Global Journal of Computer Science and Technology: B
Cloud and Distributed
Volume 14 Issue 4 Version 1.0 Year 2014
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

Efficient Security Solution for Privacy Cloud Services

By V Sai Vaishnav & A Harshita

K L University, India

Abstract- In this paper, we exhibit a novel protection protecting security answer for cloud services. We manage client nameless access to cloud benefits and imparted stockpiling servers. Our answer furnishes enlisted clients with unacknowledged access to cloud services. Our answer offers unacknowledged verification. This implies that clients' close to home qualities (age, legitimate enrollment, fruitful installment) can be demonstrated without uncovering clients' character. Accordingly, clients can utilize services without any risk of profiling their conduct. Then again, if clients break supplier's tenets, their right to gain entrance rights are renounced. We dissect current security safeguarding answers for cloud services and layout our answer in light of cutting edge cryptographic segments. Our answer offers nameless access, unlinkability and the privacy of transmitted information. Also, we execute our answer and we yield the trial comes about and look at the execution with related arrangements.

Keywords: *authentication, cloud computing,cryptography, encryption, privacy, security.*

GJCST-B Classification : *C.2.4 D.4.7*

EFFICIENTSECURITYSOLUTIONFORPRIVACYCLOUDSERVICES

Strictly as per the compliance and regulations of:

Efficient Security Solution for Privacy Cloud Services

V Sai Vaishnav [α] & A Harshita [σ]

Abstract- In this paper, we exhibit a novel protection protecting security answer for cloud services. We manage client nameless access to cloud benefits and imparted stockpiling servers. Our answer furnishes enlisted clients with unacknowledged access to cloud services. Our answer offers unacknowledged verification. This implies that clients' close to home qualities (age, legitimate enrollment, fruitful installment) can be demonstrated without uncovering clients' character. Accordingly, clients can utilize services without any risk of profiling their conduct. Then again, if clients break supplier's tenets, their right to gain entrance rights are renounced. We dissect current security safeguarding answers for cloud services and layout our answer in light of cutting edge cryptographic segments. Our answer offers nameless access, unlinkability and the privacy of transmitted information. Also, we execute our answer and we yield the trial comes about and look at the execution with related arrangements.

Keywords: authentication, cloud computing, cryptography, encryption, privacy, security.

I. Introduction

Developing cloud services are getting to be undeniable parts of current data and correspondence frameworks what's more venture into our every day lives. Some cloud services, for example, Amazon's Simple Storage Service, Box.net, Cloudsafe and so forth. use client character, individual information and/or the area of customers. Subsequently, these distributed computing services open a number of security and protection concerns. The momentum exploration challenge in cloud services is the safe and protection protecting validation of clients. Clients, who store their touchy data like budgetary data, wellbeing records, and so on., have a central right of protection. There are few cryptographic devices and plans like unnamed validation plans, bunch marks, zero learning conventions that can both shroud client character and give validation. The suppliers of cloud services need to control the verification process to allow the right to gain entrance of just legitimate customers to their services. Further, they must have the capacity to repudiate malevolent customers and uncover their personalities. In practice, many clients can access cloud services in the meantime. Thus, the confirmation methodology of client access must be as productive as would be prudent and the computational cryptographic overhead must be insignificant.

We propose a novel security answer for cloud services that offers nameless validation. We point mostly on the productivity of the confirmation methodology and client security. Our answer additionally gives the privacy and respectability of transmitted information in the middle of clients and cloud administration suppliers. Additionally, we execute our answer as a confirmation of-idea application and contrast the execution of our answer and related plans. Our results demonstrate that our answer is more effective than the related arrangements. The paper is composed as take after: The following segment presents the related work. At that point, we break down cryptographic privacypreserving plans utilized as a part of distributed computing. In segment IV., we present our novel protection saving security answer for cloud services. Segment V. contains our trial results. At last, the finish of our work is introduced.

