

Institutional Sign In

Browse

My Settings

Get Help

Subscribe

Advertisement

**Need Full-Text**  
access to IEEE Xplore for your organization?

**REQUEST A FREE TRIAL >**

Abstract

Authors

Figures

Browse Conferences > Communication, Networks and S...

Back to Results | Next >  
References

# Proposed anonymous authentication scheme for academic service in the university

## Related Articles

Improving smart card security using self-timed circuits

Citations

Invertible spread-spectrum watermarking for image authentication and multilevel ...

Keywords

Back to Top  
View All

Sign In or Purchase  
to View Full Text

4  
Author(s)

Linawati ; Made Sudarma ; Nyoman Putra Sastra ; Totok Suryawan

View All Authors

<b>Abstract</b>	Authors	Figures	References	Citations	Keywords	Metrics	Media
-----------------	---------	---------	------------	-----------	----------	---------	-------

### Abstract:

The paper discusses about anonymous authentication system for academic service in the university. The anonymous authentication system is proposed to apply in the university to protect the students' identity when they report academic misconduct in the university system. Generally the system is designed and developed using two sub-systems namely the system for user management and the system for file management feedback submitted by students. The "User Management" system facilitates users for new enrollment, registration verification, and key distribution to system users. Whereas "Student Feedback" system facilitates users in making feedback, encrypting and description of files, and sending feedback. The file encryption process used the Attribute-Based Encryption (ABE) algorithm. Both systems will be integrated using the secret API. The testing process in this study used data of Udayana University's community service participants in year 2016. The tests were conducted on anonymous authentication process, encryption process and file description, key distribution process, and feedback process and feedback status. The evaluation showed good results. This is indicated that the user authentication process can be done in just 4.6 seconds, and the process of sending feedback within 6.4 seconds.

**Published in:** Communication, Networks and Satellite (Comnetsat), 2017 IEEE International Conference on

**Date of Conference:** 5-7 Oct. 2017

**DOI:** 10.1109/COMNETSAT.2017.8263586

**Date Added to IEEE Xplore:** 23 January 2018

**Publisher:** IEEE

**ISBN Information:**

**Conference Location:** Semarang, Indonesia, Indonesia

Advertisement

get the latest  
**IEEE** Research  
Anytime, anywhere

My Xplore™  
Mobile App

GET THE FREE APP

Download on the App Store

GET IT ON Google Play

Download PDF

### Keywords

Download Citation

### IEEE Keywords

Authentication, Encryption, Cloud computing, Access control, Conferences, Satellites

View References

### Author Keywords

Anonymous Authentication, Student Feedback, Academic Service

Email

Print

Request Permissions

Export to Collabratec

Alerts

**Authors**

Linawati  
Electrical Engineering Department, Universitas, Udayana, Bali, Indonesia

Made Sudarma  
Electrical Engineering Department, Universitas, Udayana, Bali, Indonesia

Nyoman Putra Sastra  
Electrical Engineering Department, Universitas, Udayana, Bali, Indonesia

Totok Suryawan  
STMIK STIKOM Indonesia, Bali, Indonesia

**Related Articles**

Improving smart card security using self-timed circuits  
S. Moore; R. Anderson; P. Cunningham; R. Mullins; G. Taylor

Invertible spread-spectrum watermarking for image authentication and multilevel access to precision-critical watermarked images  
J. Domingo-Ferrer; F. Sebe

Reconfiguration of resources in middleware  
H.A. Duran-Limon; G.S. Blair

Role-based access control for CORBA distributed object systems  
R.R. Obelheiro; J.S. Fraga

A study of encrypted, tunneling models in virtual private networks  
S. Al-Khayatt; S.A. Shaikh; B. Akhgar; J. Siddiqi

Performance of multimedia applications with IPSec tunneling  
S. Al-Khayatt; S.A. Shaikh; B. Akhgar; J. Siddiqi

Construction of CORBA based object group platform for distributed real-time services  
Chang-Sun Shin; Myung-Hee Kim; Young-Sik Jecing; Sung-Kook Han; Su-Chong Joo

Real time issues on coordinating cooperative autonomous objects  
C. Mitidieri; C.E. Pereira; L.L. Penz

Format-compliant selective scrambling for multimedia access control  
Wenjun Zeng; Jiangtao Wen; M. Severa

Timed information flow among objects based on role concept  
K. Izaki; K. Tanaka; M. Takizawa

