JES
Journal of Engineering Sciences

Vol 13, Issue 04, APRIL /2022

ISSN NO:0377-9254

A Novel Method For Web-Based Cloud Computing Services With Fine-Grained Two-Factor Access Control

Nitin Kundu[1], K Prithvi Raj [2], K Rohith Sai[3], Reddy Siva Sankar Vara Prasad[4], K Balaji[5]

#1,##2,#3,#4,#5 Student, Department of ECE, GITAM (deemed to be University), Gandhi nagar Rushikonda Visakhapatnam 530045 Andhra Pradesh, INDIA

ABSTRACT_ In this paper, we introduce a new fine-grained two-factor authentication (2FA) get entry to manipulate machine for web-based cloud computing services. Specifically, in our proposed 2FA get right of entry to manage system, an attribute-based get entry to manipulate mechanism is applied with the necessity of each person secret key and a light-weight protection device. As a person can't get right of entry to the machine if s/he does no longer keep both, the mechanism can beautify the safety of the system, in particular in these situations the place many customers share the equal laptop for web-based cloud services. In addition, attribute-based manage in the machine additionally allows the cloud server to preclude the get admission to to these customers with the equal set of attributes whilst retaining person privacy, i.e., the cloud server solely is aware of that the consumer fulfills the required predicate, but has no thinking on the precise identification of the user. Finally, we additionally elevate out a simulation to exhibit the practicability of our proposed 2FA system.

1.INTRODUCTION

Cloud computing could be a virtual host ADP (Automatic Data Processing)system that enables enterprises to shop, for lease, sell, or distribute software in other digital resources over the web as an on demand service. It not depends on a server or variety of machines that physically exist, because it could be a virtual system. There are several applications of cloud computing, like knowledge sharing [1],[3],[4],[6] , knowledge storage [2],[5], big knowledge management , medical system [7] etc. As sensitive knowledge is also keep within the cloud for sharing purpose or convenient access; and eligible users may access the cloud system for numerous applications and services, user authentication has become a vital part for any cloud system. A user is needed to login before exploitation the cloud services or accessing the sensitive knowledge keep within the cloud. There are 2 issues for the normal account/password based mostly system. First, the normal account/password-based authentication isn't privacy-preserving. However, it is well acknowledged that privacy is a necessary feature that has to be thought of in cloud computing systems. Second, it is common to share a laptop/desktop among completely different folks. It's going to be simple for hackers to put in some spyware to be told the login password from the web-browser. A recently planned access control model known as attribute-based access management could be a sensible candidate to tackle the matter. It not solely provides anonymous authentication however conjointly any defines access control policies supported completely different attributes of the requester, environment, or the info object. In an attribute-based access control system,1 each user has a user secret key issued by the authority. In practice, the user secret key is stored inside the personal computer. When we consider the above mentioned second problem on webbased services, it is common that computers may be shared by many users especially in some large enterprises or organizations. For example, let us consider the following two

scenarios: • In a hospital, computers are shared by different staff. Dr. Alice uses the computer in room A when she is on duty in the daytime, while Dr. Bob uses the same computer in the same room when he is on duty at night. A more secure way is to use two-factor authentication (2FA). 2FA is very common among web-based e-banking services. In addition to a username/password, the user is also required to have a device to display a one-time password. Some systems may require the user to have a mobile phone while the one-time password will be sent to the mobile phone through SMS during the login process. By using 2FA, users will have more confidence to use shared computers to login for web-based e-banking services. For the same reason, it will be better to have a 2FA system for users in the webbased cloud services in order to increase the security level in the system.

2.LITERATURE SURVEY

1) Mobile cloud computing: A survey

AUTHORS: N. Fernando, S. W. Loke, and W. Rahayu

Despite growing utilization of cell computing, exploiting its full workable is tough due to its inherent troubles such as useful resource scarcity, widespread disconnections, and mobility. Mobile cloud computing can tackle these issues via executing cellular functions on useful resource companies exterior to the cellular device. In this paper, we furnish an sizeable survey of cell cloud computing research, whilst highlighting the particular worries in cell cloud computing. We existing a taxonomy primarily based on the key problems in this area, and talk about the distinctive techniques taken to handle these issues. We conclude the paper with a crucial evaluation of challenges that have now not but been completely met, and spotlight instructions for future work.

