A Dynamic Cross-Domain Access Control Model for Collaborative Healthcare Application

Ahmad Salehi S.*†, Carsten Rudolph* and Marthie Grobler†
*Monash University, Melbourne, Australia
†CSIRO's Data61, Melbourne, Australia
*Email:{ahmad.salehishahraki and carsten.rudolph}@monash.edu
†Email:{ahmad.salehishahraki and marthie.grobler}@data61.csiro.au

***Abstract*—Authorization models have become a hot topic for debate in recent years because of sharing healthcare data among different resources. Although authorization models have been developed and applied to various applications to prevent unauthorized access to sensitive healthcare data, there is no system model on cross-domain access control and combined context of team collaboration and workflow. This paper describes a cross-domain healthcare scenario based on current issues and interaction of relevant entities. This work has led us to propose a new fully decentralized access control framework for a dynamic cross-domain authorization model, where this framework is policy based to meet the requirements of cross-domain in healthcare environments.**

Keywords–anonymity, attribute-based access control (ABAC), cross-domain, distributed environments, healthcare, privacy, security.

I. Introduction

An increasing global population combined with rapid development of technologies generate enormous amounts of data in healthcare institutes and devices [1]. These sensitive data may be shared with different users in different domains, such as health professionals and healthcare service providers (HSPs) in different hospital settings [2]. These stakeholders use the data to improve the treatment and quality of life of patients [3]–[6].

The sensitive data are stored and shared over different storage systems such as hospitals with the goal of providing better and safer treatment [7]–[9]. The data must comply with relevant healthcare standards and requirements [10]–[12] to ensure privacy of shared healthcare data.

The current situation is that data is held by separate entities and various policies and access control mechanisms are used to prevent malicious and unauthorized access to data by insiders or outsiders. Cross-domain access is restricted to mechanisms for the explicit sharing of particular pieces of information. Approaches to provide wider access are either based on centralized storage or require synchronized cross-domain policies. Centralized data creates huge risks for privacy breaches or attacks affecting the complete set of available data. Furthermore, entities would need to give up data sovereignty and a highly trusted entity needs to be established to control access, i.e. decide on and enforce policies.

978-3-903176-15-7

In order to provide and receive healthcare services, users and patients need to register in a local domain. Thus, there needs to be a process to identify a person. A distributed cross-domain access control model can rely on this identification process to provide cross-domain identity information. The goal of developing a cross-domain model is to restrict any central authority to this minimal role of identification and then satisfy fundamental security requirements.

In this paper, we briefly look at the history and background of access control models and their limitations, which helps to understand the concept of existing access control models. We next discuss access control concepts and existing studies and investigate the interactions and cooperation between different entities in cross-domains. We then focus on two aspects of a network model that result from centralized and decentralized scenarios to identify the effects of these relationships on access control models. To overcome the identified access control challenges, we propose a novel access control model, the dynamic cross-domain attribute-based group signature (DCD-ABGS). This model can identify and support users and their need to access data to meet cross-domain requirements. Additionally, the proposed model guarantees the privacy of attributes and prevents user and attribute collusion, as well as impersonation attacks. To our knowledge, this is the first study to propose a fully decentralized access control model based on real healthcare systems and prevent unauthorized user access in cross-domains.

This paper is organized as follows. Section II discusses current related work. Section III presents the system model and security requirements. Section IV discusses our proposed model. Section V makes some conclusions and mentions future work.

II. Related Work

We investigate and review the cross-domain suitability of traditional and cryptographic access control models.

A. Traditional ABAC Model

In the attribute-based access control mode (ABAC) [13], [14] users' attributes are formulated and common attributes can be defined to provide trust between domains. Based on this model, a hierarchical group ABAC framework was proposed to assign the attributes based on each group [15].

John et al. [16] proposed a multi-domain approach by reducing the number of rules and permissions. This model was extended by Faber et al. [17] to include policy delegation. This model was revised to an administrative authorization model [18] using the hierarchical group ABAC concept making it suitable for large environments. The multi-tenant ABAC access control model [19] was proposed to minimize the complexity of the system uing the concepts proposed by [20], [21]. Additionally, risk-adaptive access control (RAdAC) [22] and the quantitative ABAC authorization model was proposed [23] to rank the attributes based on their priority and condition as well as target.

