Privileged Document Access In Google Cloud Environment

[1]Miss. S.V. Sarode,[2]Prof. K.N.Shedge
[1]PG student, [2]Assi. Professor
[1]Computer Engineering Department,
[1]SVIT, Chincholi, Sinner, Nashik, India

***Abstract*— In many situations users suffers from misbehaviors of cloud services as it breaks the security perimeter. Due to impropriety, user loses control over data and there exist a reasonable security issues that negligible adoption of Cloud computing. A rule-based access control (RBAC) technique is proposed to restrict system access for authorized users. It is data-centric security approach in which policy control mechanism defined around roles and privileges. The roles are created for different job functions. The permission to perform certain operations is assigned to particular roles. The primary rules are: Role assignment, Role authorization and permission authorization. It gives the role and resource hierarchy support with high expressiveness. Logical formalization offer by semantic web technologies can enables advanced rule management. RBAC is integrated within Google services. System will contribute modifications and deletion of document.**

***IndexTerms*— Data-centric security, Cloud computing, Role-based access control, AuthorizationData-centric security, Cloud computing, Role-based access control, Authorization**

I. INTRODUCTION

A concept of Re-encryption where `a' and `b' is the key pair. Now proxy can re-encrypt a ciphertext `Ca' that previously encrypted under the `a' public key to another `Cb' which can further decrypted using private key `b'.

Identity Based encryption scheme: It is public key cryptography techniques uses key pair for given entity are generated based on identify of that entity. IBE avoids the need to generate and manage public and private key for every authorization element. MSK is Master Secret Key is used to generate secret keys from identities. In this approach user can encrypt piece of data using identity to obtain cipher-text under identity.

IBPRE scheme is as authorization solution which is not tied to any PRE scheme. As IBE contains key pair which could be key generate and management problem therefore, only pure PRE scheme can be better solution. Data centric security: If user wants to retrieve data from cloud server then it should be evaluated by CSP upon an access request in order to decide whether such a request is permitted or not. Data centric authorization has self protection mechanism that assures data can only accessed by authorized subject according to rules of data owner.

SecRBAC is a data-centric access control solution for self-protected data that can run in untrusted CSPs. It can provide extended Role-Based Access Control expressiveness. It provides a rule-based approach following the RBAC scheme, where roles are used to ease the management of access to the resources. This approach can help to control and manage security and to deal with the complexity of managing access control in Cloud computing. A data centric approach SecRBAC is used for self protection in which some novel cryptographic techniques are used such as, PRE (Proxy-Re-encryption), IBE (Identity Based Encryption) and IBPRE (Identity Based Proxy Re-encryption). This technique allows re-encrypt data from one key to another without getting access and to use identities in cryptographic operations, it also allows protecting both data and authorization model. Each piece of data is ciphered with its own encryption key linked to the authorization model and rules are cryptographically protected to preserve data against the service provider access or misbehavior when evaluating the rules. It also combines a user-centric approach for authorization rules, where the data owner can define a unified access control policy for his data. A rules-based approach can use for user authorization in which rules are under the control of data owner and access control computations is outsourced to the CSP. From an authorization point of view, this can be seen as a simple rule where only the user with privilege to access the data will be able to decrypt it. However, no access control expressiveness is provided by this approach. Only that simple rule can be enforced and just one single rule can apply to each data package. Thus, multiple encrypted copies should be created in order to deliver the same data to different receivers. Problem to generate more data copies that can be further delivered to other receiver. To cope with this issue SecRBAC utilized a data centric approach. Existing schemes are Key-Policy ABE (KP-ABE) and Ciphertext-Policy ABE (CP-ABE).Then, the key issuer just asserts the attributes of users by including them in private keys. However, either in KP-ABE or CP-ABE, the expressiveness of the access control policy is limited to combinations of AND-ed or OR-ed attributes. RBAC may require the definition of a large number of roles for fine-grain authorization. ABAC is also easier to set up without need to make an effort on role analysis as needed for RBAC. On another hand, ABAC may result in a large number of rules since a system with n attributes would have up to 2 n possible rule combinations. ABAC separates authorization rules from user attributes, making it difficult to determine permissions available to a particular user, while RBAC is deterministic and user privileges can be easily determined by the data owner.