2) Cloud-based augmentation for cellular devices: motivation, taxonomies, and open challenges

AUTHORS: S. Abolfazli, Z. Sanaei, E. Ahmed, A. Gani, and R. Buyya

Recently, Cloud-based Mobile Augmentation (CMA) procedures have received great floor from academia and industry. CMA is the contemporary cellular augmentation mannequin that employs resource-rich clouds to increase, enhance, and optimize computing competencies of cell units aiming at execution of resource-intensive cellular applications. Augmented cell gadgets envision to operate large computations and to shop huge records past their intrinsic skills with least footprint and vulnerability. Researchers make use of diverse cloud-based computing sources (e.g., far-off clouds and close by cellular nodes) to meet a range of computing necessities of cellular users. However, using cloud-based computing assets is no longer a simple panacea. Comprehending vital elements (e.g., cutting-edge country of cellular purchaser and far flung resources) that affect on augmentation procedure and most fulfilling decision of cloud-based useful resource sorts are some challenges that avert CMA adaptability. This paper comprehensively surveys the cell augmentation area and gives taxonomy of CMA approaches. The targets of this find out about is to spotlight the outcomes of faraway sources on the best and reliability of augmentation techniques and talk about the challenges and possibilities of using various cloud-based assets in augmenting cellular devices. We existing augmentation definition, motivation, and taxonomy of augmentation types, which includes usual and cloud-based. We seriously analyze the brand new CMA procedures and classify them into 4 companies of far-off fixed, proximate fixed, proximate mobile, and hybrid to current a taxonomy. Vital choice making and overall performance problem elements that affect on the adoption of CMA tactics are brought and an exemplary

selection making flowchart for future CMA processes are presented. Impacts of CMA techniques on cell computing is mentioned and open challenges are introduced as the future lookup directions.

3) Mobile cloud computing: Standard method to defending and securing of cellular cloud ecosystems

AUTHORS: R. Kumar and S. Rajalakshmi

The standards of Cloud computing are naturally meshed with cellular units to allow on-the-go functionalities and benefits. The cellular cloud computing is rising as one of the most vital branches of cloud computing and it is predicted to increase the cell ecosystems. As greater cell gadgets enter the market and evolve, surely safety problems will develop as well. Also, sizeable increase in the range of units related to the Internet will similarly pressure protection needs. Understanding the authentic plausible of cell cloud computing and figuring out troubles with cellular cloud security, privacy, feasibility and accessibility continue to be a primary situation for each the clients and the enterprises. This paper covers the cell cloud protection problems and challenges with the aid of searching at the contemporary country of cloud protection breaches, vulnerabilities of cellular cloud devices, and how to tackle these vulnerabilities in future work in element of cell machine administration and cell records protection. Also, it highlights on utilization of SCWS (Smart Card Web Services) competition to intensify safety of cell cloud computing.

3.PROPOSED SYSTEM

In this paper, we advocate a fine-grained two-factor get entry to manage protocol for web-based cloud computing services, the usage of a light-weight safety device. The system has the following properties: (1) it can compute some light-weight algorithms, e.g. hashing and exponentiation; and (2) it is tamper resistant, i.e., it is assumed that no one can wreck into it to get the secret facts saved inside.

In this paper, we endorse a fine-grained two-factor get right of entry to manage protocol for web-based cloud computing services, the usage of a light-weight safety device. The gadget has the following properties. It can compute some light-weight algorithms, e.g. hashing and exponentiation; and it is tamper resistant, i.e., it is assumed that no one can damage into it to get the secret data saved inside.

With this device, our protocol offers a 2FA security. First the person secret key (which is typically saved internal the computer) is required. In addition, the protection system ought to be additionally related to the pc (e.g. via USB) in order to authenticate the person for getting access to the cloud. The consumer can be granted get admission to solely if he has each items.

Furthermore, the consumer can't use his secret key with any other machine belonging to others for the access. Our protocol helps fine-grained attribute-based get admission to which gives a exquisite flexibility for the gadget to set one of a kind get admission to insurance policies in accordance to one-of-a-kind scenarios. At the equal time, the privateness of the person is additionally preserved. The cloud device solely is aware of that the consumer possesses some required attribute, however no longer the actual identification of the user. To exhibit the practicality of our system, we simulate the prototype of the protocol

