Context-Aware Attribute Based Access Control for Cloud-based SCADA Systems

1st Workshop on Enhanced Network Techniques and Technologies for the Industrial IoT to Cloud Continuum (IIoT-Nets)

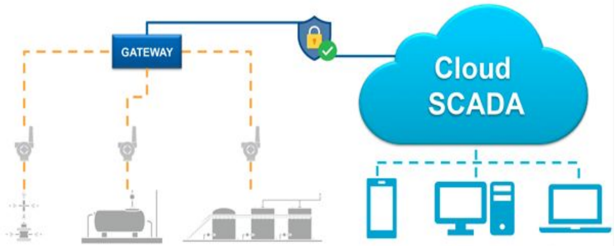
Kasturi Routray, Padmalochan Bera

Indian Institute of Technology, Bhubaneswar

10th September 2023
School of Electrical Sciences
Indian Institute of Technology Bhubaneswar

Cloud-based SCADA Systems

- Powerful tool for leveraging the IoT
- Allows automation, data monitoring and control and gain real-time insights
- Reduce operational costs, improve safety, and increase efficiency



Challenges of Cloud-based SCADA Systems

- Data Privacy and Confidentiality
- Data Integrity
- Access Control
- Authentication and Authorization
- Key Management

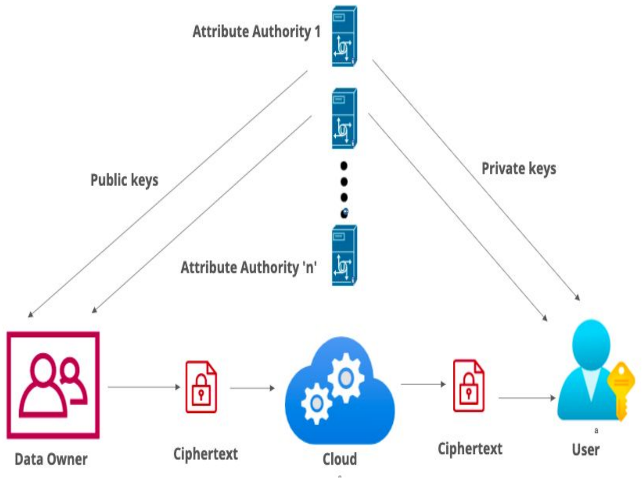
Techniques for Secure Data Storage and Sharing

Limitations of Traditional Cryptographic Scheme:

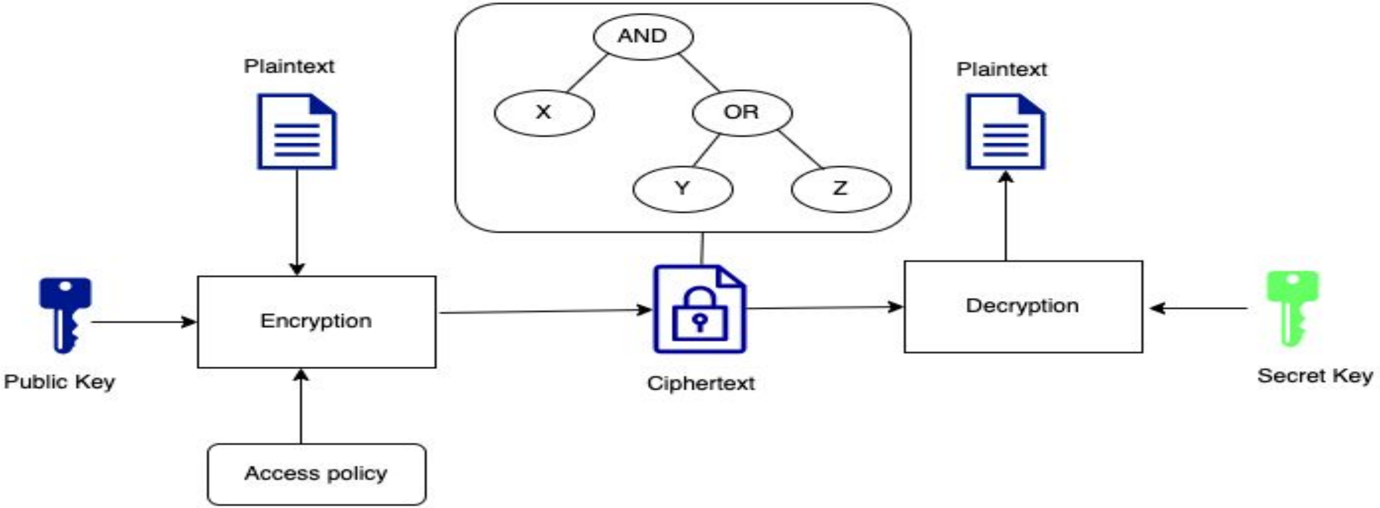
- One-to-one schemes: lacks expressiveness of data sharing
- Requires PKI and certificate management functions