Abstract

Authors

Figures

References

Citations

Keywords

Back to Top

**IEEE Account**

- » Change Username/Password
- » Update Address

**Purchase Details**

- » Payment Options
- » Order History
- » View Purchased Documents

**Profile Information**

- » Communications Preferences
- » Profession and Education
- » Technical Interests

**Need Help?**

- » **US & Canada:** +1 800 678 4333
- » **Worldwide:** +1 732 981 0060
- » Contact & Support

[About IEEE Xplore](#) | [Contact Us](#) | [Help](#) | [Accessibility](#) | [Terms of Use](#) | [Nondiscrimination Policy](#) | [Sitemap](#) | [Privacy & Opting Out of Cookies](#)

A not-for-profit organization, IEEE is the world's largest technical professional organization dedicated to advancing technology for the benefit of humanity.  
© Copyright 2018 IEEE - All rights reserved. Use of this web site signifies your agreement to the terms and conditions.

[Abstract](#)

[Authors](#)

[Figures](#)

[References](#)

[Citations](#)

[Keywords](#)

[Back to Top](#)

# Proposed Anonymous Authentication Scheme for Academic Service in the University

Linawati<sup>1</sup>, Made Sudarma<sup>2</sup>, Nyoman Putra Sastra<sup>3</sup>, Totok Suryawan<sup>4</sup>  
<sup>1,2,3</sup>) Electrical Engineering Department, Universitas Udayana, Bali, Indonesia  
<sup>4</sup>) STMIK STIKOM Indonesia, Bali, Indonesia

*Abstract*— The paper discusses about anonymous authentication system for academic service in the university. The anonymous authentication system is proposed to apply in the university to protect the students' identity when they report academic misconduct in the university system. Generally the system is designed and developed using two sub-systems namely the system for user management and the system for file management feedback submitted by students. The "User Management" system facilitates users for new enrollment, registration verification, and key distribution to system users. Whereas "Student Feedback" system facilitates users in making feedback, encrypting and description of files, and sending feedback. The file encryption process used the Attribute-Based Encryption (ABE) algorithm. Both systems will be integrated using the secret API. The testing process in this study used data of Udayana University's community service participants in year 2016. The tests were conducted on anonymous authentication process, encryption process and file description, key distribution process, and feedback process and feedback status. The evaluation showed good results. This is indicated that the user authentication process can be done in just 4.6 seconds, and the process of sending feedback within 6.4 seconds.

**Keywords** — *Anonymous Authentication, Student Feedback, Academic Service.*

## I. INTRODUCTION

Academic service in the university can be improved significantly when the university system can accommodate student's feedbacks and complaints, such as in student community service course, while powerfully protecting students' identity. The course is a compulsory subject in some Universities in Indonesia and it involves multi discipline subjects in the university. The students are grouped then sent to many villages. The group members are from many departments. The activity itself in the village takes one to two months [1]. This is one of the process for students to complete higher education by living, socializing, and adapting to society. Uniting students with lecturers and the community as well as an opportunity for students to apply science, technology, work culture and tolerance among the fellows and the community. Surely there problems arise during the activity. Mostly students are afraid to report if they face problem with their supervisor or other officials. Therefore the University should provide the system that can be accessed by the students to report securely and protect their identity. Then the system must be secured from unauthorized access. Thus this paper proposes anonymous authentication system and its implementation in the subject in Udayana University is as a study case.

Currently Udayana University has 16,737 active undergraduate students [2] and all students are required to attend community service course. To improve the quality of this course is by providing the parties to provide feedback or complaints of the implementation of the activity. The feedback can be given by students, community and lecturers and will be addressed to the responsible of the activity at Udayana University.

To facilitate the provision of the feedback and to increase response speed, therefore the feedback system should be developed that is easily accessible by the parties. However, this feedback is sensitive, thus maintaining and protecting the privacy of users is a top priority in developing this system. Studies related to privacy protection of system users are explained by [3] [4] [6].

This research develops an anonymous authentication system for student complaint about the implementation of the course in Udayana University. To safeguard the data and protect the students' privacy, then the identity of the students will be hidden in this system. The system will only receive feedback from students as well as the supporting files needed. The system will be developed using the laravel framework and will be equipped with file encryption facility to save the data.

## II. ANONYMOUS AUTHENTICATION MODEL

This section includes several models of Anonymous Authentication System. Some researches have been done in Anonymous Authentication model [7] [8] [9]. Generally several algorithms that are used along with Anonymous Authentication on data storage in the cloud including *Attribute-Based Encryption (ABE)*, *Attribute-Based Signature (ABS)* [10] [11], *Key Policy Attribute Based Encryption (KP-AB)* [12], *Public Key Encryption (PKE)*, *Pailler Cripto system*, *Fuzzy Encryption Identity-Based*, *Multi Authority Attribute Based Encryption*, *Message Authentication Code*, SHA, and SHA-1, RFID [13], homomorphic encryption [14], and *Chiper text Police Attribute Based Encryption (CP-ABE)* by [15].

*Attribute-Based Encryption (ABE)* approach that only user who has a match attribute, can use the service from the cloud. Algorithms of ABE and ABS on the data storage medium in the cloud are selected. Using ABE, users are given the appropriate attribute set, only users who have a match set of attributes that can describe the information in the cloud. There are four processes in the ABE algorithm, namely: System Initialization,

## V. PERFORMANCE EVALUATION

Trials are initially focused on two things: Anonymous Authentication Access and feedback delivery by students to the feedback manager. We have tested it by calculating the total time required by "User Manager" to verify the user, and trial to the process of sending feedback by student to recipient. Figure 8 shows the trial result.

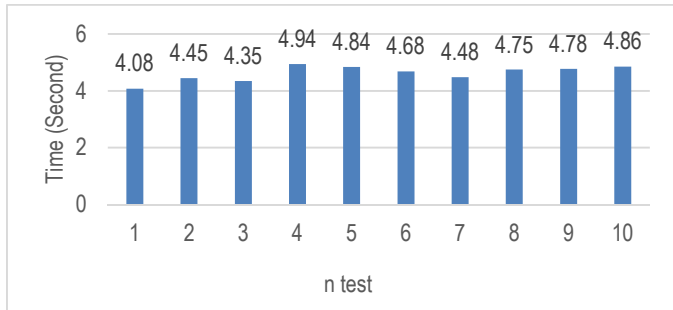


Figure 8. User Verification Test Results (in second)

As can be seen in Figure 8, trials for user verification are performed ten times. The fastest time of the test result is 4.08 seconds and the longest result of the test result is 4.94 seconds. Of the ten experiments performed on average the user verification process takes 4.6 seconds. For the results of feedback delivery trials can be seen in Figure 9.

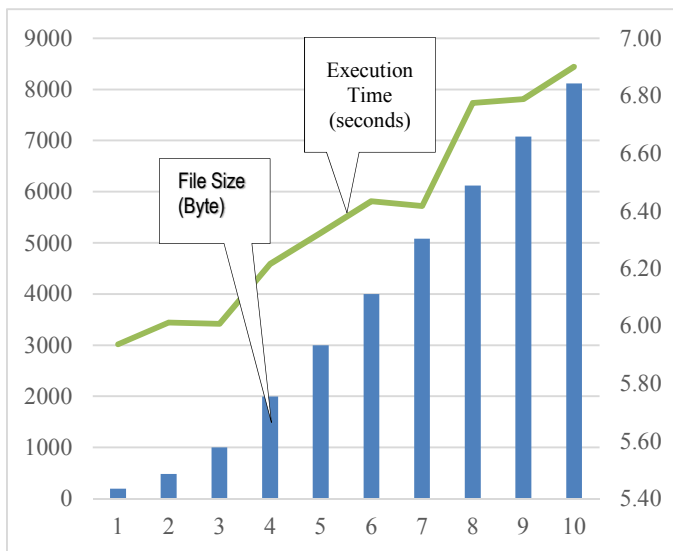


Figure 9. The results of feedback delivery trials

Figure 9 shows that the test is performed ten times. Trials are performed using different file sizes differently, ranging from 197 bytes to 8116 bytes. The fastest time of the test result is 6 seconds and the longest is 6.9 seconds. From the test shows the average execution time of feedback delivery with the average file size of 3797 bytes is 6.38 seconds.

## VI. CONCLUSION

In this paper we have presented a new scheme for anonymous authentication system for student feedback of community service course in Udayana University as a case study. The system protected the student identity or in other word, the student can submit feedback with a hidden identity. Two important things that have been resolved in this paper are the schemes authenticate user without knowing the identity of the user itself. Then for security purposes, the created scheme can encrypt feedback messages and distribute keys to the user to describe the message. Finally the performance result in term of speed process in seconds, the implementation of this scheme shows good results. This is evidenced that the user authentication process can be done in just 4.6 seconds, and the process of sending feedback within 6.4 seconds.