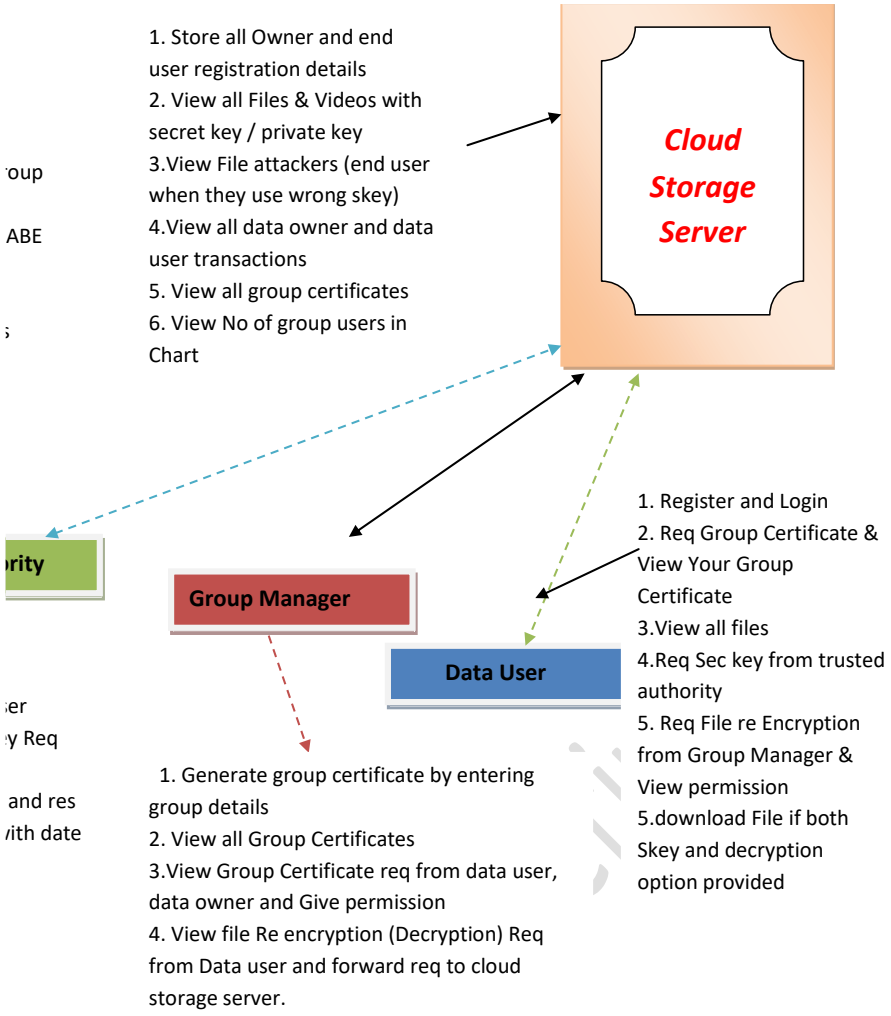

Fig 1: Architecture

3.1 IMPLEMENTAION

- **Data Owner**

In this module, the data owner uploads their data in the cloud server. For the security purpose the data owner encrypts the data file and then store in the cloud. The Data owner can have capable of manipulating the encrypted data file. And the data owner can set the access privilege to the encrypted data file.

- **Cloud Server**

The cloud service provider manages a cloud to provide data storage service. Data owners encrypt their data files and store them in the cloud for sharing with data consumers. To access the shared data files, data consumers download encrypted data files of their interest from the cloud and then decrypt them. It is responsible for authorizing all end users.

- **Key Distribution centre**

KGC who is trusted to store verification parameters and offer public query services for these parameters such as generating secret key based on the file and send to the corresponding end users. It is responsible for capturing the attackers.

- **Data Consumer/End User**

In this module, the user can only access the data file with the encrypted key if the user has the privilege to access the file. For the user level, all the privileges are given by the Data owner and the Data users are controlled by the data owner only. Users may try to access data files either within

their access privileges, so malicious users may collude with each other to get sensitive files beyond their privileges. He is sending request to KGC to generate secret key and KGC will generate the skey and send to corresponding end user.

- **Attacker (Unauthorized User)**

Attacker adds the malicious data to a block in cloud server. Then the Unauthorized user will considered as a attacker

.