II. Related Work

Protection saving distributed computing arrangements have been created from hypothetical suggestions to cement cryptographic suggestions. There are numerous works which manage general security issues in distributed computing however just few works bargain additionally with client security. The creators [1] investigate the expense of normal cryptographic primitives (AES, Md5, SHA-1, RSA, DSA, and ECDSA) and their practicality for cloud security purposes. The creators manage the encryption of distributed storage yet don't say security protecting access to a distributed storage. The work [2] utilizes a blending based mark plan BLS to make the protection safeguarding security review of distributed storage information by the Outsider Evaluator (TPA). The arrangement uses cluster check to diminish correspondence overhead from cloud server and reckoning cost on TPA side. Further, the paper [3] presents the check conventions that can suit dynamic information records. The paper investigates the issue of giving synchronous open auditability furthermore information progress for remote information honesty weigh in Cloud Figuring in a security saving manner. These arrangements [2] furthermore [3] give security saving open review however don't offer the unacknowledged access of clients to cloud services.

Author α σ: Electronics & Computer Engineering, K L University. e-mails: vaishnav.vagicherla@kluniversity.in, keepsmiling.harshi@gmail.com

The work [4] secures prerequisites for a safe and unacknowledged correspondence framework that uses a cloud structural planning (Tor and Freenet). By the by, the creator does not plot any cryptographic arrangement. An alternate non-cryptographic arrangement guaranteeing client security in cloud situations is displayed in [5]. The creators propose a customer based security chief which lessens the danger of the spillage of client private data. By the by, the arrangement does not ensure against the link ability of client sessions which can result in unapproved client profiling.

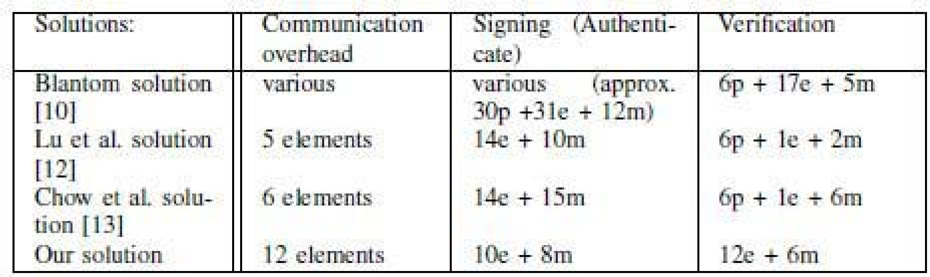
Jensen et. at. [6] propose a nameless and responsible access strategy to cloud focused around ring and gathering marks. In any case, their proposal uses a gathering mark plan [7] which is wasteful on the grounds that the mark size develops with the number of clients. The work [8] presents a security approach which uses zero-information evidences giving client unnamed confirmation. The fundamental disadvantage of the proposal is a vast correspondence overhead between a client and a cloud server because of the Fiat-Shamir distinguishing proof plan [9]. In the work [10], the creator utilizes the CL mark plan [11] and zero knowledge verifications of learning to accomplish client's unknown access to services like computerized daily papers, advanced libraries, music accumulations, and so on. The work [12] presents a cryptographic plan to guarantee unnamed client access to data and the classifiedness of touchy records in cloud stockpiles. We examine the arrangements [10], [12] and [13] in the following segment.

III. Execution Analysis of Cryptographic Security Preserving Solutions used in Cloud Computing

In this segment, we examine the current cryptographic arrangements which give the unnamed or pseudonymous access to cloud benefits and imparted stockpiles. We point on the confirmation stages utilized as a part of protection safeguarding cloud services. In the accompanying execution examination, we take into account just lavish operations like bilinear pairings (p), measured exponentiation (e) and duplication (m). Agreeing to the aftereffects of former works [15], [16], we overlook the quick operations like expansion, subtraction or hash capacities which have a negligible effect on the general execution.

Table I demonstrates the execution examination of the Blantom arrangement [10], the Lu et al. arrangement [12], the Chow et al. arrangement [13] and our answer portrayed in Section IV. Blantom in [10] proposes an answer utilizing the CL marks [11]. To build unnamed verification, the CL mark is joined with a Zero Knowledge Proof of Knowledge (ZKPK) conventions. The computational multifaceted nature of Blantom arrangement depends on the membership sort and is variable. Lu et al. [12] propose a blending based cryptographic plan guaranteeing unnamed verification of clients getting to cloud services. A client needs to sign a test got from a server and after that he/she sends it once more to check it. Chow et al. [13] utilize bunch signature plans proposed by Boyen and Waters in [14] and [17] (BW plans). The BW plan [17] is utilized to make a gathering signature which gives the unknown confirmation of clients. By and by, these arrangements have 6 blending operations in check. In the following segment, we exhibit our answer that does not utilize expensive blending operations.

