Northwestern | THE GRADUATE SCHOOL

Application for Admission

App Type **New Student**

Submitted Date **10-01-2018**

App ID# **78319466**

Intended Status **Full-time**

Entry Quarter **Fall 2019**

Prior TGS Applicant (Program)

Last Name **Liu**

First **Yuke**

Middle

Gender Pronouns (US only)

Birthdate **01-02-1998**

Gender **Female**

Program **Computer Science: MS**

Specialization/Area of Interest **Systems and Networking**

Cluster

Secondary PhD (MEAS Only)

MS Consideration (MEAS Only)

JD/PhD **No**

DPT/PhD **No**

Fee Waiver

US Vet/Active Forces

Ethnicity **Asian**

Hispanic **No**

Citizenship **CHINA**

Visa

Citizenship Status **International Student**

Country of Birth **CHINA**

Green Card #

Current Address

266 Xinglong Section of Xifeng Road

Xi'an
CHINA

Permanent Address

No.305 Minzu Avenue

Wuhan, 430073
CHINA

Current Phone **+8618971159579**

Permanent Phone

Cell Phone

Preferred Phone Number **Current Phone Number**

Email Address **yukeliu98@163.com**

Previous Institution	From	To	Field of Study	Level	Degree	Date
Xidian University	**09-01-2015**	**06-20-2019**	**Information Security**		**International Undergraduate Degree**	

Cumulative UG GPA	**3.79**	UG Junior/Senior Year GPA	**3.90**
Cumulative UG GPA - Unconverted		Max UG GPA Scale	
Cumulative Grad GPA			
Cumulative Grad GPA - Unconverted		Max Grad GPA Scale	

Letters of Recommendation

1. **Junwei Zhang** **jwzhang@xidian.edu.cn**
2. **Yueyu Zhang** **yyzhang@xidian.edu.cn**
3. **Shiyang He** **syhe@xidian.edu.cn**
4.
5.

Are you interested in studying with specific faculty members? (List names below)

1. First Name Last Name
2. First Name Last Name
3. First Name Last Name
4. First Name Last Name

Please indicate the highest level of education completed by your parent(s) or guardian(s) (the one or two people most responsible for raising you)

First individual's highest level of education completed: **Graduate or professional degree**

If other, please explain:

Second individual's highest level of education completed: **Graduate or professional degree**

If other, please explain:

Language	Reading	Writing	Speaking

Self-Reported Test Scores

GRE Gen	03-17-2018	Verbal	157	76	Quant	168	94	A.W.	4.0	59	
GRE Sub								LSAT			
TOEFL	04-21-2018	Ovr	114	Read	29	List	30	Speak	26	Writ	29
IELTS		Ovr									
GMAT		Tot			Verb			Quant			
A.W.			I.R.								
MCAT		Bioscience			Verbal			Physical Science			

Please list any honors you have been awarded

Honors: Dean's List
Awards: Special Prize in 2018 National English Contest for College Students;
The 3rd place of women's doubles in the 13th Tennis Tournament for College Students in Shaanxi Province in 2017

Have you applied for or been awarded an external fellowship?

Yes ○ No ⊗ If yes, please specify;

Please describe your plans for the future.

My dream career is about working with innovative IT companies as a competent engineer.

Other Universities Applied (in preferred rank order)

1. School Drop Down **University of California-Irvine**
2. School Drop Down
3. School Drop Down
4. School Drop Down
5. School "other"
6. School "other" **NYU Tandon**
7. School "other"
8. School "other"

Academic misconduct? Yes ○ No ⊗ Convicted of crime? Yes ○ No ⊗

If answered yes, applicant is asked to upload explanation. If uploaded, explanation will be attached to end of application PDF.