4.RESULTS AND DISCUSSION

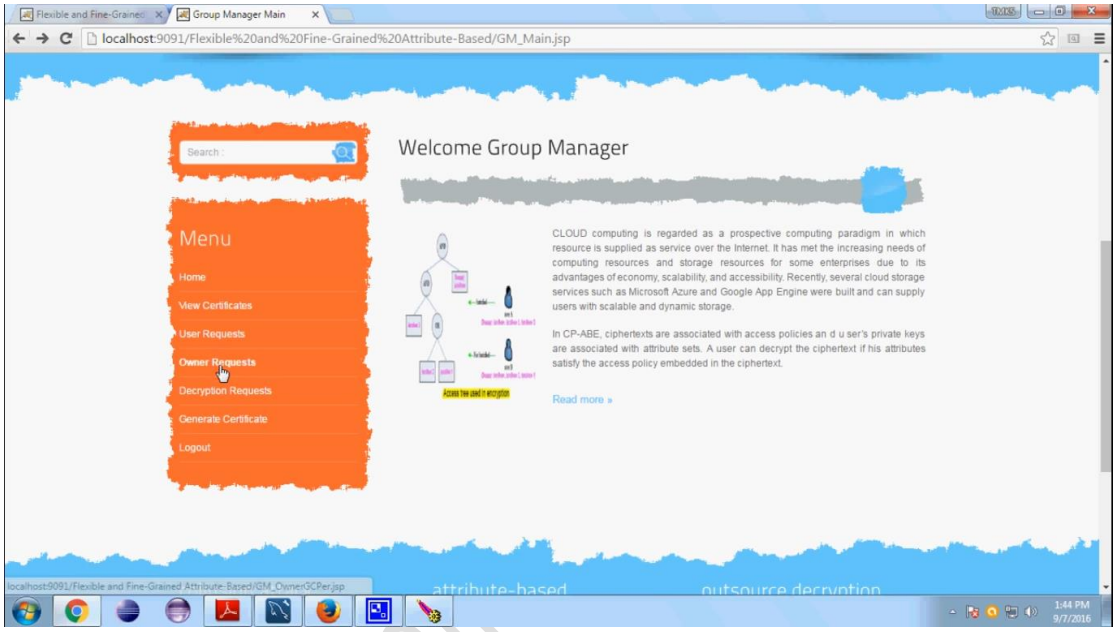

Fig 2: Group Manager Home Page

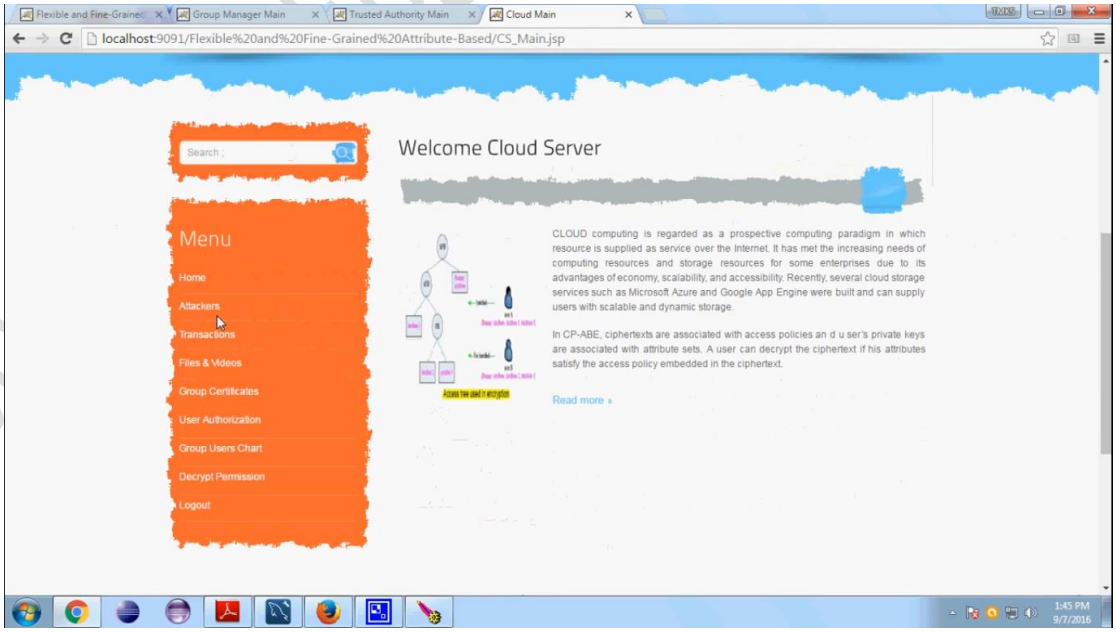

Fig 3:Cloud server Home Page

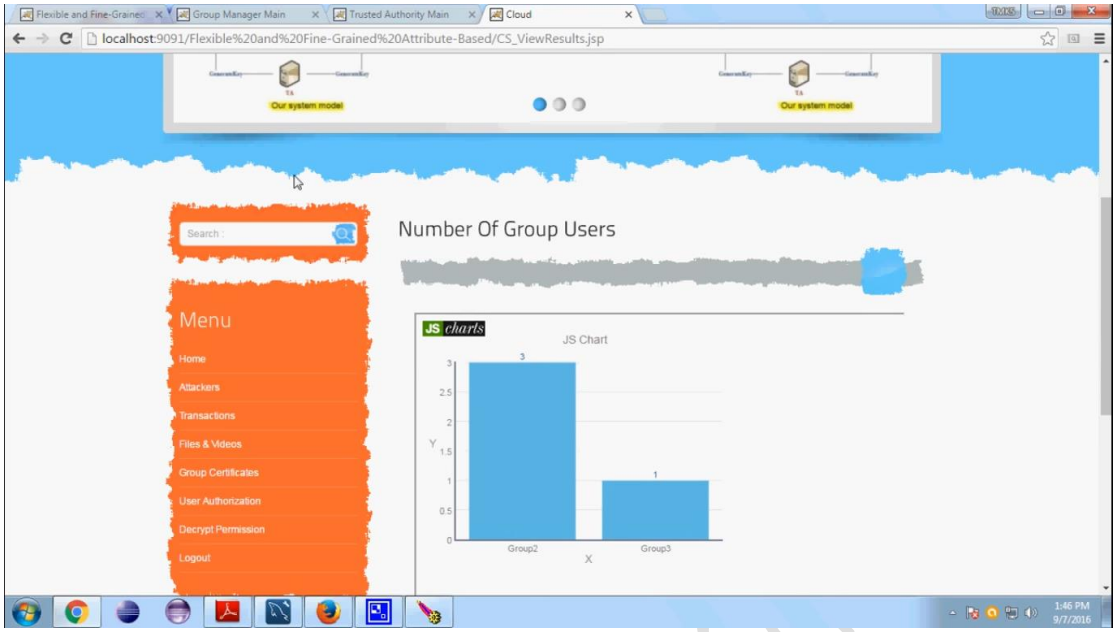

Fig 4:Grop User Data In Graphical Format

5.CONCLUSION

In this research, we provide a completely new 2FA access control system for web-based cloud computing services that includes both a user secret key and a lightweight security device. Based on the attribute-based access management mechanism, the proposed 2FA access system is known to not only allow the cloud server to limit access to those users who have an analogous set of attributes, but also to protect user privacy. A thorough security study reveals that the proposed 2FA access control system meets the necessary security requirements. We have a tendency to establish that the construction is "viable" through performance analysis. We tend to leave as future work to further improve the potency while retaining all of the system's great features.

REFERENCES

[1] A. Sahai and B. Waters, "Fuzzy Identity-Based Encryption," *EUROCRYPT '05*, LNCS, vol. 3494, pp. 457-473, 2005.

