International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

Design and Implementation of User Anonymity and Authentication Scheme for Decentralized Access Control in Clouds: Review

Pooja R. Vyawhare[1], Namrata D. Ghuse[2]

[1]Department of Computer Science & Engineering, PRMIT, Amravati, Maharashtra, India

[2] Professor Department of Computer Science & Engineering, PRMIT, Amravati, Maharashtra, India

Abstract: ***Placing critical data in the hands of a cloud provider should come with the guarantee of security and availability for data at rest, in motion, and in use. Several alternatives exist for storage services, while data confidentiality solutions for the database as a service paradigm are still immature. To protect outsourced data in cloud storage against corruptions, adding fault tolerance to cloud storage, along with efficient data integrity checking and recovery procedures, becomes critical. So, this work proposes a new decentralized access control scheme for secure data storage in clouds, which supports anonymous authentication. In the proposed scheme, the cloud verifies the authenticity of the ser without knowing the user's identity before storing data. Our scheme also has the added feature of access control in which only valid users are able to decrypt the stored information. The scheme prevents replay attacks and supports creation, modification, and reading data stored in the cloud. We also address user revocation. Moreover, our authentication and access control scheme is decentralized and robust, unlike other access control schemes designed for clouds which are centralized. The communication, computation, and storage overheads are comparable to centralized approaches.***

Keywords: *Access Control, Cloud Computing,* Cloud Storage, Anonymous Authentication, decentralized access

1. Introduction

Cloud computing provides seemingly unlimited "virtualized" resources to users as services across the whole Internet, while hiding platform and implementation details. Today's cloud service providers offer both highly available storage and massively parallel computing resources at relatively low costs. As cloud computing becomes prevalent, an increasing amount of data is being stored in the cloud and shared by users with specified *privileges*, which define the access rights of the stored data. One critical challenge of cloud storage services is the management of the ever-increasing volume of data. IN a cloud context, where critical information is placed in infrastructures of untrusted third parties, ensuring data confidentiality is of paramount importance[20].

Much of the data stored in clouds is highly sensitive, for example, medical records and social networks. Security and privacy are, thus, very important issues in cloud computing. In one hand, the user should authenticate itself before initiating any transaction, and on the other hand, it must be ensured that the cloud does not tamper with the data that is outsourced. User privacy is also required so that the cloud or other users do not know the identity of the user. The cloud can hold the user accountable for the data it outsources, and likewise, the cloud is itself accountable for the services it provides[29].

Considering the following situation: A law student, Alice, wants to send a series of reports about some malpractices by authorities of University X to all the professors of University X, research chairs of universities in the country, and students belonging to Law department in all universities in the province. She wants to remain anonymous while publishing all evidence of malpractice. She stores the information in the cloud. Access control is important in such case, so that only authorized users can access the data. It is also important to verify that the information comes from a reliable source. The problems of access control, authentication, and privacy protection should be solved simultaneously. We address this problem in its entirety in this paper.

Access control in clouds is gaining attention because it is important that only authorized users have access to valid service. A huge amount of information is being stored in the cloud, and much of this is sensitive information. Care should be taken to ensure access control of this sensitive information which can often be related to health, important documents (as in Google Docs or Dropbox) or even personal information (as in social networking). There are broadly three types of access control: user-based access control (UBAC), role-based access control (RBAC), and attribute-based access control (ABAC). In UBAC, the access control list contains the list of users who are authorized to access data. This is not feasible in clouds where there are many users. In RBAC (introduced by Ferraiolo and Kuhn [10]), users are classified based on their individual roles. Data can be accessed by users who have matching roles. The roles are defined by the system. For example, only faculty members and senior secretaries might have access to data but not the junior secretaries. ABAC is more extended in scope, in which users are given attributes, and the data has attached access policy. Only users with valid set of attributes, satisfying the access policy, can access the data. For instance, in the above example certain records might be accessible by faculty members with more than 10 years of research experience or by senior secretaries with more than 8 years experience.

It is just not enough to store the contents securely in the cloud but it might also be necessary to ensure anonymity of

the user. For example, a user would like to store some sensitive information but does not want to be recognized. The user might want to post a comment on an article, but does not want his/her identity to be disclosed. However, the user should be able to prove to the other users that he/ she is a valid user who stored the information without revealing the identity.