Advantage of Attribute Based Encryption:

- One to Many Public Key Encryption Scheme
- Exact list of users need not be known apriori
- Less overhead of Key management

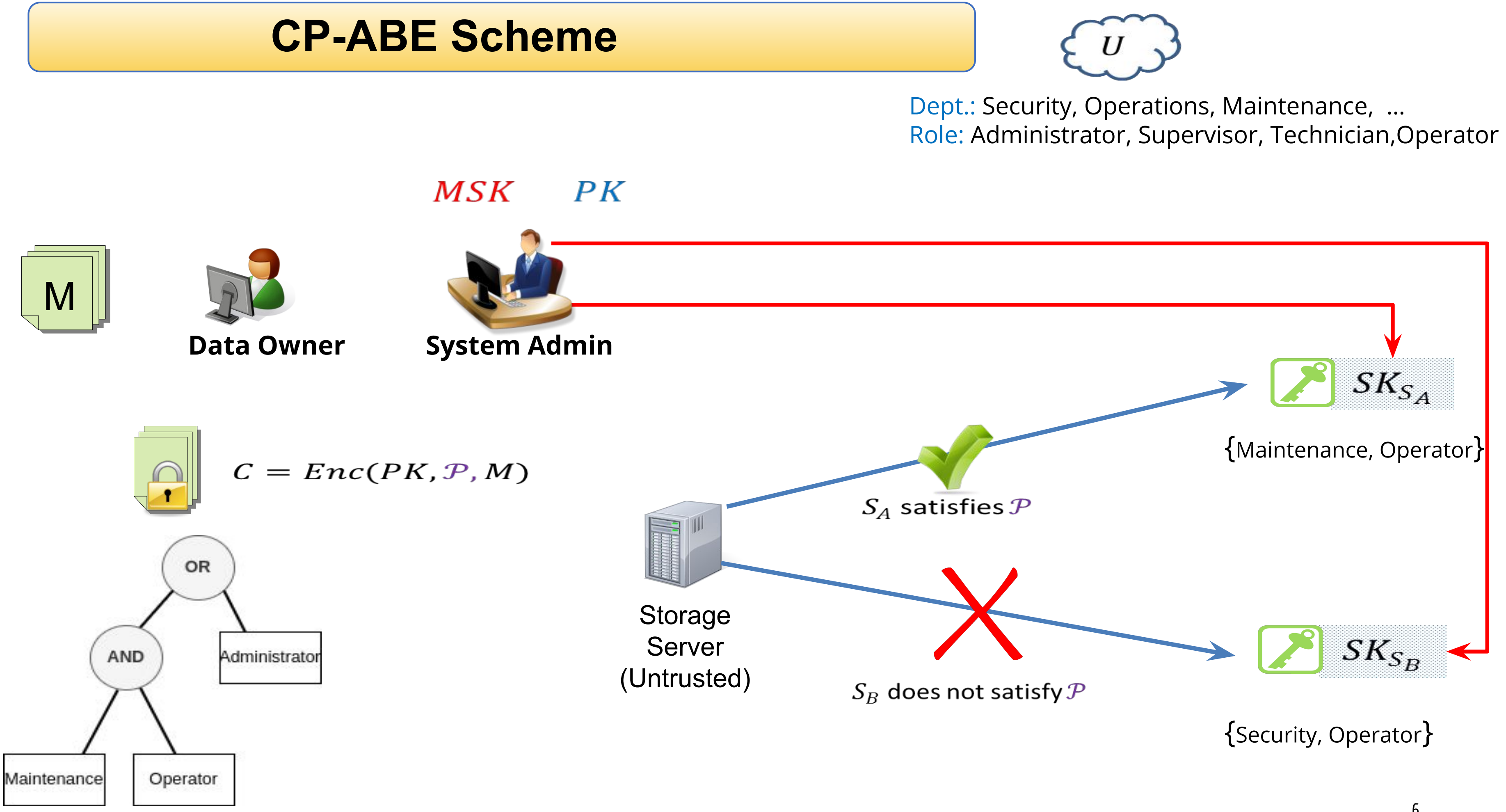


What is CP-ABE?



- **User** : Set of descriptive attributes.
- **Private key** : Depends on users attributes
- **Ciphertext** : Associated with access policy defined over attributes
- **Decryption :** If user attributes satisfies access policy

CP-ABE Scheme



Existing Schemes on CP-ABE

References	Comments
Bethencourt et al. [2007]	Proposed a bitwise approach which uses a policy tree (consists of 0/1 branches) to realize integer comparison. Inefficient for practical applications.
Zhu et al. [2012]	Supports the time attribute with range using forward/backward derivation functions.
Zhu et al. [2012]	Handle current time controls with the help of proxy-based re-encryption mechanism
Balani et al. [2014]	Proposed a temporal access control scheme with user revocation.