[2] J. Bethencourt, A. Sahai and B. Waters, "Ciphertext-Policy Attribute- Based Encryption," *Proc. IEEE Symposium on Security and Privacy*, IEEE Transactions on Services Computing,Volume:PP,Issue:99,Date of Current Version:22.January.2016pp. 321-334, May 2007, doi: 10.1109/SP.2007.11.

[3] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-Based En-cryption for Fine-Grained Access Control of Encrypted Data," *Proc. 13th ACM Conference on Computer and Communications Security (CCS '06)*, pp. 89-98, 2006, doi:10.1145/1180405.1180418.

[4] D. Boneh and M.K. Franklin, "Identity-Based Encryption from the Weil Pairing," *SIAM Journal of Computing*, vol. 32, no. 3, pp. 586-615, 2003.

[5] A. Boldyreva, V. Goyal, and V. Kumar , "Identity-Based En-cryption with Efficient Revocation," *Proc. 15th ACM conference on Computer and communications security (CCS ' 08)*, pp. 417-426, 2008.

[6] S. Yu, C. Wang, K. Ren, and W. Lou , "Attribute Based Data Sharing with Attribute Revocation," *Proc. 5th ACM Symposium on Information, Computer and Communications Security (ASIACCS ' 10)*, pp. 261-270, 2010.