II. RELATED WORK

J.M. Marin Perez et al [1], presented a SecRBAC approach. It is data centric approach which gives access control solution with enhanced role-based expressiveness. It concerned on security of user data careless by cloud service provider. In proposed authorization model a novel identity based re-encryption technique is referred for security purpose. Authorization model gives the high oration with resource and role hierarchy. Discussed solutions depict logical formalization given by Semantic Web Technologies.

The proprietary company, partner organizations provide access rights to the resources are managed and administered. It permits the consistent definition of permissions, dynamic roles etc. across all connected systems. SPML (Service Provisioning Markup Language) technique gives validity proof of documents. It can be attempted to map the deployment requests generated by this approach to structures defined in SPML.An attribute authorization of requested system might be invalid and it is defined as future scope [2].

A cryptosystem for fine-grained sharing of encrypted data is developed which is also call as, Key-Policy Attribute-Based Encryption (KP-ABE). In cryptosystem ciphertexts are identify with sets of attributes and private keys are associated with access structures. The applicability of their construction to sharing of audit-log information and broadcast encryption is also demonstrated. The development supports delegation of private keys which subsumes Hierarchical Identity-Based Encryption (HIBE). Hiding the set of attributes is open challenge remain in this scheme[3].

ABE i.e. attribute based encryption a scheme is discussed in paper [4]. Deployment of Cloud application is depends on several factors like load balancing, bandwidth, data size and security. Access into the cloud environment is determined by the access control techniques provided by the cloud service provider. Several attacks like insider attacks, collusion attack, and denial of service attacks occurred due to weak access control technique. It is necessary for a cloud environment to have an access control policy to give fine grained and scheduled access to users. Multiple access control policies available for cloud computing ranging from Discretionary access control (DAC), Mandatory Access control (MAC), Role based access control (RBAC) and Attribute based encryption access control (ABAC). Each of these access control has been designed for policy neutral, administrative convenient access design .The imperative properties of DAC and MAC are combined together to get RBAC. While DAC is user discretionary, MAC is based on lattices. In this paper the comparison table of various ABE based schemes based on various features such as computation overhead, decryption and user revocation efficiency, collusion resistant, application relevancy, association of attributes and association of access policy in a five scale rating form is given [6].

A mechanism for realizing CP-ABE under the concrete and non-interactive cryptographic assumptions is represented in [5]-[7]. It embeddings LSSS challenge matrix directly into the public parameters. There are three constructions are proposed, first is the system proven selectively secure under assumption that is also known as decisional Parallel Bilinear Diffie-Hellman Exponent (PBDHE) assumption which can be viewed as a generalization of the BDHE assumption.

Ciphertext-Policy ABE (CP-ABE) scheme is the form of ABE. In this policies are associated with encrypted data and attributes are associated with keys. In work they focused on improving the flexibility of representing users attribute in key. A design of efficient CP-ASBE schemes that is secure in the standard model and extending CP-ASBE to a multi-authority setting [8]. In final process they applied Proxy-reencryption and lazy re-encryption techniques to developed scheme. In future work they were mentioned that to design more expressive scheme, which can be proved to have full security under the standard model with best performance. A Hierarchical Attribute Set Based Encryption (HASBE). It is implemented using cipher text policy by encrypting and decrypting the data in the cloud therefore, cloud system become more flexible and scalable by enforcing data owners to share their data with data consumers controlled by the domain authority.

Role-Based Access Control Models is mostly known as, ``RBAC''. A pure RBAC technique gives an inadequate support for dynamic attributes such as time of day, which might need to be considered when determining user permissions. An appropriate trade-off retains the benefits of RBAC while extending its utility into distributed application. RBAC control model includes the attribute in access control model [9].

ABAC and RBAC schemes are similar having specific merits and demerits. Significantly, current research in this topic includes the Role-Centric Attribute-Based Access Control (RABAC) has realized one of the first reference models combining both roles and attributes in a reliable manner that preserves the best features of both access control methods. Commercial implementations are also developing that use both role-centric and dynamic role capabilities combined with the features of ABAC's fine-grained authorization, demonstrating that the approach defined by ANSI/INCITS 494-2012 is practical, and can combine the best features of RBAC and ABAC for the enterprise[10].