西安电子科技大学
XIDIAN UNIVERSITY

Name: Yuke Liu
Application for: CS(MS) in EECS Department
Tel: +86 18971159579
E-mail: yukeliu98@163.com

Statement of Purpose

My interest in computer science originated from taking a road trip on vacations every year with my family. Advanced computer technology has radically changed the way we travel. We can easily use GPS navigation, book a hotel instantly, or even check for local food places in advance by using our smart phones today. However, my father could merely depend on a map for directions when I was a little kid. Amazed at the boon brought by internet, I was intensely curious about the way it works. Thus, I went to the School of Cyber Engineering at Xidian University for my undergraduate study, where I got thrilled to discover my potential in this field and began to envision some kind of a career in the computer industry. With a keen desire to unravel more puzzles in computer science where innovations occur at a bewildering rate, I intend on applying for the Master of Science program in Computer Science at Northwestern University.

My undergraduate program provided me with a sound theoretical background and proficient programming skills, boosting my confidence to undertake further relevant study. Ranking No.5 out of 158, I have completed my core courses (Operating System, Programming Languages, Data structure and Algorithm Analysis) with an efficient self-learning scheme. Also, obtaining a first-class scholarship for the third year in a row was living proof of my distinction in this field. Meanwhile, I've conducted some technical projects and experiments successfully. For instance, I built and maintained a backend database for a student registration system with C and MySQL, developed a file searching program which was platform independent by Java, and combined LDAP and RADIUS servers to manage a student information system with openLDAP and freeradius.

Coursework apart, my research experiences in the area of networks gave me new insights into a broad range of work in computer science. Under the supervision of Professor Junwei Zhang, I designed a blockchain-based scheme for secure cloud file-sharing with fine-grained access control. I utilized the blockchain technology for decentralized safety administration and introduced Ciphertext-Policy Attribute Based Encryption to realize fine-grained data access control of the stored files. The paper was accepted by 2018 International Conference on Networking and Network Applications in Xi'an, China and recommended to SCI journal World Wide Web. Besides, under the guidance of Professor Yueyu Zhang, I utilized gr-gsm tools, captured and analyzed GSM data through Wireshark. Additionally, I used HackRF to broadcast pseudo GPS signals and perform the GPS spoofing attack on Android.

To gain exposure to the computer industry, I endeavored to get an internship in iSoftStone Information Technology Group Co., Ltd in Wuhan city. The project I was engaged in was about developing the safety protocol of ZigBee communication

module for condition monitoring of electrical power facilities. I performed the functional testing of the security certification platform. This practice offered me a precious chance to participate in the software development circle in an IT company, leaving me be aware of the necessity of going to a graduate school to get more professional training.

My dream career is about working with innovative IT companies as a competent engineer. Especially, I'm interested in networks and software engineering, but I am open to trying new ideas as well. I find the MS program in Computer Science at Northwestern University fit my academic and professional goals exceptionally well. I'm planning to acquire more technical expertise and a global perspective in the program.

With Northwestern's historic emphasis on interdisciplinary collaboration, the MS program in computer science produces whole-brain engineers whose deep technical skills are augmented by creative and humanistic thinking. It's also remarkable that graduate students can tailor a curriculum to fit their career aspirations. The program I apply for offers a well-structured curriculum, including appealing courses like Advanced Communication Networks and Software Project Management & Development. In addition, I find my research interests parallel some of the renowned faculty there, such as Professor Yan Chen whose research includes measurement and diagnosis for networking and large-scale distributed systems, Professor Robby Findler who focuses on programming languages and program development environments, and so on. It would be a privilege to study under the guidance of all the outstanding professors there.

I'm confident that a couple of special qualities I possess make me qualified for this program. Firstly, I enjoy being challenged. I was told that science comes more naturally to boys when I got started. As a girl student, I suspect that no one was ever born knowing calculus. I just had to work harder to get good at it, and I made it. Besides, I'm meticulous about my work. When the teachers' lectures appeared perplexing to me, I would record them for further review after class. I even revised my first paper for 12 times for preciseness. In addition, I have my own way to handle stress. I'm gifted in playing tennis, which relieves me from work overload. By the way, I won the 3rd place of women's doubles in the 13th tennis tournament for college students in Shannxi, China.

Overall, I aspire to join an invigorating community of scholars in The Department of Electrical Engineering and Computer Science. Also, I'm ready for my graduate program with determination, dedication and discipline. I believe it would enable me to explore the limitless possibilities in the marvelous world of computer science.

西安电子科技大学学生中文成绩单

姓 名	刘予珂	学 号	15180110044	性 别	女	
出生日期	19980102	入学日期	20150821	学制	4年	
专 业	信息安全	专业方向	信息安全普通			
院 系	网络与信息安全学院	班级	1518011			

修读学期	课 程	学分	课程属性	成绩	修读学期	课 程	学分	课程属性	成绩
2015秋季	大学生职业发展	1.0	必修	通过	2015秋季	大学体育（Ⅰ）	1.0	必修	97
2015秋季	大学物理（Ⅰ）	3.0	必修	92	2015秋季	大学英语（Ⅰ）	4.0	必修	1免修
2015秋季	高等数学A（Ⅰ）	6.0	必修	93	2015秋季	高级英语（Ⅰ）	3.0	必修	90
2015秋季	计算机导论与C语言程序设计	5.0	必修	81	2015秋季	军事理论	2.0	必修	89
2015秋季	军事训练	1.0	必修	通过	2015秋季	思想道德修养与法律基础	3.0	必修	89
2015秋季	新生研讨课	1.0	必修	5良好	2015秋季	形势与政策（Ⅰ）	0.3	必修	通过
2015秋季	专业教育（Ⅰ）	0.3	必修	5良好	2016春季	大学生心理健康教育	1.0	必修	94
2016春季	大学体育（Ⅱ）	1.0	必修	95	2016春季	大学物理（Ⅱ）	5.0	必修	91
2016春季	大学英语（Ⅱ）	4.0	必修	1免修	2016春季	高等数学A（Ⅱ）	6.0	必修	90
2016春季	高级英语（Ⅱ）	3.0	必修	87	2016春季	国家英语四级	1.0	必修	611
2016春季	离散数学	3.5	必修	89	2016春季	马克思主义基本原理	3.0	必修	81
2016春季	物理实验（Ⅰ）	1.0	必修	5优秀	2016春季	线性代数	3.0	必修	91
2016春季	形势与政策（Ⅱ）	0.3	必修	通过	2016秋季	大学体育（Ⅲ）	1.0	必修	99
2016秋季	大学英语（Ⅲ）	4.0	必修	1免修	2016秋季	电路、信号与系统实验（Ⅰ）	0.5	必修	75
2016秋季	电路与电子技术	4.0	必修	83	2016秋季	电子线路实验（Ⅰ）	1.0	学院选修	88
2016秋季	复变函数	2.0	必修	97	2016秋季	概率论与数理统计	3.0	必修	86
2016秋季	高级听力	2.0	学校选修	88	2016秋季	高级语言程序设计	3.0	必修	90
2016秋季	国家英语六级	2.0	公共任选	644	2016秋季	金工实习	2.0	必修	5良好
2016秋季	普通心理学	2.0	人文限选	60	2016秋季	实验实践能力达标测试（I理工类物理）	0.3	必修	通过
2016秋季	数据结构与算法分析	3.5	必修	79	2016秋季	数字电路与逻辑设计	3.0	必修	97
2016秋季	物理实验（Ⅱ）	1.0	必修	5良好	2016秋季	形势与政策（Ⅲ）	0.3	必修	79
2016秋季	中国近现代史纲要	2.0	必修	78	2016秋季	专业教育（Ⅱ）	0.3	必修	5优秀
2017春季	大学体育（Ⅳ）	1.0	必修	100	2017春季	大学英语（Ⅳ）	4.0	必修	1免修
2017春季	电路、信号与系统实验（Ⅱ）	0.5	必修	81	2017春季	电装实习	1.0	必修	5良好
2017春季	电子线路实验（Ⅱ）	1.0	学院选修	85	2017春季	翻译有“道”	2.0	人文限选	96
2017春季	计算机网络	3.0	必修	84	2017春季	毛泽东思想和中国特色社会主义理论体系概论	6.0	必修	91
2017春季	实验实践能力达标测试（I理工类计算机）	0.2	必修	100	2017春季	数据库原理	2.0	必修	85
2017春季	外国文学名著与电影赏析	2.0	人文限选	92	2017春季	微机原理与系统设计	2.0	必修	75
2017春季	信号与系统	4.0	必修	77	2017春季	信息安全数学基础	3.0	必修	88
2017春季	形势与政策（Ⅳ）	0.3	必修	85	2017秋季	编译原理	2.0	必修	88
2017秋季	操作系统原理	3.0	必修	97	2017秋季	软件逆向工程	3.0	学院选修	96
2017秋季	实效口语（中级）	2.0	公共任选	100	2017秋季	数字信号处理	2.0	学院选修	98
2017秋季	通信原理	3.0	学院选修	95	2017秋季	网络安全理论与技术	4.0	必修	95
2017秋季	西安古都与城市文化	2.0	人文限选	94	2017秋季	现代密码学	4.0	必修	94
2017秋季	信息安全法律法规（社工）	1.0	必修	95	2017秋季	形势与政策（Ⅴ）	0.3	必修	88
2018春季	就业指导	1.5	必修	94	2018春季	实验实践能力达标测试（Ⅱ）	0.5	必修	通过
2018春季	网络对抗原理	3.0	必修	94	2018春季	无线通信	2.0	学院选修	92
2018春季	无线通信安全	2.0	学院选修	91	2018春季	形势与政策（Ⅵ）	0.3	必修	93