### ACKNOWLEDGMENT

This work is supported by *Lembaga Penelitian dan Pengabdian Kepada Masyarakat (LPPM)* Udayana University under grants number: 415.19/UN14.4.A/PL/2017.

### REFERENCES

- [1]. DGHE of Republic of Indonesia, Panduan Pelaksanaan Hibah Kuliah Kerja Nyata – Pembelajaran Pemberdayaan Masyarakat, 2013. Available on <http://simlitabmas.dikti.go.id>
- [2]. DGHE of Republic of Indonesia, "A Database Of Higher Education Ministry Of Research, Technology And Higher Education Of The Republic Of Indonesia July 2017". Available on <https://forlap.ristekdikti.go.id>
- [3]. Linawati, I. G. T. Suryawan And M. Sudarma, "Anonymous Authentication With Centralize Access Control Of Data Storage In Cloud," *International Journal of Security and Its Applications*, Vol. 11, No. 1, 179–192, 2017.
- [4]. L. Malina, J. Hajny, P. Dzurenda, And V. Zeman, "Privacy-Preserving Security Solution For Cloud Services," *Journal of Applied. Resesarch and Technoly*, Vol. 13, No. 1, Pp. 20–31, 2015.
- [5]. D. Kumar And A. Ranjan, "Shared Authority Based Privacy-Preserving Authentication Protocol In Cloud Computing," *International Journal of Advanced Computer Technology*, Vol. 4, No. Iv, Pp. 1602–1605, 2015.
- [6]. S. Ruj, M. Stojmenovic, And A. Nayak, "Privacy Preserving Access Control With Authentication For Securing Data In Clouds," 12th IEEE/ACM Int. Symp. Clust. Cloud Grid Comput., pp. 556–563, May (2012) 2012.
- [7]. R. Ranjith And D. K. Devi, "Secure Cloud Storage Using Decentralized Access Control With Anonymous Authentication", *International Journal of*

*Advanced Research in Computer and Communication Engineering*. Vol. 2, No. 11, 2013.

- [8]. Lenin, G, Vanitha B, and Vijayalakshmi “Secure Data Storage Using Decentralized Access Control With Anonymous Authentication Using Cloud”, *International Journal of Innovative Research Engineering*. Vol. 3, Issue 1, Pp. 553–559, 2015.
- [9]. Megalai R. V, and Meka R “A Literature Survey On Decentralized Access Control With Anonymous Authentication Of Data Stored In Clouds Using Kdc”, *International Journal of Advanced in Electronics and Communication Engineering*. Vol. 3, No. 12, Pp. 1812–1817, 2014.
- [10]. N. Karthika And S. Ranilakshmi, “Decentralized Access Control With Anonymous Authentication Of Data Stored In Clouds”, *International Conference on Information and Image Processing*. Pp. 186–188, 2014.
- [11]. Ruj Sushmita, Stojmenovic Milos, and Nayak Amiya. “Decentralized Access Control With Anonymous Authentication Of Data Stored In Clouds”, *IEEE Transactions on Parallel and Distributed System*, Vol. 25, No. 2, Pp. 384–394, 2014.
- [12]. G. G. Nikhila, A. B. Pramida, P. Jyothsna, And K. Lavanya, “Anonymous Authentication Of Data Storage In Cloud Computing Administration With Decentralized Access”, *International Journal of Computer Engineering in Research Trends*, Vol. 1, Issue 4, Pp. 195–198, 2014.
- [13]. F. Birinci And M. Ali, “Anonymous RFID Authentication For Cloud Services”, *International Journal of Information Security Science*, Vol. 1, No. 2, Pp. 32–42, 2012.
- [14]. S. Murthy, “Cryptographic Secure Cloud Storage Model With Anonymous Authentication And Automatic File Recovery”, *ICTACT Journal on Soft Computing*, Vol. 5 Issue 01, Pp. 844–849, 2014.
- [15]. K. Yang, X. Jia, K. Ren, And B. Zhang, “Dac-Macs : Effective Data Access Control For Multi-Authority Cloud Storage Systems”, *Proceedings IEEE INFOCOM*, Pp. 2895–2903, 2013.