Although efficiently computable, the wide-spread adoption of BBS re-encryption has been hindered by considerable security risks. Proxy re-encryption allows proxy to transform a ciphertext computed under user `X' public key into one that can open by other user `Y's secret key. Several applications of proxy re-encryption such as, secure file system, outsourced filtering of encrypted form etc. To improve re-encryption schemes they introduced the concept of bilinear maps. It is pairing based scheme realized important new features [11].

An identity based encryption scheme is secure against the adaptive chosen identity and chosen plaintext attack in the standard model. An efficiency of the lattice-based IBE scheme, unlike the identity string is encoded into a matrix by a group of public matrices in several known constructions, the identity string of l bits is encoded into a vector with the help of l + 1 vectors in this paper. As a result, the public key size of the proposed scheme is shorter than that of the known constructions of the lattice-based IBE scheme. There are still many open problems which need to be studied in the lattice-based IBE scheme, such as how to design a lattice-based HIBE in the standard model by their design techniques [12].

O.K. Jasim Mohammad, represented a development of AES i.e. advanced encryption standard algorithm. Their main aim is focused on combination of AES and S-Boxes. In this specific key generated from quantum key distribution. Symmetric ciphertext is divided into two broad categories such as, block cipher and stream cipher. AES algorithm uses individual key for encryption and

decryption. Basically, key length is defined as, 128; 192; 256- bits. Quantum Key Distribution (QKD) technology is also known as, Cerberis, it offers entire new approach for network security based approach on fundamental principle of quantum physic. QAES merges AESNIST which is high speed encryption with quantum key distribution. QAES development does not deny security of the AES algorithm [13].

R. Bobba, et al [14], introduced Ciphertext-Policy ABE (CP-ABE). It is the form of ABE in which policies are correlated with encrypted data and attributes are associated with keys. They were focusing on to improve flexibility of user attributes in keys. A prototype implementation is provided in this paper to evaluate performance overhead. Interesting direction for future work is predicted for the study of potential of CP-ASBE approaches.

G.Wang et al[15], proposed fine-grained cryptographic approach. In this approach decryption keys are disclosed only to authorize user. The proposed scheme helps enterprises to efficiently share sensitive data on cloud servers. In this HIBE i.e. hierarchical identity-based encryption and CP-ABE ciphertext-policy attribute-based encryption combined and further, performance-expressivity tradeoff is applied on it. It has several qualities such as, high performance, scalability, fine-grained access control etc. In future work they predicted to work for improvement of complete security under standard model with better quality performance.

III. PROBLEM DEFINITION

Many large organization, business firms outsourced their data to the cloud to avoid headache of data management. Now days, there are certain security challenges arrives in cloud environment as it breaks the organizations bounds. There is need of such system in which user has self control on their cloud stored data.

To design develop and test a system to provide google cloud storage services with encryption and authorization technique.