Table 1 : Execution Analysis Of Solutions In Cloud Computing



Solutions:	Communication overhead	Signing (Authenticate)	Verification
Blantom solution [10]	various	various (approx. 30p +31e + 12m)	6p + 17e + 5m
Lu et al. solution [12]	5 elements	14e + 10m	6p + 1e + 2m
Chow et al. solution [13]	6 elements	14e + 15m	6p + 1e + 6m
Our solution	12 elements	10e + 8m	12e + 6m

IV. Our Solution

In this part, we present our security answer for security protecting cloud services. We diagram our framework model, security prerequisites, cryptography foundation and cryptographic conventions.

a) System Model

Our solution comprises of three crucial gatherings:

- Cloud Service Provider (CSP). CSP oversees cloud services what's more imparted stockpiles. CSP is normally an organization which carries on as a mostly trusted gathering. CSP gives cloud services, confirms clients when they get to a cloud administration. CSP additionally issues access credits to clients. All things considered, when CSP needs to disavow and distinguish a malignant client then CSP must team up with a disavowal director.

- Revocation Manager (RM). RM is a somewhat trusted gathering, e.g. government power, who chooses if the disavowal of a client personality is legitimate or not. Just the participation in the middle of CSP and RM can uncover the client personality. RM additionally collaborates with CSP amid client enlistment when the client's right to gain entrance characteristics are issued.
- User (U). U is a customary client who gets to into a cloud and uses cloud services, imparted stockpiles, and so on. Clients are unknown in the event that they appropriately take after the tenets of CSP. To build security, clients utilization alter safe gadgets or ensured neighborhood stockpiles.

b) Requirements

Our solution gives the accompanying security prerequisites:

- Anonymity. Each fair client stays unnamed when utilizations cloud services. Client characters are shrouded if clients carry on genuinely and don't break principles.
- Confidentiality. Each client's session to CSP is secret. Nobody without a mystery session key has the capacity get information transmitted in the middle of U and CSP.
- Integrity. Information sent in client's session can't be altered without a mystery key.
- Unlinkability. The client's sessions to cloud services are unlinkable. Nobody other than CSP working together with RM has the capacity connect two or more sessions between a certain U furthermore CSP.
- Untraceability. Different clients are not able to follow client's validation and cement clients' correspondence.
- Revocation. Each client can be denied by the coordinated effort of CSP and RM.

c) Cryptography Used

In our answer, we utilize discrete logarithm duties portrayed in earlier work [18]. Further, the arrangement utilizes conventions [19] to demonstrate of discrete logarithm information, representation what's more identicalness [20]. To repudiate a client, we utilize the Okamoto- Uchiyama Trapdoor One-Way Function portrayed in [21]. For more insights about the utilized fundamental cryptographic squares see former works [22], [18].

d) Proposed Protocol

Our convention comprises of five stages: initialization, registration, anonymous access, secure communication and revocation. The basic principle of the proposed convention is delineated in Fig. 1.

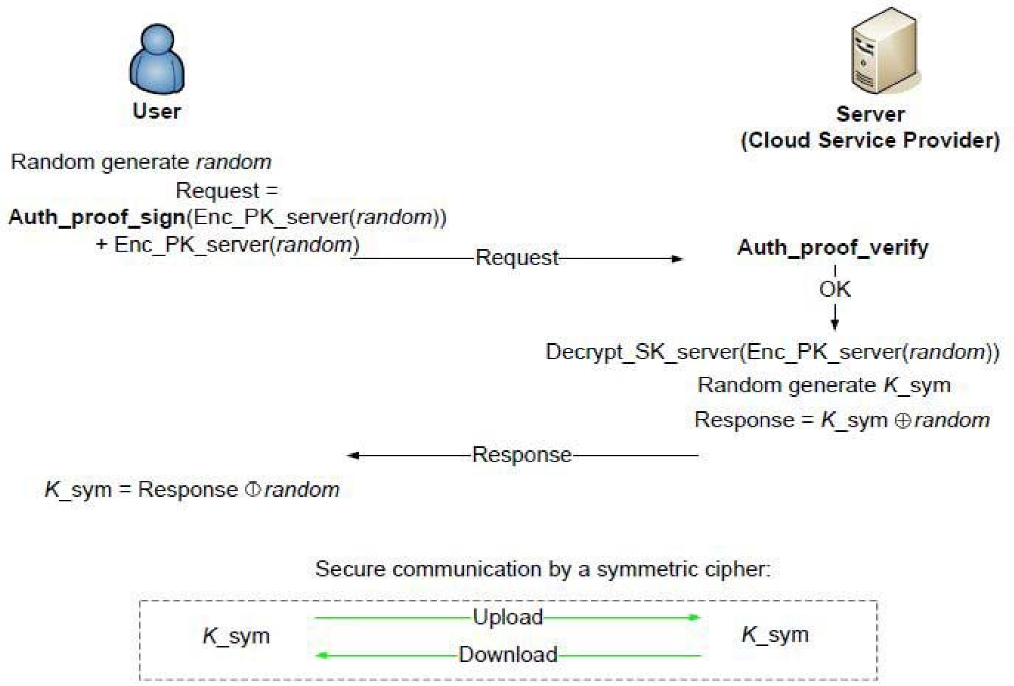

User
Server
(Cloud Service Provider)
Random generate *random*
Request =
Auth_proof_sign(Enc_PK_server(*random*))
+ Enc_PK_server(*random*)
Request
Auth_proof_verify
OK
Decrypt_SK_server(Enc_PK_server(*random*))
Random generate *K*_sym
Response = *K*_sym ⊕ *random*
Response
*K*_sym = Response ⊕ *random*
Secure communication by a symmetric cipher:
*K*_sym
Upload
Download
*K*_sym

Figure 1 : The Basic Principle of the Proposed Protocol

1) Initialization: The instatement stage is controlled by Cloud Administration Provider (CSP) and Revocation Manager (RM). CSP creates a gathering H characterized by a vast prime modulus p, generators h1, h2 of prime request q and q|p - 1. CSP creates a RSA key match and stores own private key KCSP. RM produces a gathering G characterized by a huge modulus n = r2s where r = 2r` + 1; s = 2s` + 1 and r, s, r`, s` are large primes. RM additionally creates a generator g1, request ord(g1 modr2) = r(r - 1) in Z*r 2 and ord(g1) = rr`s` in Z*n and arbitrarily picks secret values S1, S2, S3. RM figures verification evidence Aproof = g1 s1 mod n which is open and regular for all substances in framework. In our answer, the RM has the capacity issue more sorts of validation verifications A1 proof :::AN proof got from S11 :::S1 N that are identified with distinctive client rights in cloud services. At long last, RM processes generators g2 = g1 s2 mod n and g3 = g1 s3 mod n and stores mystery values r, s as denial key KRK. All open cryptographic parameters q, p, n, g1, g2, g3, h1, h2, Aproof are distributed and shared.

2) Registration: In the registration stage, a client registers also asks for a client expert key which they use in unacknowledged access to cloud services. Firstly, U must physically enlist on CSP. CSP checks client's ID. At that point, U creates mystery values w,w2 and makes the dedication: CCSP = hw1 1 hw2 2 mod p. U digitally signs CCSP , e.g. by RSA, and sends this mark Sigu(CCSP) with the development of rightness verification PK{w1,w2 : CCSP = h1 w1 h2 w2}to CSP, by documentation of Camenisch and Stadler [20]. CSP checks the client's evidence and the mark. At that point, CSP stores the pair CCSP, Sigu(CCSP), signs the responsibility SigCSP (CCSP) and sends it back to U. Secondly, U demands a client expert key from RM. U computes A`proof =g1 w1 g2 w2 mod n and sends it with CCSP, SigCSP (CCSP ) and the development of rightness evidence Pk{w1,w2 : CCSP = h1 w1h2 w2 ^ A`proof = g1 w1g2 w2} to RM. RM checks the evidence, CSP's signature SigCSP (CCSP) also registers a mystery commitment wRM such that Aproof = g1 w1 g2 w2g3 wRM mod n holds. After this step, U gets own client master key KU which is triplet (w1,w2,wRM). U gets value wRM just with participation with RM which knows the factorization of n. Any legitimate client can repeat the request for the client master key or demand other verification proofs if CSP agrees with that.

