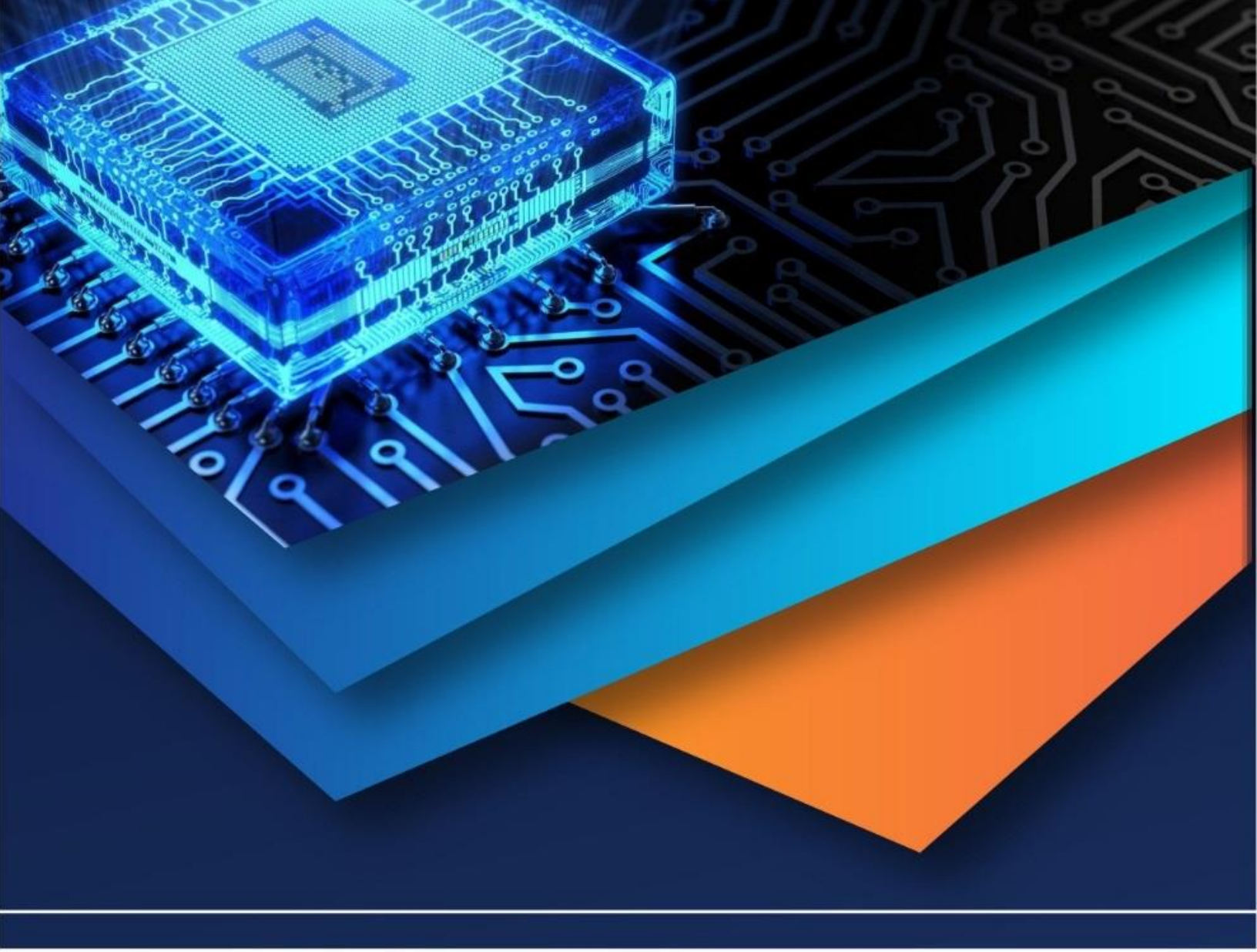
[9] H. Min-Shiang, ''A cryptographic key assignment scheme in a hierarchy for access control,'' Math. Comput. Model., vol. 26, no. 2, pp. 27–31, Jul. 1997.

[10] P. D'Arco, A. De Santis, A. L. Ferrara, and B. Masucci, ''Variations on a theme by Akl and Taylor: Security and tradeoffs,'' Theor. Comput. Sci., vol. 411, no. 1, pp. 213–227, 2010.

[11] M. J. Atallah, M. Blanton, N. Fazio, and K. B. Frikken, ''Dynamic and efficient key management for access hierarchies,'' ACM Trans. Inf. Syst. Secur., vol. 12, no. 3, pp. 1–43, Jan. 2009.

[12] V. R. L. Shen and T.-S. Chen, ''A novel key management scheme based on discrete logarithms and polynomial interpolations,'' Comput. Secur., vol. 21, no. 2, pp. 164–171, 2002.

[13] E. S. V. Freire, K. G. Paterson, and B. Poettering, ''Simple, efficient and strongly KI-secure hierarchical key assignment schemes,'' in Topics in Cryptology—CT-RSA (Lecture Notes in Computer Science), vol. 7779, E. Dawson, Ed. Berlin, Germany: Springer, 2013.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY