

Fine-Grained Two Factor Access Control for Web Based Cloud Computing Services

Ambati.Manohara Reddy¹, A.D.Sivarama Kumar²

¹P.G. Scholar, ²Assistant Professor

^{1,2} Computer Science and Engineering

^{1,2} SVR Engineering College

Email: -¹ a.manohar93@gmail.com, ²kumar.durga@gmail.com

ABSTRACT

Mediated cryptography was first familiar as a procedure with allow provoke refusal of open keys. The key idea of mediated cryptography is to use an on-line mediator for each trade. This on-line center individual is implied a SEM (Security Mediator) since it gives a control of security capacities. In case the SEM does not team up then no trades with individuals when all is said in done key are possible any more. The general idea of key-protected security was to store whole deal enters in a physically-secure anyway computationally-obliged device. Without further ado secret keys are kept by customers on a skilled yet temperamental device where cryptographic figurings happen. Without a moment's hesitation insider certainties are then stimulated at discrete periods by methods for Co-activity between the customer and the base while the all inclusive community key remains unaltered all through the lifetime of the system.

In this paper, we propose a fine-grained two-factor get the chance to control tradition for online conveyed processing organizations, using a lightweight security contraption. The contraption has the going with properties: (1) it can figure some lightweight estimations, e.g. hashing and exponentiation; and (2) it is change safe, i.e., it is acknowledged that no one can break into it to get the secret information set away inside. In this paper, we propose a fine-grained two-factor get the chance to control tradition for online disseminated figuring

organizations, using a lightweight security contraption. The device has the going with properties. It can process some lightweight computations, e.g. hashing and exponentiation;

what's more, it is adjust safe, i.e., it is normal that no one can break into it to get the riddle information set away inside.

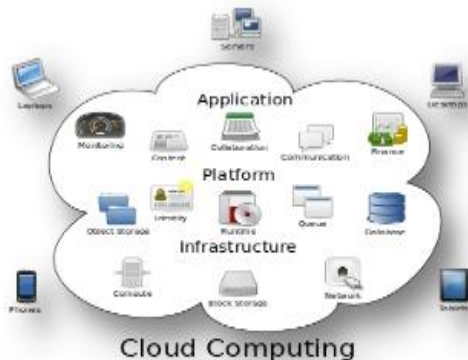
With this contraption, our tradition gives a 2FA security. At first the customer secret key (which is commonly secured inside the PC) is required. Furthermore, the security contraption should be moreover connected with the PC (e.g. through USB) with a particular ultimate objective to approve the customer for getting to the cloud. The customer can be yielded get to simply in case he has the two things.

Index Terms— Fine-grained, two-factor, access control, Web services.

INTRODUCTION

Cloud computing is the utilization of computing assets (hardware and software) that are conveyed as an administration over a system (commonly the Internet). The name originates from the normal utilization of a cloud-formed image as a reflection for the mind boggling foundation it contains in framework graphs. Cloud computing depends remote administrations with a client's data, software and calculation. Cloud computing comprises of hardware

and software assets made accessible on the Internet as overseen outsider administrations. These administrations commonly give access to cutting edge software applications and top of the line systems of server PCs.



Structure of cloud computing

The objective of cloud computing is to apply customary supercomputing, or superior computing power, typically utilized by military and research offices, to perform many trillions of calculations for every second, in buyer arranged applications, for example, money related portfolios, to convey customized information, to give data stockpiling or to influence huge, vivid PC diversions.

The cloud computing utilizes systems of extensive gatherings of servers ordinarily running ease purchaser PC innovation with specific associations with spread data-preparing errands crosswise over them. This mutual IT framework contains vast pools of frameworks that are connected together. Frequently, virtualization methods are utilized to amplify the intensity of cloud computing.

Characteristics and Services Models:

- The notable qualities of cloud computing dependent on the definitions given by the National Institute of

Standards and Terminology (NIST) are sketched out beneath:

- On-request self-benefit: A customer can singularly arrangement computing capacities, for example, server time and system stockpiling, as required naturally without requiring human cooperation with each specialist co-op's. ata focus). Precedents of assets incorporate capacity, preparing, memory, organize data transmission, and virtual machines.
- Rapid flexibility: Capabilities can be quickly and flexibly provisioned, now and again consequently, to rapidly scale out and quickly discharged to rapidly scale in. To the customer, the abilities accessible for provisioning frequently have all the earmarks of being boundless and can be acquired in any amount whenever.
- Measured benefit: Cloud frameworks consequently control and enhance asset use by utilizing a metering ability at some dimension of reflection proper to the kind of administration (e.g., capacity, handling, transfer speed, and dynamic client accounts). Asset utilization can be overseen, controlled, and announced giving straightforwardness to both the supplier and buyer of the used administration.

EXISTING SYSTEM

- Mediated cryptography was first acquainted as a strategy with permit prompt disavowal of open keys. The fundamental thought of mediated cryptography is to utilize an on-line mediator for each exchange. This on-line mediator is alluded

to a SEM (Security Mediator) since it gives a control of security abilities. In the event that the SEM does not collaborate then no exchanges with general society key are conceivable any more.

➤ The general thought of key-protected security was to store long haul keys in a physically-secure however computationally-constrained gadget. Here and now mystery keys are kept by clients on a ground-breaking however unreliable gadget where cryptographic calculations occur. Here and now privileged insights are then invigorated at discrete eras by means of connection between the client and the base while people in general key stays unaltered all through the lifetime of the framework

DISADVANTAGES OF EXISTING SYSTEM

- Key-protected cryptosystem requires all clients to refresh their keys in each era. The key refresh process requires the security gadget.
- Once the key has been refreshed, the marking or unscrambling calculation does not require the gadget any longer inside a similar era.
- The conventional record/secret phrase based verification isn't security saving. In any case, it is all around recognized that protection is a basic element that must be considered in cloud computing frameworks.
- It is basic to share a PC among various individuals. It might be simple for programmers to introduce some spyware to take in the login secret word from the internet browser.
- The foe goes about as the job of the cloud server and endeavors to discover

the personality of the client it is communicating with.

- Access without Secret Key: The foe endeavors to get to the framework (inside its benefits) with no mystery key. It can have its own security gadget.

PROPOSED SYSTEM

- Key-protected cryptosystem requires all clients to refresh their keys in each day and age. The key refresh process requires the security gadget.
- Once the key has been refreshed, the marking or unscrambling calculation does not require the gadget any longer inside a similar day and age.
- The customary record/secret phrase based verification isn't security saving. Nonetheless, it is very much recognized that security is a basic element that must be considered in cloud computing frameworks.
- It is basic to share a PC among various individuals. It might be simple for programmers to introduce some spyware to take in the login secret key from the internet browser.
- The enemy goes about as the job of the cloud server and endeavors to discover the personality of the client it is connecting with.
- Access without Secret Key: The foe attempts to get to the framework (inside its benefits) with no mystery key. It can have its very own security gadget.

PROPOSED SYSTEM

- In this paper, we propose a fine-grained two-factor get to control convention for electronic cloud computing

administrations, utilizing a lightweight security gadget. The gadget has the accompanying properties: (1) it can figure some lightweight calculations, e.g. hashing and exponentiation; and (2) it is alter safe, i.e., it is expected that nobody can break into it to get the mystery information put away inside.

- In this paper, we propose a fine-grained two-factor get to control convention for online cloud computing administrations, utilizing a lightweight security gadget. The gadget has the accompanying properties. It can figure some lightweight calculations, e.g. hashing and exponentiation; and it is alter safe, i.e., it is expected that nobody can break into it to get the mystery information put away inside.
- With this gadget, our convention gives a 2FA security. First the client mystery key (which is normally put away inside the PC) is required. Furthermore, the security gadget ought to be likewise associated with the PC (e.g. through USB) with the end goal to confirm the client for getting to the cloud. The client can be allowed get to just in the event that he has the two things.
- Furthermore, the client can't utilize his mystery key with another gadget having a place with others for the entrance. Our convention underpins fine-grained quality based access which gives an incredible adaptability to the framework to set distinctive access approaches as indicated by various situations. In the meantime, the security of the client is likewise safeguarded. The cloud framework just realizes that the client has some required property, however not the genuine personality of the client. To demonstrate the common sense of

our framework, we recreate the model of the convention.

FOCAL POINTS OF PROPOSED SYSTEM

- Our convention bolsters fine-grained trait based access which gives an incredible adaptability to the framework to set distinctive access strategies as indicated by various situations. In the meantime, the security of the client is additionally protected. The cloud framework just realizes that the client has some required characteristic, however not the genuine personality of the client.
- To demonstrate the common sense of our framework, we mimic the model of the convention.
- Tamper-obstruction. The substance put away inside the security gadget isn't open nor modifiable once it is instated. Likewise, it will dependably pursue the calculation particular.

LITERATURE SURVEY

1) PERM: Practical reputation-based blacklisting without TTPS

AUTHORS: M. H. Au and A. Kapadia

A few clients may get into mischief under the front of namelessness by, e.g., mutilating site pages on Wikipedia or posting profane remarks on YouTube. To forestall such maltreatment, a couple of mysterious accreditation plans have been recommended that deny access for getting out of hand clients while keeping up their obscurity with the end goal that no confided in outsider (TTP) is associated with the repudiation procedure. As of late we proposed BLACR, a sans ttp plot that

underpins 'reputation-based boycotting' - the specialist co-op can score clients' unknown sessions (e.g., great versus wrong remarks) and clients with deficient notoriety are denied get to.

The real disadvantage of BLACR is the straight computational overhead in the extent of the notoriety list, which enables it to help notoriety for just a couple of thousand client sessions in useful settings. We propose PERM, a denial window-based plan (mischievous activities must be gotten inside a window of time), which makes calculation free of the extent of the notoriety list. PERM in this manner underpins a great many client sessions and makes notoriety based boycotting down to earth for expansive scale organizations.

2) **BLACR: TTP-free blacklistable anonymous credentials with reputation**

AUTHORS: M. H. Au, A. Kapadia, and W. Susilo

Mysterious verification can give clients the permit to act mischievously since there is no dread of retaliation. As an impediment, or intends to renouncement, different plans for responsible namelessness include some sort of (conceivably disseminated) confided in outsider (TTP) with the ability to recognize or connect acting up clients. As of late, plans, for example, BLAC and PEREA demonstrated how mysterious denial can be accomplished without such TTPs—unknown clients can be renounced on the off chance that they get into mischief, but then no one can distinguish or connection such clients cryptographically. Notwithstanding being the best in class in mysterious denial, these plans permit just a fundamental type of renouncement adding up to 'repudiate anyone with d or more mischievous activities' or 'disavow anyone whose consolidated misconduct score is too

high' (where mischievous activities are doled out a 'seriousness' score). We present BLACR, which altogether progresses mysterious renouncement in three different ways: 1) It establishes a first endeavor to sum up notoriety based unknown repudiation, where negative or positive scores can be allocated to unknown sessions over various classifications. Servers can square clients dependent on strategies, which determine a boolean blend of notorieties in these classes; 2) We present a weighted expansion, which permits the aggregate seriousness score to increase for numerous mischievous activities by a similar client; and, 3) We make a huge enhancement in confirmation times through a procedure we call express path verification, which makes notoriety based mysterious disavowal down to earth.

3) **Constant-size dynamic k-TAA**

AUTHORS: M. H. Au, W. Susilo, and Y. Mu

Dynamic k-times mysterious confirmation (k-TAA) plans enable individuals from a gathering to be verified namelessly by application suppliers for a limited number of times, where application suppliers can autonomously and progressively allow or repudiate get to appropriate to individuals in their very own gathering. In this paper, we build a dynamic k-TAA conspire with existence complexities of $O(\log(k))$ and a variation, in which the confirmation convention just requires steady reality complexities at the expense of $O(k)$ - estimated open key. We additionally portray some tradeoff issues between various framework qualities. We detail all the zero-learning verification of-information conventions included and demonstrate that our development is secure in the irregular prophet display under the q-solid Diffie–Hellman presumption and q-decisional Diffie–Hellman reversal supposition. We

give a proof-of-idea usage, investigate its execution, and demonstrate that our plan is handy.

4) A secure cloud computing based framework for big data information management of smart grid

AUTHORS: J. Baek, Q. H. Vu, J. K. Liu, X. Huang, and Y. Xiang

Brilliant lattice is a mechanical development that enhances productivity, unwavering quality, financial aspects, and maintainability of power administrations. It assumes a urgent job in present day vitality foundation. The fundamental difficulties of brilliant lattices, nonetheless, are the means by which to oversee diverse kinds of front-end canny gadgets, for example, control resources and shrewd meters effectively; and how to process an enormous measure of data got from these gadgets. Cloud computing, an innovation that gives computational assets on requests, is a decent possibility to address these difficulties since it has a few decent properties, for example, vitality sparing, cost sparing, readiness, versatility, and adaptability. In this paper, we propose a protected cloud computing based system for enormous data information administration in brilliant networks, which we call "Savvy Frame." The fundamental thought of our system is to construct a various leveled structure of cloud computing focuses to give distinctive sorts of computing administrations for information administration and huge data examination. Notwithstanding this auxiliary structure, we present a security arrangement dependent on character based encryption, mark and intermediary re-encryption to address basic security issues of the proposed system.

5) Cipher text-policy attribute based encryption

AUTHORS: J. Bethencourt, A. Sahai, and B. Waters

In a few circulated frameworks a client should just have the capacity to get to data if a client forces a specific arrangement of accreditations or characteristics. Presently, the main strategy for upholding such arrangements is to utilize a believed server to store the data and intervene get to control. Be that as it may, if any server putting away the data is endangered, at that point the secrecy of the data will be imperiled. In this paper we present a framework for acknowledging complex access control on encoded data that we call Cipher content Policy Attribute-Based Encryption. By utilizing our strategies scrambled data can be kept classified regardless of whether the capacity server is untrusted; additionally, our techniques are secure against arrangement assaults. Past Attribute Based Encryption frameworks utilized ascribes to portray the scrambled data and incorporated arrangements with client's keys; while in our framework credits are utilized to depict a client's qualifications, and a gathering encoding data decides an approach for who can decode.

MODULES

- Data User Module
- Authority Module
- Trustee Module
- Cloud server

MODULES DESCRIPTION

Data User Module

- Every user need to register while accessing to cloud.
- After user registered, at the time of user login then user need to provide one time key to access user home.
- One time key will be provided by cloud key will be corresponding user mail id.

- After user access the user home, User can view the all files upload in cloud.
- User need to send the file request for both trustee and authority.
- After user have the two factor access control, user can download the corresponding file.

Two Factor Access Control

- If user need to access file in cloud. They need to get the two factor access control.
- 1. Trustee: Need to get security response from trustee for corresponding file.
- 2. Authority: Need to get secret key from authority for corresponding file.

Authority

- Authority will upload the file in cloud. And uploaded file will store in drive HQ in encrypted format.
- Authority will give secret key for all files when user request for any file and the secret key will be send to corresponding user mail Id.

Trustee Module

- It acts as admin for cloud server.
- Trustee will give request for all files security response when user request for any file.

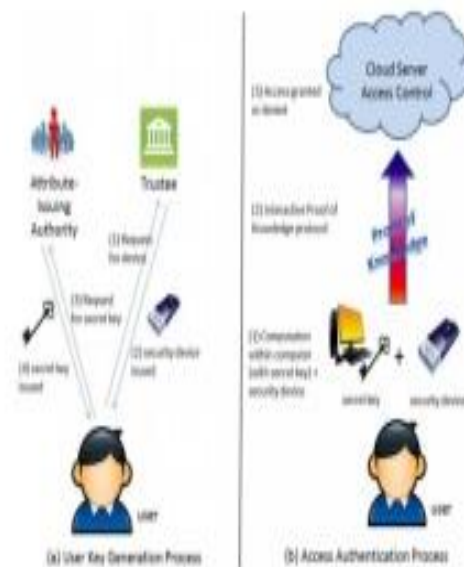
4.3 DATA DICTIONARY


















































Authority

Cloud Server Module






















- Cloud view uploaded files in cloud.
- Cloud view Downloaded files by user in cloud.

4.2 DIAGRAMS SYSTEM ARCHITECTURE













































Field	Type	Collation	Attributes	Null	Default	Extra	Action
<input type="checkbox"/> <u>file_name</u>	varchar(45)	latin1_swedish_ci		No	None		      
<input type="checkbox"/> <u>request</u>	varchar(45)	latin1_swedish_ci		No	None		      
<input type="checkbox"/> <u>date</u>	timestamp		on update CURRENT_TIMESTAMP	No	CURRENT_TIMESTAMP	on update CURRENT_TIMESTAMP	      
<input type="checkbox"/> <u>size</u>	varchar(45)	latin1_swedish_ci		No	None		      
<input type="checkbox"/> <u>status</u>	varchar(45)	latin1_swedish_ci		No	No		      
<input type="checkbox"/> <u>status2</u>	varchar(45)	latin1_swedish_ci		No	No		      
<input type="checkbox"/> <u>author</u>	varchar(45)	latin1_swedish_ci		No	No		      

f-download

Field	Type	Collation	Attributes	Null	Default	Extra	Action
<input type="checkbox"/> <u>id</u>	int(10)		UNSIGNED	No	None	auto_increment	      
<input type="checkbox"/> <u>file_name</u>	varchar(45)	latin1_swedish_ci		No	None		      
<input type="checkbox"/> <u>down</u>	varchar(45)	latin1_swedish_ci		No	None		      

Files

Field	Type	Collation	Attributes	Null	Default	Extra	Action
<input type="checkbox"/> <u>file_name</u>	varchar(45)	latin1_swedish_ci		No	None		      
<input type="checkbox"/> <u>size</u>	varchar(45)	latin1_swedish_ci		No	None		      
<input type="checkbox"/> <u>date</u>	timestamp			No	CURRENT_TIMESTAMP		      
<input type="checkbox"/> <u>file</u>	blob		BINARY	No	None		      
<input type="checkbox"/> <u>data</u>	blob		BINARY	No	None		      
<input type="checkbox"/> <u>skey</u>	varchar(45)	latin1_swedish_ci		Yes	NULL		      

Register

Field	Type	Collation	Attributes	Null	Default	Extra	Action
username	varchar(45)	latin1_swedish_ci		No	None		
name	varchar(45)	latin1_swedish_ci		No	None		
password	varchar(45)	latin1_swedish_ci		No	None		
mail	varchar(45)	latin1_swedish_ci		No	None		
phoneno	varchar(45)	latin1_swedish_ci		No	None		
one_key	varchar(45)	latin1_swedish_ci		Yes	NULL		

Trustee

Field	Type	Collation	Attributes	Null	Default	Extra	Action
file_name	varchar(45)	latin1_swedish_ci		No	None		
request	varchar(45)	latin1_swedish_ci		No	None		
date	timestamp		on update CURRENT_TIMESTAMP	No	CURRENT_TIMESTAMP	on update CURRENT_TIMESTAMP	
size	varchar(45)	latin1_swedish_ci		No	None		
status	varchar(45)	latin1_swedish_ci		No	None		
status1	varchar(45)	latin1_swedish_ci		No	No		
trust	varchar(45)	latin1_swedish_ci		No	No		