Yang et al. [2016]	Suggests refreshing the update key at every time slot and sending it to the users who possess eligible attributes at that time slot.
Wang et al. [2015]	Wang et al. presented a novel range derivation function for comparative attribute-based encryption. But their scheme only focused on handling all attributes with range constraints.
Hong et al. [2017]	Introduced timed-release encryption into the architecture of CP-ABE. Not applicable for time range intervals
Arfaoui et al. [2020]	Proposed embedding the contextual information into access structures using contextual information. But incurs additional overhead.

Limitations of Existing CP-ABE schemes

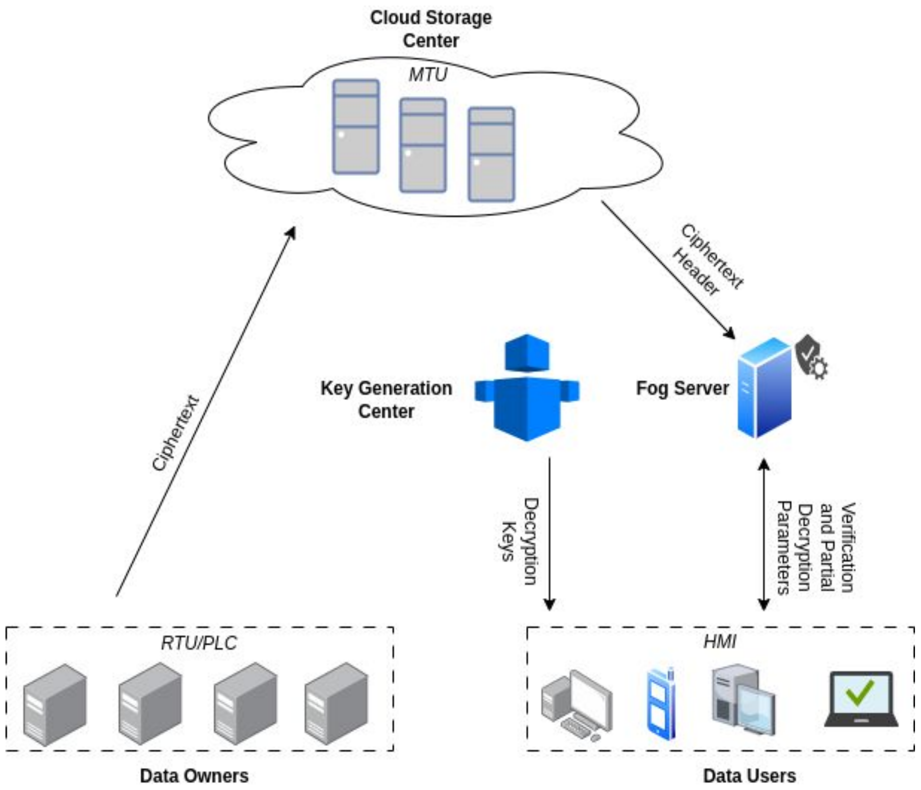
- Not considering ***Contextual information***.
- Expensive Operations $\longrightarrow$ Not suitable resource constrained devices.
- Attribute Privacy Issues
- Limitations in addition and removal of users.
- Limited practical applicability for cloud assisted CPS.