[7] M. Yang, F. Liu, J. Han, and Z. Wang, "An Efficient Attribute based Encryption Scheme with Revocation for Outsourced Data Sharing Control," *Proc. 2011 International Conference on Instru-mentation, Measurement, Computer, Communication and Control*, pp. 516-520, 2011.

[8] P.K. Tysowski and M.A. Hasan, "Hybrid Attribute-Based Encryption and Re-Encryption for Scalable Mobile Applica-tions in Clouds," *IEEE Transactions on Cloud Computing*, pp. 172-186, 2013.

[9] J. Hur and D. K. Noh, "Attribute-Based Access Control with Efficient Revocation in Data Outsourcing Systems," *IEEE Transactions on Parallel and Distributed Systems*, pp. 1214-1221, 2011.

[10] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving Secure, Scal-able, and Fine-Grained Data Access Control in Cloud Comp u-ting," *Proc. of IEEE INFOCOM '10*, pp. 1-9, 2010.

[11] M. Green, S. Hohenberger and B. Waters, "Outsourcing the decryp-tion of ABE ciphertexts," *Proc. 20th USENIX Conference on Security (SEC '11),* pp. 34, 2011.

[12] J. Li, X.F. Chen, J.W. Li, C.F. Jia, J.F. Ma and W.J. Lou, "Fine-Grained Access Control System Based on Outsourced Attribute-Based Encryp-tion," *Proc. 18th European Symposium on Research in Computer Security (ESORICS '13)*, LNCS 8134, Berlin: Springer-Verlag, pp. 592-609, 2013.

[13] J.W. Li, C.F. Jia, J. Li and X.F. Chen, "Outsourcing Encryption of At-tribute-Based Encryption with Mapreduce," *Proc. 14th International Conference on Information and Communications Security (ICICS '12),* LNCS 7618, Berlin: Springer-Verlag, pp. 191-201, 2012. doi: 10.1007/978-3-642-34129-8_17

[14] M. Chase, "Multi-authority Attribute Based Encryption," *Proc. 4th Theory of Cryptography Conference (TCC '07)*, LNCS 4392, Berlin: Springer-Verlag, pp. 515-534, 2007.

[15] Z. Liu, Z. Cao, Q. Huang, D. S. Wong and T. H. Yuen, "Fully Secure Multi-Authority Ciphertext-Policy Attribute-Based Encryption with-out Random Oracles," *Proc. 16th European Symposium on Research in Computer Security (ESORICS '11)*, LNCS 6879, Berlin: Springer-Verlag, pp. 278-297, 2011.

[16] J.G. Han, W. Susilo, Y. Mu and J. Yan, "Privacy-Preserving Decentral-ized Key-Policy Attribute-Based Encryption," *IEEE Transactions on Parallel and Distributed Systems*, vol. 23, no.11, pp. 2150-2162, Nov 2012, doi: 10.1109/TPDS.2012.50.

[17] H.L. Qian, J.G. Li and Y.C. Zhang, "Privacy-Preserving Decentralized Ciphertext-Policy Attribute-Based Encryption with Fully Hidden Ac-cess Structure," *Proc. 15th International Conference on Information and Communications Security (ICICS '13)*, LNCS 8233, Berlin: Springer- Verlag, pp. 363-372, 2013.

[18] H.L. Qian, J.G. Li, Y.C. Zhang and J.G. Han, "Privacy Preserv-ing Personal Health Record Using Multi-Authority Attribute- Based Encryption with Revocation," *International Journal of Information Security*, doi: 10.1007/s10207-014-0270-9.

[19] Z. Liu, Z.F. Cao and Duncan S. Wong, "Black-Box Traceable CP-ABE: How to Catch People Leaking Their Keys by Selling Decryption Devices on eBay," *Proc. 2013 ACM SIGSAC Conference on Computer and Communications Security (CCS '13)*, pp. 475-486, 2013, doi: 10.1145/2508859.2516683.

Vol 13, Issue 04, APRIL /2022

ISSN NO:0377-9254

[20] Z. Liu, Z.F. Cao and Duncan S. Wong, "White-Box Traceable Ciphertext-Policy Attribute-Based Encryption Supporting Any Monotone Access Structures," *IEEE Transactions on Information Fo-rensics and Security*, vol. 8, no. 1, pp. 76-88, 2013, doi: 10.1109/TIFS.2012.2223683.