2. Literature Survey

Vipul Goyal, Omkant Pandey, Amit Sahai, Brent Waters[27]introduced the concept of Attribute-Based Encryption for Fine Grained Access Control of Encrypted Data in 2006. He introduces the new cryptosystem for fine grained sharing of encrypted data that we call Key-Policy Attribute-Based Encryption (KPABE). In cryptosystem, ciphertexts are labeled with sets of attributes and private keys are associated with access structures that control which ciphertexts a user is able to decrypt. Fine-grained access control systems facilitate granting differential access rights to a set of users and allow flexibility in specifying the access rights of individual users. Several techniques are known for implementing fine grained access control. Secret-sharing schemes (SSS) are used to divide a secret among a number of parties.

Matthew Pirretti and Brent Waters[31]introduce a novel secure information management architecture based on emerging attribute-based encryption (ABE) primitives also they propose cryptographic optimizations in Secure Attribute Based Systems in 2007. A performance analysis of ABE system and example applications demonstrates the ability to reduce cryptographic costs by as much as 98% over previously proposed constructions. Through this, demonstrates that the attribute system is an efficient solution for securely managing information in large, loosely-coupled, distributed systems. Decryption decrypts a ciphertext encrypted by the Encryption. This process begins with the decrypting party verifying that they have the required attributes. The party performing decryption will then use their attributes to decrypt the decrypt the ciphertext in order to obtain the AES and HMAC key.

John Bethencourt, Amit Sahai, Brent Waters[26]introduces Ciphertext-Policy Attribute-Based Encryption in 2008. they employ a trusted server to store the data and mediate access control. In several distributed systems a user should only be able to access data if a user posses a certain set of credentials or attributes. Currently, the only method for enforcing such policies is to employ a trusted server to store the data and mediate access control. However, if any server storing the data is compromised, then the confidentiality of the data will be compromised. In addition, they provide an implementation of our system and give performance measurements. The primary challenge in this line of work is to find a new systems with elegant forms of expression that produce more than an arbitrary combination of techniques.

Sabrina De Capitani di Vimercati, Sara Foresti, Sushil Jajodia, Stefano Paraboschi, Pierangela Samarati describes combination of access control and cryptography in 2010. It illustrate the basic principles on which an architecture for combining access control and cryptography can be built. then illustrate an approach for enforcing authorization policies and supporting dynamic authorizations, allowing policy changes and data updates at a limited cost in terms of bandwidth and computational power. It We also described an approach for policy evolution that takes into account the main features of the scenario and is able to guarantee in most cases confidentiality of the information in the presence of significant policy updates, clearly identifying the exposure to collusion when this risk may arise. Other issues to be investigated include the integration with the Web paradigm, and the efficient execution of queries.

Markulf Kohlweiss, Ueli Maurer, Cristina Onete, Bjorn Tackmann, Daniele Venturi[9]introduced Anonymity-preserving Public-Key Encryption:A Constructive Approach where public-key cryptosystems with enhanced security properties have been proposed. it investigate constructions as well as limitations for preserving receiver anonymity when using public-key encryption (PKE). They use the constructive cryptography approach by Maurer and Renner and interpret cryptographic schemes as constructions of a certain ideal resource (e.g. a confidential anonymous channel) from given real resources (e.g. a broadcast channel). We define appropriate anonymous communication resources and show that a very natural resource can be constructed by using a PKE scheme which fulfills three properties that appear in cryptographic Literature. results do not only support the trust in existing schemes and constructions; they also show that the simpler and more efficient weakly robust schemes can be used safely.

Junbeom Hur, Dong Kun Noh[23] introduces the concept of Attribute-Based Access Control with Effcient Revocation in Data Outsourcing Systems in May 16, 2012. The attribute based crypto-systems were introduced such as Ciphertext-Policy Attribute-Base Encryption (CP-ABE) with an addition of two new functions. The first function is KEKGen(U)) which is used to generate keys to encrypt attributes for groups. The other extra function is the ReEncrypt(CT;G) which is a re-encryption that takes the ciphertext and re-encrypt it so that a user in Group G can only access it.

R.Ranjith and D.Kayathri Devi[16] describes the concept of Secure Cloud Storage using Decentralized Access Control with Anonymous Authentication in 2013. we implemented secure cloud storage by providing access to the files with the policy based file access using Attribute Based Encryption (ABE) scheme with RSA key public-private key combination. Private Key is the combination of the user's credentials. So that high security will be achieved. Time based file Revocation scheme is used for file assured deletion. When the time limit of the file expired, the file will be automatically revoked and cannot be accessible to anyone in future. Manual Revocation also supported. Policy based file renewal is proposed. The Renewal can be done by providing the new key to the existing file, will remains the file until the new time limit reaches.