Problem Statement

Objective : Develop a lightweight practical Attribute based encryption system for secure data sharing in cloud based SCADA .

- ➢ Integrating contextual locks in access policies
- ➢ Preventing Key Escrow Attacks
- ➢ Hiding the Access Policy Attributes
- ➢ Outsourcing of decryption operations

Proposed Cryptosystem



<u>**System Model of Proposed CP-ABE scheme**</u>

Features:

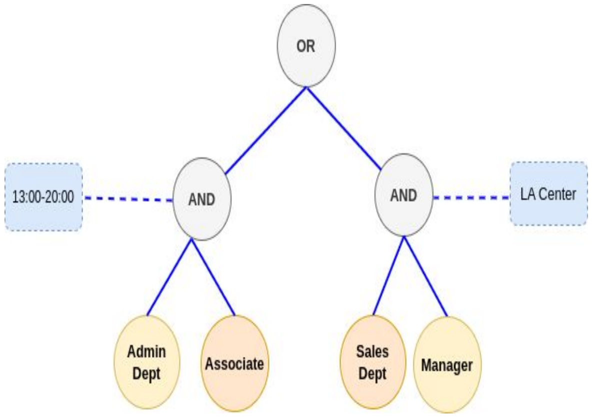
- *Prevents Key Escrow Attacks*
- *Obfuscate Attributes of access policy*
- *Context Verification and Partial decryption by fog server*

Keys Phases:

- ❖ *System Initialization Phase:*
  - ➢ *Key Generation Center Setup*
  - ➢ *Fog Server Setup*
  - ➢ *Cloud Storage Center Setup*
- ❖ *Data Publication Phase:*
  - ➢ *Data Encryption*
- ❖ *User Key Generation Phase:*
  - ➢ *Key Generation*
  - ➢ *Transformed Key Generation*
- ❖ *Data Access Phase:*
  - ➢ *Context Verification*
  - ➢ *Partial Decryption*
  - ➢ *Final Decryption*

Building Blocks

- **Encrypted symmetric key :** Prevents attacks on cloud server.
- **Expressive Access Policies :** Integration of dynamic attribute
- **One-way anonymous key agreement protocol** [14] : Access Policy Attribute Obfuscation
- **Key secrecy property** : Prevent key escrow attacks.



$$CT_{Header} = \{\widetilde{\mathcal{T}},\ C = \mathcal{K}_e \cdot \mathcal{K}_S \cdot e(g,g)^{\alpha s}, \widetilde{C} = g^s,$$
$$\forall y \in \mathbf{Y}:\ C_y,\ C'_y;\ \ \forall CL_y \in \mathcal{T}:\ CL_y = (A_y^{c_j},\ B_y^{c_j})\}$$

$$CT_{Data} = \{\bar{C} = Enc_{\mathcal{K}_e}(M)\}$$

$$CL_y = \{A_y^{c_j} = g^{r_c},\ B_y^{c_j} = s_y^{\rho} + H_2(e(H_1(c_j)),\ g^{\delta_{c_j}})\}$$
$$C_y = g^{s_y^1} \text{ and } C'_y = H_1(Att(y))^{s_y^1}$$