SCREEN SHOTS

Home page



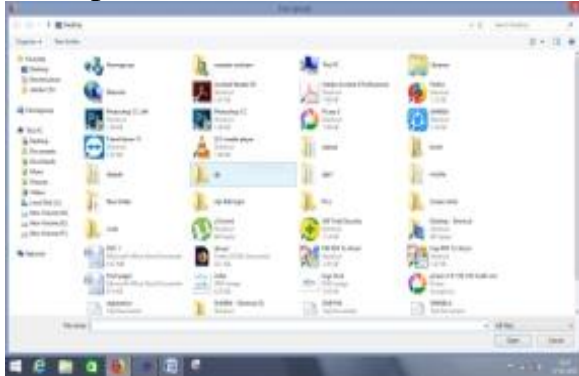
Authority login



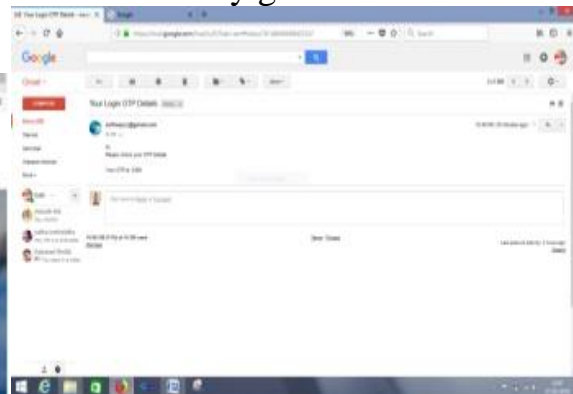
Authority Homepage



File upload



One time key generation



Key verification

User registration



User's home page

User login



Trustee login page



Trustee and Authority Request



Trustee home page



File download page



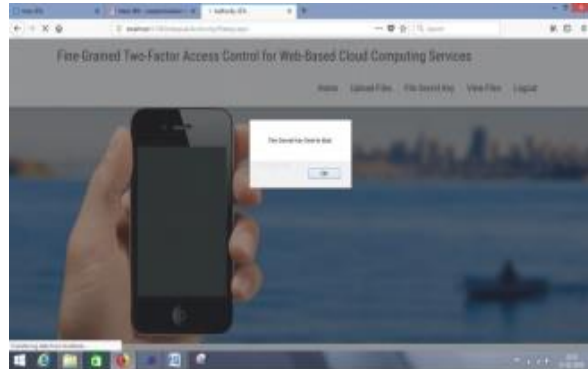
File security response



File security response issued



Authority login



Obtaining secret key



Authority home



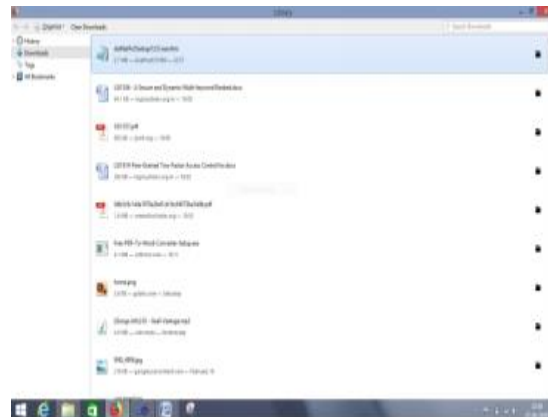
User login



File secret key



Key verification



Accessing the file



CONCLUSION AND FUTURE ENHANCEMENT

In this paper, we have presented a new 2FA (including both user secret key and a lightweight security device) access control system for web-based cloud computing services. Based on the attribute-based access control mechanism, the proposed 2FA access control system has been identified to not only enable the cloud server to restrict the access to those users with the same set of attributes but also preserve user privacy. Detailed security analysis shows that the proposed 2FA access control system achieves the desired security requirements. Through performance evaluation, we demonstrated that the construction is “feasible”. We leave as future work to further improve the efficiency while keeping all nice features of the system.

Downloading the file



File downloaded

- [1] M. H. Au and A. Kapadia, “PERM: Practical reputation-based blacklisting without TTPS,” in Proc. ACM Conf. Comput. Commun. Secur. (CCS), Raleigh, NC, USA, Oct. 2012, pp. 929–940.
- [2] M. H. Au, A. Kapadia, and W. Susilo, “BLACR: TTP-free blacklistable anonymous credentials with reputation,” in Proc. 19th NDSS, 2012, pp. 1–17.