Mr. Parjanya C.A and Mr. Prasanna Kumar M[15]describes the concept of Advance Secure Multi-Owner Data Sharing

for Dynamic Groups in the Cloud in march 2014. They were presented the new framework for MONA. In this method further presented how to manage the risks like failure of group manager by increasing the number of backup group manager, hanging of group manager in case number of requests more by sharing the workload in multiple group managers. This method claims required efficiency, scalability and most importantly reliability. Extensive analyses show that our proposed scheme satisfies the desired security requirements and guarantees efficiency as well. Here we also show that how user gets extra time even after the time out this also one of the advantage of proposed schema.

S Divya Bharathy and T Ramesh[14] intrdused the concept of privacy preserving access control scheme for data storage, which supports anonymous authentication and performs decentralized key management in Securing Data Stored in Clouds Using Privacy Preserving Authenticated Access Control in April 2014. In the proposed scheme, the cloud adopts an access control policy and attributes hiding strategy to enhance security. This new scheme supports secure and efficient dynamic operation on data blocks, including: data update, creation, modification and reading data stored in the cloud. Moreover, our authentication and access control scheme is decentralized and robust, unlike other access control schemes designed for clouds which are centralized.

User revocation and access control policies highly contributes to avoid abuse of cloud services and shared technology issues. Sushmita Ruj, Milos Stojmenovic, AmiyaNayak[1]-[17] introduces Decentralized Access Control with Anonymous Authentication of Data Stored in Clouds in 2014. They propose a new decentralized access control scheme for secure data storage in clouds that supports anonymous authentication. In the proposed scheme, the cloud verifies the authenticity of the series without knowing the user's identity before storing data. Our scheme also has the added feature of access control in which only valid users are able to decrypt the stored information. We have presented a decentralized access control technique with anonymous authentication, which provides user revocation and prevents replay attacks. The cloud does not know the identity of the user who stores information, but only verifies the user's credentials. Key distribution is done in a decentralized way. One limitation is that the cloud knows the access policy for each record stored in the cloud. In future, we would like to hide the attributes and access policy of a user.

Table 1: Tables of Comparison

SR. No.	*Year*	*Author*	*Advantages*
1	2006	Vipul Goyal, Omkant Pandey, Amit Sahai, Brent Waters	Introduces new cryptosystem for ew encrypted data
2	2007	Matthew Pirretti and Brent Waters	Information management architecture based on emerging attribute-based encryption (ABE) primitives and cryptographic optimizations in Secure Attribute Based Systems
3	2008	John Bethencourt, Amit Sahai, Brent Waters	introduces Ciphertext-Policy Attribute-Based Encryption and the confidentiality of the data will be compromised
4	2010	Sabrina De Capitani di Vimercati, Sara Foresti, Sushil Jajodia, Stefano Paraboschi, Pierangela Samarati	combine access control and cryptography. Allows policy changes and data updates at a limited cost in terms of bandwidth and computational power.
5	2012	Junbeom Hur, Dong Kun Noh	The attribute based crypto-systems were introduced such as Ciphertext-Policy Attribute-Base Encryption (CP-ABE) with an addition of new functions.
6	2013	R.Ranjith and D.Kayathri Devi	Secure cloud storage by providing access to the files with the policy based file access using Attribute Based Encryption (ABE) scheme with RSA key public-private key combination
7	2014	Mr. Parjanya C.A and Mr. Prasanna Kumar M	New framework for MONA and to manage the risks like failure of group manager by increasing the number of backup group manager
8	2014	S Divya Bharathy and T Ramesh	Supports anonymous authentication and performs decentralized key management in Securing Data Stored in Clouds. , the cloud adopts an access control policy and attributes hiding strategy to enhance security
9	2014	Sushmita Ruj, Milos Stojmenovic, AmiyaNayak	The cloud verifies the authenticity of the series without knowing the user's identity before storing data. only valid users are able to decrypt the stored information.