3) Anonymous Access: In this stage, the i-th client Ui anonymously gets to Cloud Service Provider (CSP). This stage comprises of two-messages used to confirm Ui and create a secret key in the middle of Ui and CSP. Ui produces an arbitrary quality irregular €R{0,1}lsym. The parameter lsym signifies the size of a shared secret key for the symmetric cipher. Ui encrypts random by the RSA public key of CSP. CSP decrypts a value Enc_pk_server(random) by its RSA private key to acquire irregular. CSP arbitrarily produces imparted secret key K_sym and uses eXclusive OR (XOR) capacity to register irregular K_sym. CSP sends a reaction message (random k_sym) back to Ui. CSP sends a response message (random K sym) back to Ui.

4) Secure Communication: In the event that the unnamed access stage is fruitful, the client Ui can transfer and download information from CSP. Information secrecy and honesty are secured by a symmetric figure. We propose to utilize AES which is well know figure and is underpinned by numerous sorts of programming and equipment stages. To encode and unscramble transmitted information, Ui and CSP utilize the AES mystery key K_sym made in the past stage.

5) Revocation: Depending on the case of guideline breaking, the revocation stage can revoke a client and/or client namelessness. In the event if the clients misuses a cloud service, they get revoked by RM. Since RM knows the factorization of n, RM has the capacity extricate wrm. Firstly, RM extricates the arbitrary session esteem KS from C2 and the mystery RM commitment esteem wRM from C1. At that point, RM distributes wRM into an open boycott. In the event that the client uses revoked key then the equation C1 C2 wRM mod n holds and the client access to cloud services is denied.

In the event that a malignant client breaks the tenets of CSP, this client can be recognized by the coordinated effort of RM and CSP. Firstly, RM removes wRM from the suspected session got by CSP. At that point, RM discovers the comparing CCSP in the database. In the event that CSP gives to RM the express confirmation of client's break, at that point RM sends CCSP to CSP. CSP has the capacity open the character of a client from database yet just with RM's assistance.

V. Experimental Results

In this segment, we layout the experimental results of our solution. We contrast our solution with related solutions and yield the execution assessment.

Table 2 : Performance Evaluation Of Our Solution

Sessions [#]	Sign/Authenticate Total time [ms]	Verify	Verify with rev = 10
1	54	70	90
10	526	721	900
20	1042	1370	1712
50	2504	3328	4091

Performance Evaluation of Our Solution:

We have actualized our proposed arrangement in JAVA. In practice, we expect that U as an end hub utilizes gadgets with sensible computational power, for example, a PC, a smart phone, atablet or a cell phone. Then again, we expect that CSP keeps servers with sufficient computational ability to guarantee hundreds sessions with end hubs in true time. We have tried our answer on a machine with Intel(r) Xeon(r) CPU X3440 @ 2.53ghz, 4 GB Ram. In our a proofof- idea execution, we pick the 1024-bit length of modulo. The primary essential piece of our answer is the Unnamed Access stage. In this stage, a client (U) convey with a Cloud Administration Supplier (CSP). The processing handle on the client side is stamped as the Sing/Confirm process. The processing process on the CSP side is stamped as the Confirm process. We have measured the aggregate time of the Sing/Verify procedure and the Confirm methodology, see Table II. In the Check methodology, Table II demonstrates two situations: with a void boycott and with the boycott that contains the renounced qualities rev = 10. The impact of the extent of boycott on the aggregate time of the Check methodology is portrayed in Fig. 2.