总实修学分	166.90	必修课实修学分	138.9		国家英语四级成绩	611
加权平均成绩	88.51	学院选修实修学分	14.0			
平均学分绩点	3.79	学校选修实修学分	公共任选实修学分	6.0	国家英语六级成绩	644
			人文素质实修学分	8.0		
毕业设计（论文）题目						
毕业设计（论文）成绩		毕业设计（论文）指导教师				

制表日期：2018年09月18日

学校公章：

验证码：XDDXBKGMHJMHJHGBHGCD

验证网址：http://zzdy.xidian.edu.cn/

XIDIAN UNIVERSITY UNDERGRADUATE STUDENT RECORD

Name	Liu Yuke		Student No.	15180110044	Sex	Female
Date of Birth	19980102	Date of Enrollment	20150821		School Years	4 years
Speciality	Information Security					
Department	School of Cyber Engineering					

Term	Course	Credit	Attribute	Grade	Term	Course	Credit	Attribute	Grade
2015/FA	College Students Occupational Development	1.0	C	Passed	2015/FA	Physical Education(Ⅰ)	1.0	C	97
2015/FA	General Physics(Ⅰ)	3.0	C	92	2015/FA	College English(I)	4.0	C	Excused
2015/FA	Advanced Mathematics(A)(I)	6.0	C	93	2015/FA	Advanced English (Ⅰ)	3.0	C	90
2015/FA	Introduction to Computer Science and Programming in C Language	5.0	C	81	2015/FA	Military Theory	2.0	C	89
2015/FA	Military Training	1.0	C	Passed	2015/FA	Morality Education and Fundamentals of Law	3.0	C	89
2015/FA	Freshmen Seminar Program	1.0	C	Good	2015/FA	Situation and Policy Education(Ⅰ)	0.3	C	Passed
2015/FA	Professional Education(Ⅰ)	0.3	C	Good	2016/SP	Mental Health Education for College Students	1.0	C	94
2016/SP	Physical Education(Ⅱ)	1.0	C	95	2016/SP	General Physics(II)	5.0	C	91
2016/SP	College English(Ⅱ)	4.0	C	Excused	2016/SP	Advanced Mathematics(A)(Ⅱ)	6.0	C	90
2016/SP	Advanced English (Ⅱ)	3.0	C	87	2016/SP	CET-4	1.0	C	611
2016/SP	Discrete Mathematics	3.5	C	89	2016/SP	Fundamental Principles of Marxism	3.0	C	81
2016/SP	Experiments on Physics(Ⅰ)	1.0	C	Excellent	2016/SP	Linear Algebra	3.0	C	91
2016/SP	Situation and Policy Education(Ⅱ)	0.3	C	Passed	2016/FA	Physical Education(Ⅲ)	1.0	C	99
2016/FA	College English(III)	4.0	C	Excused	2016/FA	Experiments on Circuits, Signals and Systems(Ⅰ)	0.5	C	75
2016/FA	Circuits and Electronic Technology	4.0	C	83	2016/FA	Experiments on Electronic Circuits (Ⅰ)	1.0	SFO	88
2016/FA	Complex Variable Functions	2.0	C	97	2016/FA	Probability Theory and Mathematical Statistics	3.0	C	86
2016/FA	Advanced Listening Comprehension	2.0	UFO	88	2016/FA	Advanced Language Programming	3.0	C	90