3. Shared Technology Issues

Scalable way by sharing infrastructure, platforms, and applications. Whether it's the underlying components that make up this infrastructure (e.g. CPU caches Cloud service providers deliver their services in a, GPUs, etc.) that were not designed to offer strong isolation properties for a multi-tenant architecture (IaaS), re-deployable platforms (PaaS), or multi-customer applications (SaaS), the threat of shared vulnerabilities exists in all delivery models. A defensive in-depth strategy is recommended and should include compute, storage, network, application and user security enforcement, and monitoring, whether the service model is IaaS, PaaS, or SaaS. The key is that a single vulnerability or misconfiguration can lead to a compromise across an entire provider's cloud. Access control in clouds is gaining attention because it is important that only authorized users have access to valid service. A huge amount of information is being stored in the cloud, and much of this is sensitive information. Care should be taken to ensure access control of this sensitive information which can often related to health, important documents (as in Google Docs or Dropbox) or

even personal information (as in social networking).Access control is also gaining importance in online social networking where users (members) store their personal information, pictures, videos and share them with selected groups of users or communities they belong to. It is not just enough to store the contents securely in the cloud but it might also be necessary to ensure anonymity of the user. For example, a user would like to store some sensitive information but does not want to be recognized.

4. Techniques used in Process

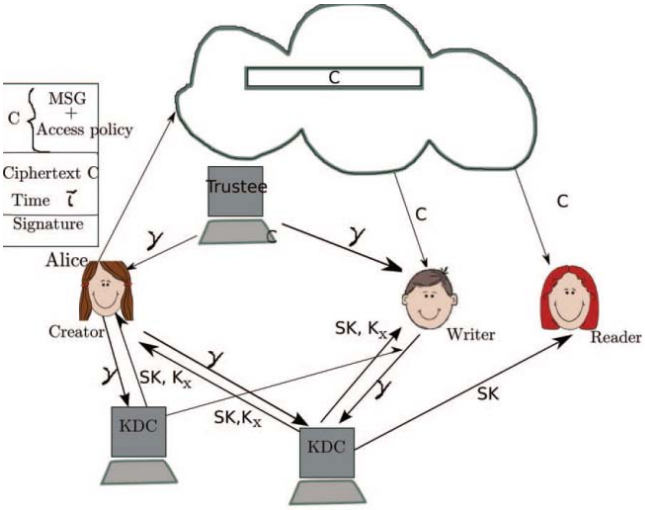

Figure: Cloud Architecture

1) System Initialization

Select a prime q, and groups G1 and G2, which are of order q. We define the mapping ˆe : G1 ×G1 → G2. Let g1, g2 be generators of G1 and hj be generators of G2, for j ∈ [tmax], for arbitrary tmax. Let H be a hash function. Let A0 = ha0 0 , where a0 ∈ Z∗ q is chosen at random. (TSig,TV er) mean TSig is the private key with which a message is signed and TV er is the public key used for verification. The secret key for the trustee is TSK = (a0, TSig) and public key is TPK = (G1,G2,H, g1,A0, h0, h1, . . . , htmax, g2, TV er).

2) User Registration

For a user with identity Uu the KDC draws at random Kbase ∈ G. Let K0 = K1/a0 base . The following token γ is output γ = (u,Kbase,K0, ρ), where ρ is signature on u||Kbase using the signing key TSig.

3) KDC setup

We emphasize that clouds should take a decentralized approach while distributing secret keys and attributes to users. It is also quite natural for clouds to have many KDCs in different locations in the world. The architecture is decentralized, meaning that there can be several KDCs for key management.

4) Attribute generation

The token verification algorithm verifies the signature contained in γ using the signature verification key TV er in TPK. This algorithm extracts Kbase from γ using (a, b) from ASK[i] and computes Kx = K1/(a+bx) base , x ∈ J[i, u]. The key Kx can be checked for consistency using algorithm ABS.KeyCheck(TPK,APK[i], γ,Kx), which checks ˆe(Kx,AijBx ij) = ˆe(Kbase, hj), for all x ∈ J[i, u] and j ∈ [tmax].

5) Sign

The access policy decides who can access the data stored in the cloud. The creator decides on a claim policy Y, to prove her authenticity and signs the message under this claim. The ciphertext C with signature is c, and is sent to the cloud. The cloud verifies the signature and stores the ciphertext C. When a reader wants to read, the cloud sends C. If the user has attributes matching with access policy, it can decrypt and get back original message.