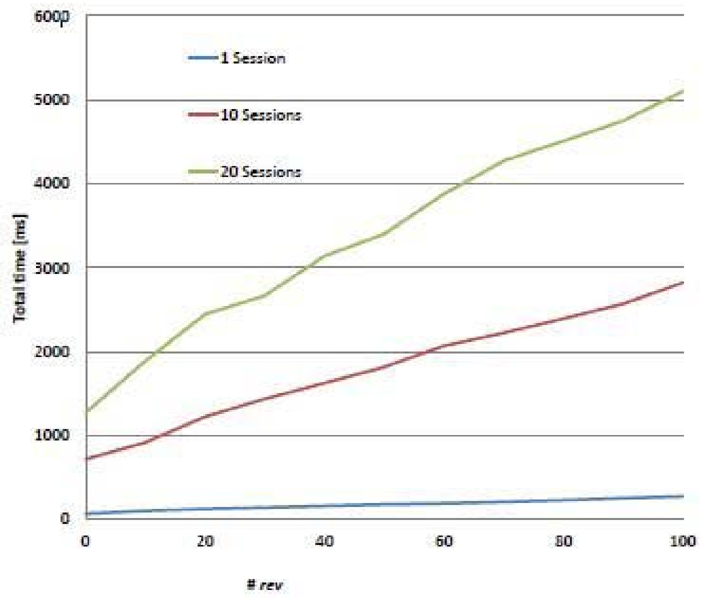


Figure 2 : Influence of the Length of the Blacklist on Total Time of Verification

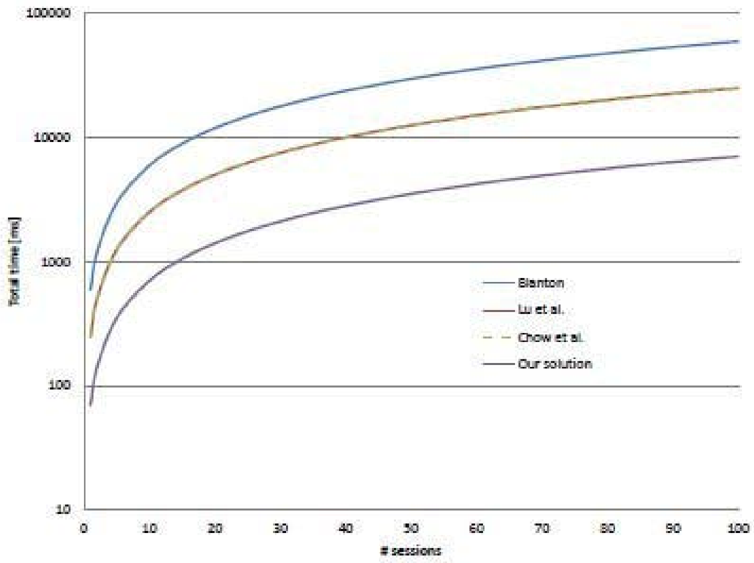


Figure 3 : Performance of the Verify Process

VI. Conclusion

The paper shows our novel security answer for privacy cloud services. We propose non-bilinear gathering marks to guarantee unnamed confirmation of cloud administration customers. Our answer offers client secrecy in confirmation stage, information honesty and classifiedness and the reasonable renouncement process for all clients. Clients utilization alter safe gadgets amid the era and putting away of client keys to secure against intrigue assaults. Our confirmation stage is more proficient than related arrangements on the customer side furthermore on the server side because of missing costly bilinear blending operations and less exponentiation operations. Because of this, cloud administration suppliers utilizing our answer can verify more customers in the same time.

Our future plans are pointed on the adjustment of the repudiation process. We might want to minimize the effect of the long-sized blacklist utilized as a part of the verify process. Likewise we will take a shot at adjustment which cause that alter safe capacity for client keys can be need.