IV. SYSTEM ARCHITECTURE

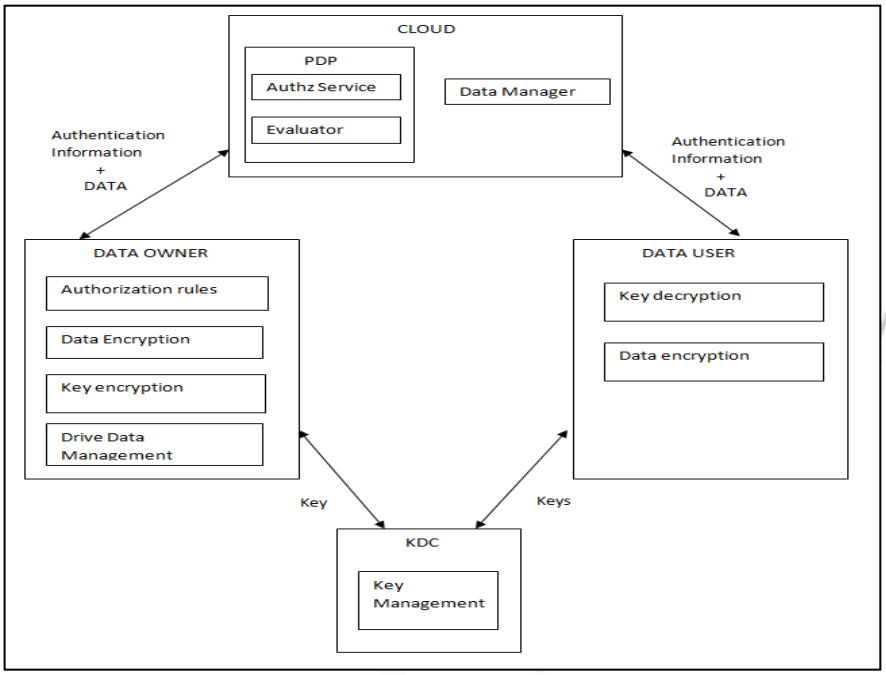

Figure 1 System Architecture

Figure 1 Fig. 1 represents the system architecture diagram of proposed system. It contains the modules as, cloud, Key distribution center-KDC, user and data owner.

1. **Data owner:**
   Data owner consists of data objects, authorization rules, Data encryption, keys encryption and drive management. In order to prevent CSP from accessing data object, it is uploaded in encrypted on cloud and manage keys on key distribution centers.
   - **Data Encryption:** This approach follows a symmetric encryption algorithm (e.g. AES) to protect the data object itself. The encryption of data is done with a random symmetric key generated for the purpose of a single encryption.
   - **Authorization Rules:** It is defined by data owner and mapped with the authorization model in cloud. It consists of corresponding elements in the binary relations. It consist of user identity, access privileges , data mapping.
   - **Keys Encryption:** It is generated by rkgen() for authorization rule. Only data owner can generate them by Master Secret Key and the identities of the involved authorization elements. The key encryption can be considered as cryptographic tokens provided by data owners in order to enable to perform operations over the authorization model. That is, a CSP will not be able to effectively apply any rule that has not been legitimately defined by the data owner. The encrypted keys are distributed using KDC center to the data user.
   - **Drive data Management:** This module is responsible for data management at cloud end. owner can modify or delete the data present on cloud and respective keys from KDC server.

2. **Cloud:**
Cloud is responsible for user authentication and data management. It includes 2 modules: **Policy Decision Point**-PDP and data manger.
   - **Data centric approach:** Applying this data-centric approach results in self contained protected object, which can be released to the Cloud and only authorized users could access the data object. This can be useful for Inter-cloud scenarios, where data can travel through different CSPs.
   - **Policy Decision Point (PDP):** It manages the authorization model and proxy re-encryptor.
   - **Authz Service:** An authorization service act as entry point to PDP for Cloud services allow to query it for authorization decisions. This module takes decisions upon a request from a user to access to a piece of data managed by the service. These decisions usually return an access granted or denied statement. For granted accesses, the response also contains the re-encryption chain that should be applied, together with the needed re-encryption keys.
   - **Data Manager:** Data manager is responsible for managing data on cloud. An provide previlages access to the user as per authorization rights provided.

3. **KDC:** KDC is responsible for key management and distribution. This is a server preserves data access keys with authorization rights.

V. ALGORITHM:

Input: p: prime number, s: secret, M : secret message
Output: Encryption key K, Cipher text-C, ReKey-Rk, Encrypted key-Rc, Decrypted message-Dm(Equal to M)
Processing
1: Setup(p, s)→ msk
2: KeyGen: (p, msk)→ K
3: Encryption(K, M)→ C
4: ReKeyGen(msk, Au)→ Rk
4: Key-encryption(msk, Rk)→Rc
5: Decryption: (Rc, Au, C)→ Dm

VI. EXPERIMENTAL EVALUATION

System is developed using Google auth service[16]. This service allows user to deal with Google document. A Google project is created with API key. This key is configured in java project to communicate with the Google docs.
Dataset: A synthetic dataset is generated containing files of different types such as: text, audio, video, images and zip files. All files sizes are varies from 1 KB to 5 MB.
Performance Measures:

a) Efficiency: System efficiency is compared with respect to the following parameters: Encryption Time: AES 256 with random keys is used to encrypt the document. Time will be calculated for key generation, encryption and decryption process for different types of files with various sizes.
b) Upload time: Time required for uploading a document on Google docs with different sizes will be calculated
c) Authorization Decision Time: For document uploading server side connection setup authorization time will be calculated.

Following Table 1 represents the time required for Encryption processing. For testing text, Image, audio, video and compassed Files are considered. Compressed file contains the combination of all file types. Compression file require higher time than other type of files.