6) Verify

The verification process to the cloud, it relieves the individual users from time consuming verifications. When a reader wants to read some data stored in the cloud, it tries to decrypt it using the secret keys it receives from the KDCs.

5. Conclusion and Future Scope

We have presented a decentralized access control technique with anonymous authentication, which provides user revocation and prevents replay attacks. The cloud does not know the identity of the user who stores information, but only verifies the user's credentials. Key distribution is done in a decentralized way. It proposes a decentralized approach, the technique does not authenticate users, who want to remain anonymous while accessing the cloud.It added features which enables to authenticate the validity of the message without revealing the identity of the user who has stored information in the cloud. we also address user revocation. We use attribute based signature scheme to achieve authenticity and privacy.

References

[1] Sushmita Ruj et. Al. "Decentralized Access Control with Anonymous Authentication of Data Stored in Clouds" IEEE Transactions On Parallel And Distributed Systems, VOL. 25, NO. 2, FEBRUARY 2014, pp. 384-394.
[2] H.K. Maji, M. Prabhakaran, and M. Rosulek, "Attribute-Based Signatures: Achieving Attribute-Privacy and Collusion-Resistance," IACR Cryptology ePrint Archive, 2008.
[3] H.K. Maji, M. Prabhakaran, and M. Rosulek, "Attribute-Based Signatures," Topics in Cryptology - CT-RSA, vol. 6558, pp. 376-392, 2011.
[4] A. Sahai and B. Waters, "Fuzzy Identity-Based Encryption," Proc. Ann. Int'l Conf. Advances in Cryptology (EUROCRYPT), pp. 457-473, 2010.
[5] X. Liang, Z. Cao, H. Lin, and D. Xing, "Provably Secure and Efficient Bounded Ciphertext Policy Attribute Based Encryption," Proc. ACM Symp. Information, Computer and Comm. Security (ASIACCS), pp 343-352, 2009.
[6] M. Chase, "Multi-Authority Attribute Based Encryption," Proc. Fourth Conf. Theory of Cryptography (TCC), pp. 515-534, 2007.