2016/FA	CET-6	2.0	PFO	644	2016/FA	Metalworking Practice	2.0	C	Good
2016/FA	General Psychology	2.0	HLO	60	2016/FA	Experimental Practice Ability Testing	0.3	C	Passed
2016/FA	Data Structure and Algorithm Analysis	3.5	C	79	2016/FA	Digital Circuits and Logic Design	3.0	C	97
2016/FA	Experiments on Physics(Ⅱ)	1.0	C	Good	2016/FA	Situation and Policy Education(Ⅲ)	0.3	C	79
2016/FA	Outline of Modern History of China	2.0	C	78	2016/FA	Professional Education (Ⅱ)	0.3	C	Excellent
2017/SP	Physical Education(Ⅳ)	1.0	C	100	2017/SP	College English(IV)	4.0	C	Excused
2017/SP	Experiments on Circuits, Signals and Systems(Ⅱ)	0.5	C	81	2017/SP	Electrical Engineering Practice	1.0	C	Good
2017/SP	Experiments on Electronic Circuits (Ⅱ)	1.0	SFO	85	2017/SP	Principles of Translation	2.0	HLO	96
2017/SP	Computer Networks	3.0	C	84	2017/SP	Introduction to Mao Zedong Thought and Theoretical System of Socialism with Chinese Characteristics	6.0	C	91
2017/SP	Experimental Practice Ability Testing	0.2	C	100	2017/SP	Principles of Database	2.0	C	85
2017/SP	Foreign Literature and Film Appreciation	2.0	HLO	92	2017/SP	Microcomputer Principles and System Design	2.0	C	75
2017/SP	Signals and Systems	4.0	C	77	2017/SP	Fundamentals of Mathematics for Information Security	3.0	C	88
2017/SP	Situation and Policy Education(Ⅳ)	0.3	C	85	2017/FA	Principles of Compilation	2.0	C	88
2017/FA	Operating System Principles	3.0	C	97	2017/FA	Software Reverse Engineering	3.0	SFO	96
2017/FA	Practical Oral English (Intermediate)	2.0	PFO	100	2017/FA	Digital Signal Processing	2.0	SFO	98
2017/FA	Communication Principles	3.0	SFO	95	2017/FA	Network Security Theory and Technology	4.0	C	95
2017/FA	Ancient Capital of Xi'an and Urban Culture	2.0	HLO	94	2017/FA	Modern Cryptography	4.0	C	94
2017/FA	Law and Statute of Information Security(Social Work)	1.0	C	95	2017/FA	Situation and Policy Education(Ⅴ)	0.3	C	88
2018/SP	Career Guidance	1.5	C	94	2018/SP	Experimental Practice Ability Testing(II)	0.5	C	Passed
2018/SP	Principles of Network Countermeasure	3.0	C	94	2018/SP	Wireless Communications	2.0	SFO	92
2018/SP	Wireless Communication Security	2.0	SFO	91	2018/SP	Situation and Policy Education(Ⅵ)	0.3	C	93