Table 1 Encryption Time

File Size IN MB	Text Encryption(Time in Sec)	Image Encryption(Time in Sec)	Audio Encryption(Time in Sec)	Video Encryption(Time in Sec)	Zip Encryption(Time in Sec)
1	1.64	1.68	1.72	1.79	1.85
2	2.69	2.62	2.93	2.95	3.2
3	3.93	3.62	4.06	4.03	4.27

Following table 2 represents the time required for data decryption for all type of files. Compressed file requires higher time than other type of files.

Table 2 Decryption Time

File Size IN MB	Text Decryption(Time in Sec)	Image Decryption(Time in Sec)	Audio Decryption(Time in Sec)	Video Decryption(Time in Sec)	Zip Decryption(Time in Sec)
1	0.68	0.73	0.77	0.78	0.91
2	1.03	1.02	1.05	1.19	1.24
3	1.68	1.66	1.69	1.72	1.93

Following table 3 represent the communication time for user authorization process, data upload, and download. Authorization time is independent of file size. This authorization is done for every cloud transaction.

Table 3 Server Communication Time

File Size IN MB	Authorization Time(Time in Sec)	Upload Time(Time in Sec)	Download Time(Time in Sec)
5	1.2	2.04	2.45
10	0.9	3.62	3.51
15	1.1	4.46	4.86
20	1.1	5.98	6.32

Figure 2 represents 3graphical results for system evaluation time mentioned in table 1, 2 and 3 respectively. Graph 1 represents the encryption time for various file sizes. Graph 2 represents the time required decryption for various file sizes. File are of various types such as: text, image, audio,video. Graph 3 represents server communication time for user authorization, upload and download.

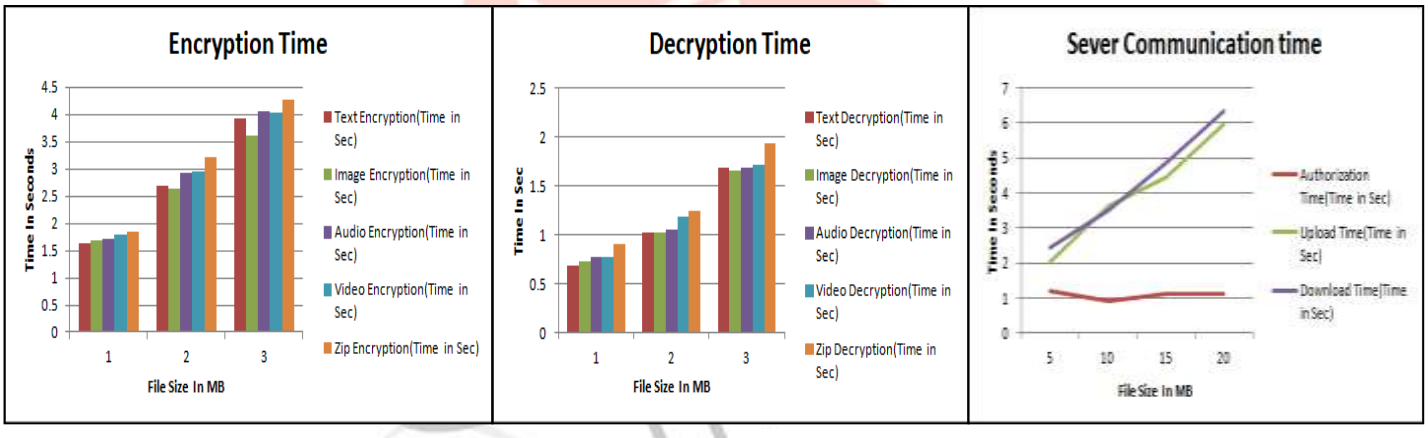

Figure 2 System Results

Following table represents the comparative study of proposed approach with existing system techniques. The checked icon represents the facility provided in the system.