[7] H. Lin, Z. Cao, X. Liang, and J. Shao, "Secure Threshold Multi- Authority Attribute Based Encryption without a Central Authority," Proc. Progress in Cryptology Conf. (INDOCRYPT), pp. 426-436, 2008.
[8] M. Chase and S.S.M. Chow, "Improving Privacy and Security in Multi-Authority Attribute-Based Encryption," Proc. ACM Conf. Computer and Comm. Security, pp. 121-130, 2009.
[9] M. Green, S. Hohenberger, and B. Waters, "Outsourcing the Decryption of ABE Ciphertexts," Proc. USENIX Security Symp., 2011.
[10] K. Yang, X. Jia, and K. Ren, "DAC-MACS: Effective Data Access Control for Multi-Authority Cloud Storage Systems," IACR Cryptology ePrint Archive, p. 419, 2012.
[11] A.B. Lewko and B. Waters, "Decentralizing Attribute-Based Encryption," Proc. Ann. Int'l Conf. Advances in Cryptology (EUROCRYPT), pp. 568-588, 2011.
[12] http://crypto.stanford.edu/pbc/, 2013.
[13] "Libfenc: The Functional Encryption Library,"http://code.google.com/p/libfenc/, 2013.
[14] S Divya Bharathy,T Ramesh,"Securing Data Stored in Clouds Using Privacy Preserving Authenticated Access Control," Proc. *IJCSMC, Vol. 3, Issue. 4, April 2014, pg.1069 – 1074.*
[15] Mr. Parjanya C.A,Mr. Prasanna Kumar M," Advance Secure Multi-Owner Data Sharing for Dynamic Groups in the Cloud," Proc. IJARCSSE, Volume 4, Issue 3, March 2014.
[16] R.Ranjith, D.Kayathri Devi," Secure Cloud Storage using Decentralized Access Control with Anonymous Authentication," Proc. IJARCCE, *Vol. 2, Issue 11, November 2013.*
[17] *S.Seenu Iropia, R.Vijayalakshmi,"DECENTRALIZED ACCESS CONTROL OF DATA STORED IN CLOUD USING KEY POLICY ATTRIBUTE BASED ENCRYPTION," Proc.* IJICSE,*Volume 1 Issue 2 2014.*
[18] Yang Tang, Patrick P.C. Lee, John C.S. Lui and Radia Perlman, "Secure Overlay Cloud Storage with Access Control and Assured Deletion", IEEE Transcations on dependable and secure computing, VOL. 9, NO. 6, NOVEMBER/DECEMBER 2012
[19] G. Wang, Q. Liu, and J. Wu, "Hierarchical attribute-based encryption for fine-grained access control in cloud storage services," in ACM CCS, , pp. 735–737, 2010
[20] Y. Tang, P.P.C. Lee, J.C.S. Lui, and R. Perlman, "FADE: Secure Overlay Cloud Storage with File Assured Deletion," Proc. Sixth Int'l ICST Conf.Security and Privacy in Comm. Networks (SecureComm), 2010
[21] R. Perlman, "File System Design with Assured Delete," Proc. Network and Distributed System Security Symp. ISOC (NDSS), 2007
[22] Ruj, A. Nayak, and I.Stojmenovic, "DACC: Distributed access control in clouds," in IEEE TrustCom, 2011
[23] A. Rahumed, H.C.H. Chen, Y. Tang, P.P.C. Lee, and J.C.S. Lui, "A Secure Cloud Backup System with Assured Deletion and Version Control," Proc. Third Int'l Workshop Security in Cloud Computing, 2011
[24] S. Yu, C. Wang, K. Ren, and W. Lou, "Attribute Based Data Sharing with Attribute Revocation," Proc. Fifth ACM Symp. Information, Computer and Comm. Security (ASIACCS), Apr. 2010
[25] W. Wang, Z. Li, R. Owens, and B. Bhargava, "Secure and Efficient Access to Outsourced Data," Proc. ACM Workshop Cloud Computing Security (CCSW), Nov. 2009
[26] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-Policy Attribute-Based Encryption," Proc. IEEE Symp. Security and Privacy, May 2006
[27] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data," Proc. ACM Conf. Computer and Comm. Security, pp. 89-98, 2006.
[28] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-Policy Attribute-Based Encryption," Proc. IEEE Symp. Security and Privacy, pp. 321-334, 2007.
[29] A.B. Lewko and B. Waters, "Decentralizing Attribute-Based Encryption," Proc. Ann. Int'l Conf. Advances in Cryptology (EUROCRYPT), pp. 568-588, 2011.
[30] "Libfenc: The Functional Encryption Library,"http://code. google.com/p/libfenc/, 2013.
[31] W. Wang, Z. Li, R. Owens, and B. Bhargava, "Secure and Efficient Access to Outsourced Data," Proc. ACM Cloud Computing Security Workshop (CCSW), 2009.
[32] J. Hur and D. Kun Noh, "Attribute-Based Access Control with Efficient Revocation in Data Outsourcing Systems," IEEE Trans. Parallel and Distributed Systems, vol. 22, no. 7, pp. 1214-1221, July 2011.
[33] C.Gentry, "A fully homomorphic encryption scheme", *Ph.D. dissertation, Stanford University, 2009, http://www.crypto.stanford.edu/craig.*
[34] personal M. Li, S. Yu, K. Ren, and W. Lou, "Securing health records in cloud computing: Patient-centric and fine-grained data access control in multi owner settings," in *SecureComm, pp. 89–106, 2010.*
[35] S. Yu, C. Wang, K. Ren, and W. Lou, "Attribute based data sharing with attribute revocation," in *ACM ASIACCS, pp. 261–270, 2010.*
[36] S. Jahid, P. Mittal, and N. Borisov, "EASiER: Encryption-based access control in social networks with efficient revocation," in *ACM ASIACCS, 2011.*
[37] F. Zhao, T. Nishide, and K. Sakurai, "Realizing fine-grained and flexible access control to outsourced data with attribute-based cryptosystems," in *ISPEC*, ser. Lecture Notes in Computer Science, *vol. 6672. Springer, pp. 83–97, 2011.*

Author Profile

Pooja R. Vyawhare received the B.E. degrees in Computer Science & Engineering from Sipna College of Engineering & management in 2013. Now she is pursing ME (CSE) from P. R. Pote (Patil) College of Engineering & management Amravati, Maharashtra, India

Ms. N. D. Ghuse received the B.E. degrees in Computer Science & Engineering from Sipna college of Engineering & Management in 2005 and completed ME (CSE) from Prof. Ram Meghe College of Engineering & management. Amravati, Maharashtra, India