Total Credits	166.9	Compulsory Course Credits	138.9	CET4	611
Weighted average score	88.51	School Free Optional Course Credits	14.0		
GPA	3.79	University Optional Course Credits: Puplic Free Optional Course Credits	6.0	CET6	644
		University Optional Course Credits: Humanities Limited Optional Course Credit	8.0		
Graduation design title					
Graduation design score		Graduation design supervisor			

Course Attribute:SFO:School Free Optional;UFO:University Free Optional;LO:Limited Optional;C:Compulsory;HLO:Humanities Limited Optional;PFO:Puplic Free Optional

S/N:XDDXFHDJAIJAEGFBCFDD

Web:http://zzdy.xidian.edu.cn/

XIDIAN University Archives

Date Issue: September 18, 2018

Yuke Liu

266 Xifeng Road
Xi'an 710126，China
+86 189-7115-9579
yukeliu98@163.com

EDUCATION

Xidian University, School of Cyber Engineering Xi'an, China
Bachelor of Engineering in Information Security Expected June 2019
Overall GPA: 3.79 ***Major GPA***: 3.9 ***Ranking***: 5/158
Relevant Coursework: Discrete Mathematics, Programming Languages, Algorithms Analysis, Database, Compilation, Operating System, Wireless Communications
Honors: Dean's List, First-class Scholarship, China Resources Scholarship
Awards: Special Prize in 2018 National English Contest for College Students

CONFERENCE PRESENTATION

Xi'an University of Posts and Telecommunications Academic Center Xi'an, China
Yuke Liu, Junwei Zhang, Qi Gao, (October 2018). *A Blockchain-based Secure Cloud Files Sharing Scheme with Fine-Grained Access.* Poster presented at 2018 International Conference on Networking and Network Applications in Xi'an, China. Paper recommended to SCI journal *World Wide Web*.

INTERNSHIP

ISoftStone Information Technology Group Co., Ltd Wuhan, China
Software Engineer Intern July 2018 - September 2018
Participated in the development of safety protocol of ZigBee communication module by performing the functional testing of the security certification platform

PROJECTS

Xidian University, School of Cyber Engineering Xi'an, China
Established the WAF in the Linux system and configured ModSecurity May 2018
Built a pseudo base station with USRP B210 and OpenBTS in Linux system April 2018
Used openLDAP and freeradius to implement LDAP and RADIUS servers March 2018
Built and maintained a backend database for a student registration system with C and MySQL October 2017
Developed a file searching program which was platform independent by Java June 2016

SKILLS

Programming Languages*:* Java, C, MySQL, MATLAB, Python
Languages*:* Mandarin Chinese (native), English (fluent) TOEFL (114), GRE(326)

ATHLETICS

Captain of women's tennis team at Xidian University
The 3rd place of women's doubles in the 13th Tennis Tournament for College Students in Shaanxi Province Xi'an, China June 2017

A Blockchain-based Secure Cloud Files Sharing Scheme with Fine-Grained Access Control

Yuke Liu, Junwei Zhang, Qi Gao
School of Cyber Engineering, Xidian University
Xi'an, China
yukeliu98@163.com, jwzhang@xidian.edu.cn, 392761924@qq.com

Abstract

As cloud services greatly facilitate file sharing online, there's been a growing awareness of the security challenges brought by outsourcing data to a third party. Traditionally, the centralized management of cloud service provider brings about safety issues because the third party is only semi-trusted by clients. Besides, it causes trouble for sharing online data conveniently. In this paper, the blockchain technology is utilized for decentralized safety administration and provide more user-friendly service. Apart from that, Ciphertext-Policy Attribute Based Encryption is introduced as an effective tool to realize fine-grained data access control of the stored files. Meanwhile, the security analysis proves the confidentiality and integrity of the data stored in the cloud server. Finally, we evaluate the performance of computation overhead of our system.