Several variations of ABAC models have been proposed and applied in a variety of scenarios [15], [21], [24]–[31]. The focus is on improving efficiency, scalability, and ease of configuration, but no unique architecture of these can be applied in multi-domain scenarios.

B. Cryptography Approach

Several cryptographic models have been proposed to grant users access to particular resources in single and multi-domains [32]–[34].

1) Attribute-based encryption (ABE): ABE is a well-known cryptographic primitive for data access control and flexible for a multi-domain approach. ABE was initially called fuzzy identity-based encryption (IBE) [35], [36]. Several ABE models were later proposed as improvement, but these do not perform well in multi-domain scenarios. Data access control in multi-domains was proposed [37], [38] where each domain is responsible for generating its attributes and a central authority handles the domain's attributes; however, these models lack in revocation. The DBMask model enforces policies based on user attributes [39]. Li et al.'s model is similar and aims at addressing key dependency issues while one authority is compromised [40], [41]. To achieve confidentiality of outsourced sensitive data and attribute privacy, a new framework based on attribute Bloom filter (ABF) was proposed [32].

2) Attribute-Based Signature (ABS): It was introduced by Shanqing [42] and extended further using the advantages of ABE and digital signature [43], [44]. A multi-authority access control scheme was further proposed [33], [45], [46], in which the central authority is responsible for managing the required parameters for entities. However, the computation cost and communication overheads is high and is dependent on a trusted third-party.

3) Attribute-Based Group Signature (ABGS): ABGS is a cryptographic technique that uses a combination of ABS [42], [46] and group signatures [47], which allows users to belong to one domain anonymously and to sign messages. The anonymity of users who sign the message was introduced [48] and then extended to achieve revocation [49], [50]. These works were extended to propose a new general framework based on ABAC to achieve user and attribute anonymity as well as full traceability within the same group [51], [52].

4) Searchable Encryption (SE): To ensure the identity of trusted third parties in the cloud and to authorize the user according to their request, several models referring to authorized private keyword searches was proposed [53], [54] with the aim of searching on encrypted data in a database. A method called ABE-EAKS was developed using the concept of ABE and SE to create expressive and authorized keyword searches [34] where the keyword must satisfy the policies for searching on the server side. Another authorization model [55], [56] have been proposed to address the issue of a single contributor; however, the model has problems with policy management.

III. System Model And Security Requirements

In this section, we propose a system model based on the ABAC approach for healthcare applications and then explain the threat model as well as the requirements of the proposed model.

A. ABAC System Model

In ABAC, access to resources is granted by evaluation of policies and attributes of the subject, object, environment, and action. In general, the subject sends the request to access the particular resources in a single domain [12]. Access is granted based on policies defined by the system and entity attributes. This provides a better access control model with greater flexibility; however, it cannot be applied in cross-domains with multiple security and privacy requirements [12].

The following are the main components of the ABAC standard introduced by the National Institute of Standards and Technology (NIST) [12]: 1) policy decision point (PDP); 2) policy administration point (PAP); 3) policy information point (PIP); and 4) policy enforcement point (PEP) (Fig. 1) [12].

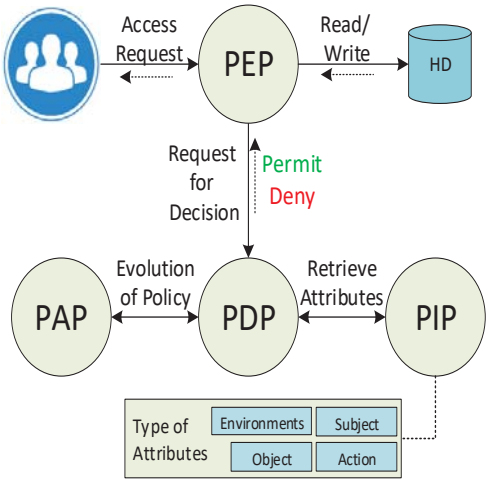

Fig. 1. NIST access control framework [12].

B. Healthcare System Model

The model of healthcare systems that we introduce relates mainly to hospital environments, where each hospital is assumed to constitute one domain with their own security

and privacy requirements. For this, we consider a number of healthcare domains such as Hospital 1, 2, 3, etc. each including several patients and users. These domains are responsible for providing a variety of healthcare services. We assume that each patient and user belong to one healthcare domain. The related patient data are stored in the local healthcare database (HD) in the hospital and are made accessible through sharing with other HSPs. The HSPs in the same or a different domain may access classified information according to their duties and responsibility. The architecture of the system model is presented in Fig. 2.