- [3] M. H. Au, W. Susilo, and Y. Mu, "Constant-size dynamic k-TAA," in Proc. 5th Int. Conf. SCN, 2006, pp. 111–125.
- [4] J. Baek, Q. H. Vu, J. K. Liu, X. Huang, and Y. Xiang, "A secure cloud computing based framework for big data information management of smart grid," IEEE Trans. Cloud Comput., vol. 3, no. 2, pp. 233–244, Apr./Jun. 2015.
- [5] M. Bellare and O. Goldreich, "On defining proofs of knowledge," in Proc. 12th Annu. Int. CRYPTO, 1992, pp. 390–420.
- [6] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in Proc. IEEE Symp. Secur. Privacy, May 2007, pp. 321–334.
- [7] D. Boneh, X. Boyen, and H. Shacham, "Short group signatures," in Advances in Cryptology. Berlin, Germany: Springer-Verlag, 2004, pp. 41–55.
- [8] D. Boneh, X. Ding, and G. Tsudik, "Fine-grained control of security capabilities," ACM Trans. Internet Technol., vol. 4, no. 1, pp. 60–82, 2004.
- [9] J. Camenisch, "Group signature schemes and payment systems based on the discrete logarithm problem," Ph.D. dissertation, ETH Zurich, Zürich, Switzerland, 1998.
- [10] J. Camenisch, M. Dubovitskaya, and G. Neven, "Oblivious transfer with access control," in Proc. 16th ACM Conf. Comput. Commun. Secur. (CCS), Chicago, IL, USA, Nov. 2009, pp. 131–140.
- [11] J. Camenisch and A. Lysyanskaya, "A signature scheme with efficient protocols," in Proc. 3rd Int. Conf. Secur. Commun. Netw. (SCN), Amalfi, Italy, Sep. 2002, pp. 268–289.
- [12] J. Camenisch and A. Lysyanskaya, "Signature schemes and anonymous credentials from bilinear maps," in Advances in Cryptology. Berlin, Germany: Springer-Verlag, 2004, pp. 56–72.
- [13] Y. Chen, Z. L. Jiang, S. M. Yiu, J. K. Liu, M. H. Au, and X. Wang, "Fully secure ciphertext-policy attribute based encryption with security mediator," in Proc. ICICS, 2014, pp. 274–289.
- [14] S. S. M. Chow, C. Boyd, and J. M. G. Nieto, "Security-mediated certificateless cryptography," in Public Key Cryptography (Lecture Notes in Computer Science), vol. 3958. Berlin, Germany: Springer-Verlag, 2006, pp. 508–524.
- [15] C.-K. Chu, W.-T. Zhu, J. Han, J.-K. Liu, J. Xu, and J. Zhou, "Security concerns in popular cloud storage services," IEEE Pervasive Comput., vol. 12, no. 4, pp. 50–57, Oct./Dec. 2013.
- [16] R. Cramer, I. Damgård, and P. D. MacKenzie, "Efficient zero-knowledge proofs of knowledge without intractability assumptions," in Public Key Cryptography (Lecture Notes in Computer Science), vol. 1751, H. Imai and Y. Zheng, Eds. Berlin, Germany: Springer-Verlag, 2000, pp. 354–373.
- [17] Y. Dodis, J. Katz, S. Xu, and M. Yung, "Key-insulated public key cryptosystems," in Proc. EUROCRYPT, 2002, pp. 65–82.
- [18] Y. Dodis and A. Yampolskiy, "A verifiable random function with short proofs and keys," in Public Key Cryptography (Lecture Notes in Computer Science), vol. 3386, S. Vaudenay, Ed. Berlin, Germany: Springer-Verlag, 2005, pp. 416–431.
- [19] M. K. Franklin, in Proc. 24th Annu. Int. Cryptol. Conf., Santa Barbara, CA, USA, Aug. 2004.