Security Analysis

Our cryptosystem satisfies following security requirement:

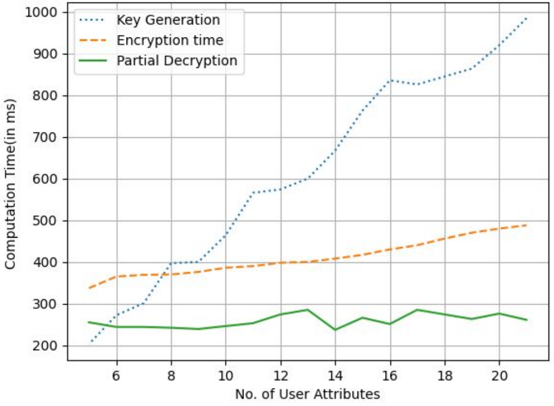
- ➢ Protection against Collusion Attacks
- ➢ Prevents Key Escrow Attack
- ➢ Access Policy Secrecy
- ➢ Revocation for unsatisfied context
- ➢ Privacy Protection Against CDC and Fog Servers

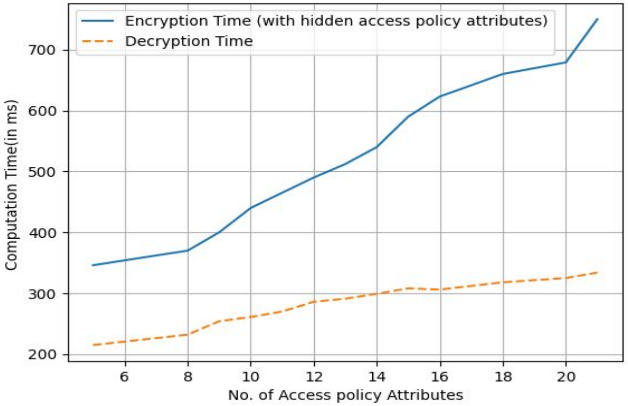
Complexity Analysis

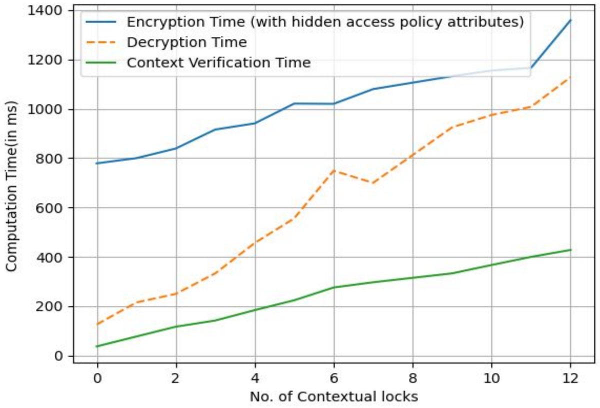
Operations	Ref. [5]	Ref. [13]	Our Scheme
Data Encryption	$E_{\mathbb{G}}(N_A+1)+E_{\mathbb{G}_T}$	$E_{\mathbb{G}}(2+N_A)+2C_B+E_{\mathbb{G}_T}$	$E_{\mathbb{G}}(2+N_A)+2C_B+E_{\mathbb{G}_T}$
Policy Obfuscation	-	-	$C_B N_A + E_{\mathbb{G}}$
Key Commitment	-	$6E_{\mathbb{G}}$	$C_B + E_{\mathbb{G}}$
Indices Generation	-	-	$N_U(C_B+2E_{\mathbb{G}})$
Key Transformation	-	-	$2E_{\mathbb{G}}N_U$
Partial Decryption	-	-	$C_B(2N_U+1)+E_{\mathbb{G}}$
User Decryption	$C_B(2N_U+1)+E_{\mathbb{G}}$	$N_U(C_B+E_{\mathbb{G}})$	$N_U E_{\mathbb{G}}$

- ➢ Transformed key generation: No bilinear pairing operations:
- ➢ Access policy obfuscation:: Required pairing operations are precomputed
- ➢ Final decryption : Requires only exponentiation operations in E_{G}.