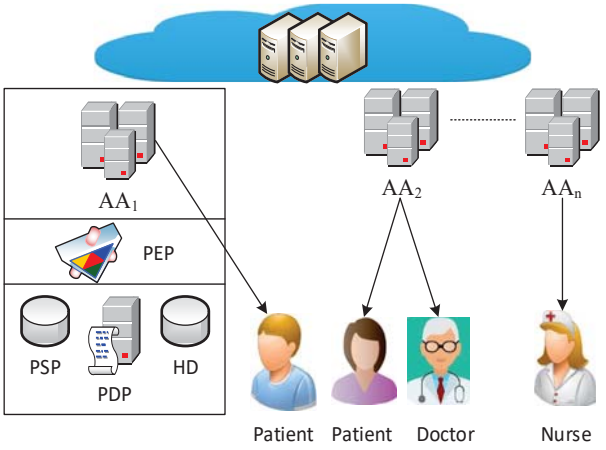

Fig. 2. Cross-Domain System Model.

The relevant components of the proposed model are as follows.

- Home healthcare domain (HHD): We consider several hospitals as a healthcare domain. Each comprises the patient, HSP, policy storage (PS), PEP, HD, and attribute authority (AA) components.
- Foreign healthcare domain (FHD): The FHD is a secondary healthcare domain, such as Hospital 2 with same functionality as HHD.
- Attribute authority (AA): The AA acts as the manager of either an HHD or FHD, working under the national and local laws and regulations of its domain.
- Healthcare database (HD): The HD is the storage component that stores the data in the local domain (HHD) for further services.
- Access structure (τ): The τ includes a group of attributes and policies that need to be satisfied by the access request to grant the user access to particular resources.

C. Threat Model

We introduce the threat model used in this research study to test our system model. The AA is assumed to be trusted by its local domain and is responsible for generating the necessary domain parameters and verifying and validating the identity of legitimate users in the cross-domain. The AA may collapse as a result of an attack where an adversary may try to obtain particular parameters such as attributes and key parameters; this is called a collusion attack. An adversary may try to compromise the AA to obtain secret information. With the illegal user trying to obtain access to resources without real authorization. The compromised AA will try to verify the user as a legal or illegal user. This is called a colluding user attack. A user can forge the attribute, which may allow access to any particular data.

D. Security Requirements

The proposed model attempts to meet the following security requirements.

- Collusion resistance: The attacker should not be allowed to use the attributes to decrypt messages or delegate to illegal domain authorities.
- Attribute anonymity: The verifier must be able to verify a user's signature in an authentication process without revealing any attributes.
- Signature privacy: The model should not reveal any attributes.
- Dynamic change: This property is required when a user dynamically joins or leaves a domain.
- Attribute collusion: It is important to prevent users in the same and different domains from using the same attributes for their access model.
- User anonymity: This property is required to secure the privacy of users while sending requests to access health data in the home authority.
- Elective revolution attribute: The least number of attributes should be used in access control models, while satisfying the τ defined by the patient.
- Traceability: Traceability is required for controlling and checking both the user and AAs are valid and issued by the correct AA.

E. Our Proposed ABAC Approach: DCD-ABGS

In our proposed model, the system initialization must first be set up with the necessary parameters, such as the attributes, public and private parameters and signature within and between AAs. An attribute key distribution based on the proposed system model is then required to permit the O (patient) and U (doctor and nurse) to receive the appreciate set of attributes and parameters from their respective AAs.

Generally, in this model, the attribute key distribution is divided into sections in which the first is the attribute key distribution to assign the attribute to the O and U via their AA. For this to happen, our system architecture is based on the concept of the cross-domain presented in Fig. 2. The HHD is called the home domain and is where the patient (O) is located and where his/her data are stored. The FHD is a foreign domain, such as the location of an HSP or other user (U). This idea is abstracted and observed from the roaming model [57]. At this stage, it is mandatory for both O and U to register in their respective AA. Each AA is responsible for generating the necessary parameters such as the attributes and either private

or public keys. This occurs independently in our system model without relying on any global or central authority.