- [20] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in Proc. 13th ACM Conf. Comput. Commun. Secur., 2006, pp. 89–98.
- [21] J. Han, W. Susilo, Y. Mu, and J. Yan, "Privacy-preserving decentralized key-policy attribute-based encryption," IEEE Trans. Parallel Distrib. Syst., vol. 23, no. 11, pp. 2150–2162, Nov. 2012.
- [22] X. Huang et al., "Cost-effective authentic and anonymous data sharing with forward security," IEEE Trans. Comput., vol. 64, no. 4, pp. 971–983, Apr. 2015.
- [23] J. Hur, "Attribute-based secure data sharing with hidden policies in smart grid," IEEE Trans. Parallel Distrib. Syst., vol. 24, no. 11, pp. 2171–2180, Nov. 2013.
- [24] J. Hur, "Improving security and efficiency in attribute-based data sharing," IEEE Trans. Knowl. Data Eng., vol. 25, no. 10, pp. 2271–2282, Oct. 2013.
- [25] T. Jiang, X. Chen, J. Li, D. S. Wong, J. Ma, and J. Liu, "TIMER: Secure and reliable cloud storage against data re-outsourcing," in Proc. 10th Int. Conf. ISPEC, 2014, pp. 346–358.
- [26] A. Juels, D. Catalano, and M. Jakobsson, "Coercion-resistant electronic elections," in Proc. WPES, 2005, pp. 61–70.
- [27] J. Lai, R. H. Deng, C. Guan, and J. Weng, "Attribute-based encryption with verifiable outsourced decryption," IEEE Trans. Inf. Forensics Security, vol. 8, no. 8, pp. 1343–1354, Aug. 2013.
- [28] M. Li, X. Huang, J. K. Liu, and L. Xu, "GO-ABE: Group-oriented attribute-based encryption," in Proc. 8th Int. Conf. NSS, 2014, pp. 260–270.
- [29] M. Li, S. Yu, Y. Zheng, K. Ren, and W. Lou, "Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption," IEEE Trans. Parallel Distrib. Syst., vol. 24, no. 1, pp. 131–143, Jan. 2013.
- [30] K. Liang et al., "A DFA-based functional proxy re-encryption scheme for secure public cloud data sharing," IEEE Trans. Inf. Forensics Security, vol. 9, no. 10, pp. 1667–1680, Oct. 2014.
- [31] K. Liang, J. K. Liu, D. S. Wong, and W. Susilo, "An efficient cloud-based revocable identity-based proxy re-encryption scheme for public clouds data sharing," in Proc. 19th ESORICS, 2014, pp. 257–272.
- [32] K. Liang, W. Susilo, and J. K. Liu, "Privacy-preserving ciphertext multi-sharing control for big data storage," IEEE Trans. Inf. Forensics Security, vol. 10, no. 8, pp. 1578–1589, Aug. 2015.
- [33] J. K. Liu, M. H. Au, W. Susilo, K. Liang, R. Lu, and B. Srinivasan, "Secure sharing and searching for real-time video data in mobile cloud," IEEE Netw., vol. 29, no. 2, pp. 46–50, Mar./Apr. 2015.
- [34] J. K. Liu, M. H. Au, W. Susilo, and J. Zhou, "Enhancing location privacy for electric vehicles (at the right time)," in Proc. 17th Eur. Symp. Res.



- Comput. Secur., Pisa, Italy, Sep. 2012, pp. 397–414.
- [35] H. K. Maji, M. Prabhakaran, and M. Rosulek, “Attribute-based signatures,” in *Topics in Cryptology*, vol. 6558. Berlin, Germany: Springer-Verlag, 2011, pp. 376–392.
- [36] M. Nabeel, N. Shang, and E. Bertino, “Privacy preserving policy-based content sharing in public clouds,” *IEEE Trans. Knowl. Data Eng.*, vol. 25, no. 11, pp. 2602–2614, Nov. 2013.
- [37] T. Okamoto, “Receipt-free electronic voting schemes for large scale elections,” in *Proc. 5th Int. Workshop Secur. Protocols*, 1997, pp. 25–35.
- [38] T. Okamoto and K. Takashima, “Efficient attribute-based signatures for non-monotone predicates in the standard model,” in *Public Key Cryptography (Lecture Notes in Computer Science)*, vol. 6571. Berlin, Germany: Springer-Verlag, 2011, pp. 35–52.
- [39] R. Ostrovsky, A. Sahai, and B. Waters, “Attribute-based encryption with non-monotonic access structures,” in *Proc. 14th ACM Conf. Comput. Commun. Secur.*, 2007, pp. 195–203.