References Références Referencias

1. Y. Chen and R. Sion, “On securing untrusted clouds with cryptography,”in Proceedings of the 9th annual ACM workshop on Privacy in the electronic society. ACM, 2010, pp. 109–114.
2. C. Wang, Q. Wang, K. Ren, and W. Lou, “Privacy-preserving public auditing for data storage security in cloud computing,” in INFOCOM, 2010 Proceedings IEEE, march 2010, pp. 1 –9.
3. Q. Wang, C. Wang, K. Ren, W. Lou, and J. Li, “Enabling public auditability and data dynamics for storage security in cloud computing,”Parallel and Distributed Systems, IEEE Transactions on, vol. 22, no. 5,pp. 847 –859, may 2011.
4. R. Laurikainen, “Secure and anonymous communication in the cloud, ”Aalto University School of Science and Technology, Department of Computer Science and Engineering, Tech. Rep. TKK-CSE-B10, 2010.
5. M. Mowbray and S. Pearson, “A client-based privacy manager forcloud computing,” in Proceedings of the Fourth International ICST Conference on COMmunication System software and middleware, ser. COMSWARE ’09. New York, NY, USA: ACM, 2009, pp. 5:1–5:8.
6. M. Jensen, S. Schage, and J. Schwenk, “Towards an anonymous access control and accountability scheme for cloud computing,” in Cloud Computing (CLOUD), 2010 IEEE 3rd International Conference on, july 2010, pp. 540 –541.
7. D. Chaum and E. Van Heyst, “Group signatures,” in Advances in CryptologyEUROCRYPT91. Springer, 1991, pp. 257–265.
8. P. Angin, B. Bhargava, R. Ranchal, N. Singh, M. Linderman, L. Othmane, and L. Lilien, “An entity-centric approach for privacy and identity management in cloud computing,” in Reliable Distributed Systems, 2010 29th IEEE Symposium on. IEEE, 2010, pp. 177–183.
9. A. Fiat and A. Shamir, “How to prove yourself: practical solutions to identification and signature problems,” in Advances in Cryptology- Crypto86. Springer, 1987, pp. 186–194.
10. M. Blanton, “Online subscriptions with anonymous access,” in Proceedings of the 2008 ACM symposium on Information, computer and communications security, ser. ASIACCS ’08. New York, NY, USA: ACM, 2008, pp. 217–227.

11. J. Camenisch and A. Lysyanskaya, “Signature schemes and anonymous credentials from bilinear maps.” in Advances in Cryptology – CRYPTO 2004, 24th Annual International CryptologyConference, Santa Barbara, California, USA, August 15-19, 2004, Proceedings, 2004, pp. 56–72.
12. R. Lu, X. Lin, X. Liang, and X. S. Shen, “Secure provenance: the essential of bread and butter of data forensics in cloud computing,” in Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security, ser. ASIACCS ’10. New York, NY, USA: ACM, 2010, pp. 282–292.
13. S. Chow, Y. He, L. Hui, and S. Yiu, “Spice–simple privacy-preserving identity-management for cloud environment,” in Applied Cryptography and Network Security. Springer, 2012, pp. 526–543.
14. X. Boyen and B. Waters, “Compact group signatures without random oracles,” Advances in Cryptology-EUROCRYPT 2006, pp. 427–444,2006.
15. L. Malina and J. Hajny, “Accelerated modular arithmetic for lowperformance devices,” I Telecommunications and Signal Processing(TSP), 2011 34th International Conference on. IEEE, 2011, pp. 131–135.
16. L. Malina and M. Zukal, “Secure authentication and key establishment in the sip architecture,” in Telecommunications and Signal Processing (TSP), 2011 34th International Conference on. IEEE, 2011, pp. 14–18.
17. X. Boyen and B. Waters, “Full-domain subgroup hiding and constantsize group signatures,” Public Key Cryptography–PKC 2007, pp. 1–15, 2007.
18. J. Hajny and L. Malina, “Unlinkable attribute-based credentials with practical revocation on smart-cards,” in Proceedings of the 11th international conference on Smart Card Research and Advanced Applications, ser. CARDIS’12. Springer-Verlag, 2013, pp. 62–76.
19. R. Cramer, “Modular design of secure, yet practical cryptographic protocols,” Ph.D. dissertation, University of Amsterdam, 1996.
20. J. Camenisch and M. Stadler, “Proof systems for general statements about discrete logarithms,” Tech. Rep., 1997.
21. T. Okamoto and S. Uchiyama, “A new public-key cryptosystem as secure as factoring,” in Advances in Cryptology - EUROCRYPT 98, ser. Lecture Notes in Computer Science. Springer Berlin / Heidelberg, 1998, vol.1403, pp. 308–318.
22. J. Hajny and L. Malina, “Practical revocable anonymous credentials,” in Communications and Multimedia Security. Springer, 2012, pp. 211–213.
23. Z. Martinasek, T. Macha, O. Raso, J. Martinasek, and P. Silhavy, “Optimization of differential power analysis,” PRZEGLAD ELEKTROTECHNICZNY,vol. 87, no. 12, pp. 140–144, 2011.

This page is intentionally left blank