Therefore, a direct connection between O and U with their respective AA is required when U from AA_2 requests access to the data for O in AA_1. To do this, the construction and concept of the group signature proposed by [50]–[52] will be used for mutual authentication. Additionally, a secure channel between the AAs (HHD and FHD) is required before the exchange of any attributes. In our model, the access decision happens in the HHD, which requires the U from an FHD to communicate securely with the authorization system in the HHD. For this, we considered the idea of a roaming technique for authentication and direct connection between AAs. We adopted our system model based on the roaming technique [57], [58] and group signature model [51], [52]. Based on the idea of roaming and group signature technique, the HHD acts as a domain manager and the FHD acts as a user member of group. This means that AA_2 can sign and AA_1 can validate AA_2 by verifying the signature during the authentication process using master and public keys. AA_1 is the group manager that controls the parameters in the cross-domain. Hence, this enables AA_1 to open the signed signature by AA_2 and the user and to check their identity using delegation traceability. This prevents unauthorized disclosure of the set of attributes between AAs. To achieve this, the concept of ABGS is used to generate the signature within and between AAs for secure authentication and better access control for final decision.

Finally, the access decision made in the HHD and based on the current permission and patient's condition after evaluating the access request. The system allows the U to access the particular data only if the attributes owned by U can satisfy τ in the patient and system model. The summary of our proposed model is listed in six step as a following:

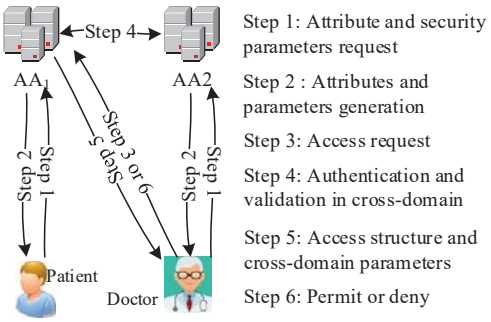

Fig. 3. Cross-Domain Key Distribution Model (DCD-ABGS).

IV. Discussion

We propose a suitable access control framework based on the use of cross-domains to meet the fundamental and security requirements, presented as the DCD-ABGS model. Our model supports the use of cross-domain, which can provide both a centralized and decentralized access control model without relying on third-party control. We investigated the concept of ABAC, roaming and ABGS approaches. This led us to propose our authorization system model, which is a fully decentralized ABAC approach that is useful for collaborative healthcare environments.

Using our proposed model, O and U remain anonymous while O stores his/her data on a local domain and the U accesses this data from a foreign domain. This enables the system to protect the privacy of the user and the HHD is unable to learn anything from the U during the authentication and authorization process. This scenario is similar for O and the domain authority as well. In addition, we achieve attribute anonymity and privacy during the authentication and authorization process. This is very important because one user may belong to a different domain, meaning that a user has several sets of attributes based on his/her activities in different domains. This also enables the system to trace the actual identity of the O, U and domain authorities.

Additionally, the proposed model and solution make our model collusion resistant in terms of attributes. The resistance to attribute collusion also prevents authorities from revealing the attributes. An impersonation attack can also be prevented because our authentication technique uses a group signature. Hence, our proposed model is fully decentralized and has the ability for dynamic authorization, which directly authorizes cross-domain users to access data without relying on a third-party and policy agreement.

V. Conclusion and Future Work

In this paper, we have presented an overview of the current state of knowledge about access control and the existing relevant models in the healthcare environment and we have discussed multiple healthcare scenarios to illustrate the current issues.

For the first time, a cross-domain framework and access control model have been proposed in a model we call DCD-ABGS. Our model is regarded as secure because the system is designed to prevent attribute collusion. Additionally, our model is fully decentralized, which allows users to access data without relying on a central authority without user privacy disclosure. We believe that our proposed DCD-ABGS scheme can overcome the problems of existing classic and cryptographic access control models and meet the security and privacy requirements in collaborative healthcare environments.

We believe that this paper proposes an appropriate access control model that are applicable in collaborative healthcare in distributed environments. Moving forward from this research paper, we plan to develop an efficient authorization protocol based on the proposed model and solution. We will evaluate the feasibility our model by applying the outcomes of this study with further security proof (e.g., attribute and user anonymity, user and domain traceability and collusion resistance attributes) and analyses. We plan to develop this model to meet the security and privacy requirements of distributed networks in real healthcare environments.