Table 4 System Comparison

	Data Encryption	Google Cloud	Auth Service	Key Management	Data Updation	Data Deletion
Privileged Document Access In Google Cloud Environment(Our Approach)	☑	☑	☑	☑	☑	☑
SecRBAC: Secure data in the Clouds[1]	☑	☑	☑			
Attribute-based encryption for fine-grained access control of encrypted data[17]	☑			☑		

VII. CONCLUSION

A novel identity-based and proxy re-encryption techniques are used to protect the authorization model. Data is encrypted and authorization rules are cryptographically protected to preserve user data against the service provider access or misbehavior. The authorization model provides high expressiveness with role hierarchy and resource hierarchy support. The solution takes advantage of the logic formalism provided by Semantic Web technologies, which enables advanced rule management like semantic conflict detection. A proof of concept implementation has been developed and a working prototypical deployment of the proposal has been integrated within Google services. Key management and delegation is done using third party key distribution server. System provide data modification and deletion facilities to the end user.

REFERENCES

[1] J. M. Marin Perez, G.M. Perez, ``SecRBAC: Secure data in the Clouds ," IEEE transaction on service computing, vol. 99, pp. 1-1, april 2016.

[2] A.Lawall, D. Reichelt, and T. Schaller, ``Resource management and authorization for cloud services," in Proceedings of the 7th International Conference on Subject-Oriented Business Process Management, ser. S-BPM ONE '15, New York, NY, USA, 2015, pp. 18:1–18:8

[3] G. Wang, Q. Liu, and J. Wu, ``Hierarchical attribute-based encryption for fine-grained access control in cloud storage services," in Proceedings of the 17th ACM Conference on Computer and Communications Security, ser. CCS '10, New York, NY, USA, 2010, pp. 735–737.

[4] B and V. P, ``Extensive survey on usage of attribute based encryption in cloud," Journal of Emerging Technologies in Web Intelligence, vol. 6, no. 3, 2014.

[5] B. Waters, ``Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization," in Public Key Cryptography - PKC 2011, 2011, vol. 6571, pp. 53–70.

[6] R. Bobba, H. Khurana, and M. Prabhakaran, ``Attribute-sets: A practically motivated enhancement to attribute-based encryption," in Computer Security - ESORICS 2009. Springer Berlin Heidelberg, 2009, vol. 5789, pp. 587–604.

[7] G. Wang, Q. Liu, and J. Wu, ``Hierarchical attribute-based encryption for fine-grained access control in cloud storage services," in Proceedings of the 17th ACM Conference on Computer and Communications Security, ser. CCS '10, New York, NY, USA, 2010, pp. 735–737.

[8] J. Liu, Z. Wan, and M. Gu, ``Hierarchical attribute-set based encryption for scalable, flexible and fine-grained access control in cloud computing," in Information Security Practice and Experience. Springer Berlin Heidelberg, 2011, vol. 6672, pp. 98–107

[9] R. Kuhn, E. J. Coyne, and T. R. Weil, ``Adding attributes to rolebased access control," Computer, vol. 43, no. 6, pp. 79–81, 2010.

[10] Coyne and T. R. Weil, ``Abac and rbac: Scalable, flexible, and auditable access management," IT Professional, vol. 15, no. 3, pp. 14–16, 2013.

[11] Ateniese, K. Fu, M. Green, and S. Hohenberger, ``Improved Proxy Re-encryption schemes with applications to secure distributed storage," ACM Transactions on Information and System Security, vol. 9, no. 1, pp. 1–30, 2006.

[12] Wang, Z. Liu, and C. Wang, ``Full secure identity-based encryption scheme with short public key size over lattices in the standard model," Intl. Journal of Computer Mathematics, pp. 1–10, 2015

[13] O. K. J. Mohammad, S. Abbas, E. M. El-Horbaty, and A. M. Salem, ``Innovative method for enhancing key generation and management in the aes-algorithm," CoRR, vol. abs/1504.03406, 2015.

[14] R. Bobba, H. Khurana, and M. Prabhakaran, ``Attribute-sets: A practically motivated enhancement to attribute-based encryption," in Computer Security - ESORICS 2009. Springer Berlin Heidelberg, 2009, vol. 5789, pp. 587–604.

[15] G. Wang, Q. Liu, and J. Wu, ``Hierarchical attribute-based encryption for fine-grained access control in cloud storage services," in Proceedings of the 17th ACM Conference on Computer and Communications Security, ser. CCS '10, New York, NY, USA, 2010, pp. 735–737.

[16]https://developers.google.com/drive/v3/web/quickstart/java

[17] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in Proceedings of the 13th ACM Conference on Computer and Communications Security, ser. CCS '06, New York, NY, USA, 2006, pp. 89–98.