Experimentation Analysis







Conclusion

- Our proposed scheme presented a privacy-preserving context-aware access control technique that offers a robust and efficient solution for securing sensitive data stored on the cloud.
- By appending contextual constraints in an access policy, hiding the access policy and employing fog node verification, our scheme addresses the challenges of fine-grained access control, dynamic contextual constraints, and access policy secrecy.
- To support resource-constrained user devices, major computations are outsourced to fog servers.

References

- J. Bethencourt, A. Sahai and B. Waters, ”Ciphertext-Policy Attribute-Based Encryption,” IEEE Symposium on Security and Privacy, 2007, pp. 321-334,
- Y. Zhu, H. Hu, G.-J. Ahn, M. Yu, and H.-J. Zhao, ”Comparison-based encryption for fine-grained access control in clouds,” in CODASPY, ACM, 2012, pp. 105-116.
- N. Balani and S. Ruj, ”Temporal Access Control with User Revocation for Cloud Data,” IEEE 13th International Conference on Trust, Security and Privacy in Computing and Communications, 2014, pp. 336-343.
- Y. Xue, J. Hong, W. Li, K. Xue and P. Hong, ”LABAC: A Location-Aware Attribute-Based Access Control Scheme for Cloud Storage,” IEEE GLOBECOM, 2016, pp. 1-6.
- Z. Wang, D. Huang, Y. Zhu, B. Li and C. -J. Chung, ”Efficient Attribute-Based Comparable Data Access Control,” in IEEE Transactions on Computers, vol. 64, no. 12, pp. 3430-3443.
- Z. Liu, Z. L. Jiang, X. Wang, S. M. Yiu, R. Zhang and Y. Wu, ”A Temporal and Spatial Constrained Attribute-Based Access Control
- Scheme for Cloud Storage,”IEEE (TrustCom/BigDataSE), 2018, pp. 614-623.
- Y. Baseri, A. Hafid and S. Cherkaoui, ”K-anonymous location-based fine-grained access control for mobile cloud,”IEEE Annual Consumer Communications Networking Conference (CCNC), 2016 pp. 720-725.
- Hong et al., ”TAFC: Time and Attribute Factors Combined Access Control for Time-Sensitive Data in Public Cloud,” in IEEE Transactions on Services Computing, vol. 13, no. 1, pp. 158-171, 2020.

References

- Amel Arfaoui, Soumaya Cherkaoui, Ali Kribeche, Sidi Mohammed Senouci, ”Context-Aware Adaptive Remote Access for IoT Applications”, IEEE Internet of Things Journal, vol.7, no.1, pp.786-799, 2020.
- ”Announcing the ADVANCED ENCRYPTION STANDARD (AES)” (PDF). FIPS 197. NIST. November 26, 2001.Diffie, Whitfield; Hellman, Martin E. ”Exhaustive Cryptanalysis of the NBS Data Encryption Standard”. Computer 1977. vol 10(6): 74–84.
- Boneh, D. (2007). Bilinear Groups of Composite Order. Pairing-Based Cryptography – Pairing 2007 Lecture Notes in Computer Science, vol
- 4575. Springer, Berlin, Heidelberg. J. Wu, L. Ping, X. Ge, Y. Wang and J. Fu, ”Cloud storage as the infrastructure of cloud computing”, Proceedings of IEEE International Conference on Intelligent Computing and Cognitive Informatics. IEEE, pp. 380-383, 2010.
- G. Niemeyer, “Geohash,” 2008. Website: https://http://geohash.org
- Sonia Jahid, Prateek Mittal, and Nikita Borisov. EASiER: encryption-based access control in social networks with efficient revocation. 6th ACM ASIACCS, 2011.