REFERENCES

[1] S. Movassaghi, M. Abolhasan, J. Lipman, D. Smith, and A. Jamalipour, "Wireless body area networks: A survey," *Communications Surveys Tutorials, IEEE*, vol. 16, no. 3, pp. 1658–1686, Third 2014.

[2] M. Beltrán, "Identifying, authenticating and authorizing smart objects and end users to cloud services in internet of things," *Computers & Security*, 2018.

[3] S. A. Salehi, M. Razzaque, I. Tomeo-Reyes, N. Hussain, and V. Kaviani, "Efficient high-rate key management technique for wireless body area networks," in *Communications (APCC), 2016 22nd Asia-Pacific Conference on*. IEEE, 2016, pp. 529–534.

[4] R. Chaudhary, A. Jindal, G. S. Aujla, N. Kumar, A. K. Das, and N. Saxena, "Lscsh: Lattice-based secure cryptosystem for smart healthcare in smart cities environment," *IEEE Communications Magazine*, vol. 56, no. 4, pp. 24–32, 2018.

[5] A. Anjum, K.-K. R. Choo, A. Khan, A. Haroon, S. Khan, S. U. Khan, N. Ahmad, B. Raza *et al.*, "An efficient privacy mechanism for electronic health records," *computers & security*, vol. 72, pp. 196–211, 2018.

[6] A. Salehi Shahraki, M. M. Razzaque, I. Tomeo-Reyes, and N. Hussain, "Ieee 802.15. 6 standard in wireless body area networks from a healthcare point of view," 2016.

[7] A. Ouaddah, H. Mousannif, A. A. Elkalam, and A. A. Ouahman, "Access control in the internet of things: Big challenges and new opportunities," *Computer Networks*, vol. 112, pp. 237–262, 2017.

[8] B. Latré, B. Braem, I. Moerman, C. Blondia, and P. Demeester, "A survey on wireless body area networks," *Wireless Networks*, vol. 17, no. 1, pp. 1–18, 2011.

[9] J. Stevovic, F. Casati, B. Farraj, J. Li, H. R. Motahari-Nezhad, and G. Armellin, "Compliance aware cross-organization medical record sharing," in *Integrated Network Management (IM 2013), 2013 IFIP/IEEE International Symposium on*. IEEE, 2013, pp. 772–775.

[10] J. Grimson, W. Grimson, and W. Hasselbring, "The si challenge in health care," *Communications of the ACM*, vol. 43, no. 6, pp. 48–55, 2000.

[11] "Guide to hipaa privacy rule and compliance," 2015. [Online]. Available: http://www.hipaa-101.com/

[12] V. C. Hu, D. Ferraiolo, R. Kuhn, A. R. Friedman, A. J. Lang, M. M. Cogdell, A. Schnitzer, K. Sandlin, R. Miller, K. Scarfone *et al.*, "Guide to attribute based access control (abac) definition and considerations (draft)," *NIST special publication*, vol. 800, no. 162, 2013.

[13] W. W. Smari, P. Clemente, and J.-F. Lalande, "An extended attribute based access control model with trust and privacy: Application to a collaborative crisis management system," *Future Generation Computer Systems*, vol. 31, pp. 147–168, 2014.

[14] W. W. Smari, J. Zhu, and P. Clemente, "Trust and privacy in attribute based access control for collaboration environments," in *Proceedings of the 11th International Conference on Information Integration and Web-based Applications & Services*. ACM, 2009, pp. 49–55.

[15] D. Servos and S. L. Osborn, "Hgabac: Towards a formal model of hierarchical attribute-based access control," in *International Symposium on Foundations and Practice of Security*. Springer, 2014, pp. 187–204.

[16] J. C. John, S. Sural, and A. Gupta, "Authorization management in multi-cloud collaboration using attribute-based access control," in *Parallel and Distributed Computing (ISPDC), 2016 15th International Symposium on*. IEEE, 2016, pp. 190–195.

[17] T. Faber, S. Schwab, and J. Wroclawski, "Authorization and access control: Abac," in *The GENI Book*. Springer, 2016, pp. 203–234.

[18] M. Gupta and R. Sandhu, "The gurag administrative model for user and group attribute assignment," in *International Conference on Network and System Security*. Springer, 2016, pp. 318–332.

[19] C. Ngo, Y. Demchenko, and C. de Laat, "Multi-tenant attribute-based access control for cloud infrastructure services," *Journal of Information Security and Applications*, vol. 27, pp. 65–84, 2016.

[20] Y. Benkaouz, M. Erradi, and B. Freisleben, "Work in progress: K-nearest neighbors techniques for abac policies clustering," in *Proceedings of the 2016 ACM International Workshop on Attribute Based Access Control*. ACM, 2016, pp. 72–75.

[21] P. Biswas, R. Sandhu, and R. Krishnan, "Attribute transformation for attribute-based access control," in *Proceedings of the 2nd ACM Workshop on Attribute-Based Access Control*. ACM, 2017, pp. 1–8.

[22] B. Farroha and D. Farroha, "Challenges of operationalizing dynamic system access control: Transitioning from abac to radac," in *Systems Conference (SysCon), 2012 IEEE International*. IEEE, 2012, pp. 1–7.

[23] A. J. Rashidi and A. Rezakhani, "A new approach to ranking attributes in attribute based access control using decision fusion," *Neural Computing and Applications*, vol. 28, no. 1, pp. 803–812, 2017.

[24] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving secure, scalable, and fine-grained data access control in cloud computing," in *Infocom, 2010 proceedings IEEE*. Ieee, 2010, pp. 1–9.

[25] S. Osborn, R. Sandhu, and Q. Munawer, "Configuring role-based access control to enforce mandatory and discretionary access control policies," *ACM Transactions on Information and System Security (TISSEC)*, vol. 3, no. 2, pp. 85–106, 2000.

[26] S. Bugiel, S. Heuser, and A.-R. Sadeghi, "Flexible and fine-grained mandatory access control on android for diverse security and privacy policies." in *USENIX Security Symposium*. Washington, DC, 2013, pp. 131–146.

[27] M. Sookhak, F. R. Yu, M. K. Khan, Y. Xiang, and R. Buyya, "Attribute-based data access control in mobile cloud computing: Taxonomy and open issues," *Future Generation Computer Systems*, vol. 72, pp. 273–287, 2017.

[28] V. C. Hu, D. R. Kuhn, and D. F. Ferraiolo, "Attribute-based access control," *Computer*, vol. 48, no. 2, pp. 85–88, 2015.

[29] R. Ahuja and S. K. Mohanty, "A scalable attribute-based access control scheme with flexible delegation cum sharing of access privileges for cloud storage," *IEEE Transactions on Cloud Computing*, 2017.

[30] R. Mahmud, R. Kotagiri, and R. Buyya, "Fog computing: A taxonomy, survey and future directions," in *Internet of everything*. Springer, 2018, pp. 103–130.

[31] N. Sultan, "Making use of cloud computing for healthcare provision: Opportunities and challenges," *International Journal of Information Management*, vol. 34, no. 2, pp. 177–184, 2014.

[32] G. Ramu, "A secure cloud framework to share ehrs using modified cp-abe and the attribute bloom filter," *Education and Information Technologies*, pp. 1–21, 2018.

[33] K. Fan, J. Wang, X. Wang, H. Li, and Y. Yang, "A secure and verifiable outsourced access control scheme in fog-cloud computing," *Sensors*, vol. 17, no. 7, p. 1695, 2017.

[34] H. Cui, R. H. Deng, J. K. Liu, and Y. Li, "Attribute-based encryption with expressive and authorized keyword search," in *Australasian Conference on Information Security and Privacy*. Springer, 2017, pp. 106–126.

[35] 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*. Acm, 2006, pp. 89–98.

[36] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in *Security and Privacy, 2007. SP'07. IEEE Symposium on*. IEEE, 2007, pp. 321–334.

[37] Z. Liu, Z. Cao, Q. Huang, D. S. Wong, and T. H. Yuen, "Fully secure multi-authority ciphertext-policy attribute-based encryption without random oracles," in *European Symposium on Research in Computer Security*. Springer, 2011, pp. 278–297.

[38] K. Yang, X. Jia, K. Ren, B. Zhang, and R. Xie, "Dac-macs: Effective data access control for multiauthority cloud storage systems," *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 11, pp. 1790–1801, 2013.

[39] M. I. Sarfraz, M. Nabeel, J. Cao, and E. Bertino, "Dbmask: fine-grained access control on encrypted relational databases," in *Proceedings of the 5th ACM Conference on Data and Application Security and Privacy*. ACM, 2015, pp. 1–11.

[40] W. Li, K. Xue, Y. Xue, and J. Hong, "Tmacs: A robust and verifiable threshold multi-authority access control system in public cloud storage," *IEEE Transactions on parallel and distributed systems*, vol. 27, no. 5, pp. 1484–1496, 2016.

[41] K. Xue, Y. Xue, J. Hong, W. Li, H. Yue, D. S. Wei, and P. Hong, "Raac: Robust and auditable access control with multiple attribute authorities for public cloud storage." *IEEE Trans. Information Forensics and Security*, vol. 12, no. 4, pp. 953–967, 2017.

[42] G. Shanqing and Z. Yingpei, "Attribute-based signature scheme," in *Information Security and Assurance, 2008. ISA 2008. International Conference on*. IEEE, 2008, pp. 509–511.

[43] S. F. Shahandashti and R. Safavi-Naini, "Threshold attribute-based signatures and their application to anonymous credential systems," in *International Conference on Cryptology in Africa*. Springer, 2009, pp. 198–216.

[44] M. Gagné, S. Narayan, and R. Safavi-Naini, "Threshold attribute-based signcryption," in *International Conference on Security and Cryptography for Networks*. Springer, 2010, pp. 154–171.
[45] X. Meng and X. Meng, "A novel attribute-based signcryption scheme in cloud computing environments," in *Information and Automation (ICIA), 2016 IEEE International Conference on*. IEEE, 2016, pp. 1976–1979.
[46] Q. Xu, C. Tan, Z. Fan, W. Zhu, Y. Xiao, and F. Cheng, "Secure data access control for fog computing based on multi-authority attribute-based signcryption with computation outsourcing and attribute revocation," *Sensors*, vol. 18, no. 5, p. 1609, 2018.
[47] D. Khader, "Attribute based group signatures." *IACR Cryptology ePrint Archive*, vol. 2007, p. 159, 2007.
[48] H. K. Maji, M. Prabhakaran, and M. Rosulek, "Attribute-based signatures: Achieving attribute-privacy and collusion-resistance." *IACR Cryptology ePrint Archive*, vol. 2008, p. 328, 2008.
[49] ——, "Attribute-based signatures," in *Cryptographers Track at the RSA Conference*. Springer, 2011, pp. 376–392.
[50] S. T. Ali and B. Amberker, "Short attribute-based group signature without random oracles with attribute anonymity," in *International Symposium on Security in Computing and Communication*. Springer, 2013, pp. 223–235.
[51] V. Kuchta, R. A. Sahu, G. Sharma, and O. Markowitch, "On new zero-knowledge arguments for attribute-based group signatures from lattices," in *International Conference on Information Security and Cryptology*. Springer, 2017, pp. 284–309.
[52] V. Kuchta, G. Sharma, R. A. Sahu, and O. Markowitch, "Generic framework for attribute-based group signature," in *International Conference on Information Security Practice and Experience*. Springer, 2017, pp. 814–834.
[53] M. Li, S. Yu, N. Cao, and W. Lou, "Authorized private keyword search over encrypted data in cloud computing," in *Distributed Computing Systems (ICDCS), 2011 31st International Conference on*. IEEE, 2011, pp. 383–392.
[54] T. Okamoto and K. Takashima, "Hierarchical predicate encryption for inner-products," in *International Conference on the Theory and Application of Cryptology and Information Security*. Springer, 2009, pp. 214–231.
[55] W. Sun, S. Yu, W. Lou, Y. T. Hou, and H. Li, "Protecting your right: Attribute-based keyword search with fine-grained owner-enforced search authorization in the cloud," in *INFOCOM, 2014 Proceedings IEEE*. IEEE, 2014, pp. 226–234.
[56] ——, "Protecting your right: verifiable attribute-based keyword search with fine-grained owner-enforced search authorization in the cloud," *IEEE Transactions on Parallel and Distributed Systems*, vol. 27, no. 4, pp. 1187–1198, 2016.
[57] G. Yang, Q. Huang, D. S. Wong, and X. Deng, "Universal authentication protocols for anonymous wireless communications," *IEEE Transactions on Wireless Communications*, vol. 9, no. 1, 2010.
[58] J. K. Liu, C.-K. Chu, S. S. Chow, X. Huang, M. H. Au, and J. Zhou, "Time-bound anonymous authentication for roaming networks," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 1, pp. 178–189, 2015.