Index Terms

blockchains; cloud storage; CP-ABE; access control; data security

1. Introduction

Nowadays, the rapid development of cloud storage has aroused the awareness of privacy-preserving service provided by enterprises. Therefore, cloud storage system should preserve the integrity and access control of confidential data. However, outsourcing sensitive information to cloud service providers may give rise to privacy issues. To address this problem, the common way is to store the data after encryption instead of plaintext. When users wish to establish a policy defining who can decrypt the sensitive data based on their identities, the traditional method is to implement the access control on a coarse level, like giving your private key to another party. Nevertheless, a fine-grained access control over sensitive data is imperative in many situations. For instance, the Academic Affairs Office need to encrypt exam papers stored in the cloud server so that only certain teachers who are in charge of corresponding subjects can decrypt them. Ciphertext-Policy Attribute-Based Encryption is a great contributor to the fine-grained access control according to the specific knowledge of underlying data. However, the traditional CP-ABE scheme makes it extremely demanding to renew encryption keys particularly for small-sized cloud service providers with limited budgets. Consequently, the blockchain technology is introduced to alleviate this problem. By combining Ciphertext-Policy Attribute-Based Encryption and blockchains, an efficient security solution is realized for cloud storage companies concerning users personal data management on a fine-grained level.

Related works Lots of researchers have been trying to optimize ABE schemes. Bethencourt J et al. [2] proposed CP-ABE (Ciphertext-Policy Attribute-Based Encryption) in 2007. In this system, the users secret key is closely associated with a set of descriptive attributes. Only when those attributes are in line with the policy of the ciphertext can this user decrypt the ciphertext. Given that the construction[1] was proved to be secure solely under the generic group model, Newport et al. [3] presented another one which was secure under the standard model to overcome this weakness. SUN Guo-zi et al. proposed a cloud storage mechanism[4] to achieve the safety and privacy of data during sharing and storage services on the internet.

In 2008, S.Nakamoto[5] proposed blockchain-based Bitcoin, a kind of cryptocurrency, along with a worldwide payment system. In the following years, many blockchain-based cryptocurrency systems[6], [7] have been invented and widely used. Blockchain, based on a peer-to-peer network, records in a verifiable and permanent way.

Data access control for cloud storage The CP-ABE based data access control for cloud storage using blockchain has following properties.

Firstly, confidentiality is the premise of other data management works in our system. On the one hand, adversaries may intentionally compromise the data stored in the cloud server, or even steal sensitive information illegally. Moreover, the service provider is considered to be genuine but curious. In this way, preventing the cloud company from leaking or snooping users personal data for its own benefits

becomes a basic safety requirement.

Secondly, this cloud storage system features fine-grained access control. One can build up a secret-sharing policy for their files, ruling out the vexation brought by confirming identity then giving out secret keys individually. For some special occasions, fine-grained access control is a must when visitors are labeled with a set of attributes that indeed determine the access levels of them.

Thirdly, our scheme guarantees the decentralized management of the data that is related with the secret keys. Utilizing blockchain technology, all the owners of data shared online must sign the ciphertext and record on the blocks.

Our contributions Nowadays, the cloud storage system begins to serve as an efficient resource-sharing platform. However, traditional authority management such as the reference monitor[8] is proved to be inefficient and inflexible considering the massive requests for the online resources in the cloud nowadays. Despite the fact that CP-ABE scheme ensures fine-grained access control over users data, we cannot neglect how complex it is for data centers to generate and renew secret keys while checking the authority of visitors. This paper proposes a privacy-preserving scheme to realize the fine-grained access control when sharing the files stored in the cloud by combining CP-ABE and blockchain technology. Its both safe and efficient for owners to record encrypted keys of the files on blockchains and for visitors to decrypt them from the records. Whats more, generating a new block would be the quickest way to inform others that the keys have been changed. Our contributions in this paper are listed below.

1) We define the required characteristics of our scheme including confidentiality of files in the cloud storage system, fine-grained access control policy designed by the owners themselves, verifiability of the identity of the owners, anti-collusion attack to attribute based access control and data integrity.
2) We propose the formal scheme of CP-ABE based efficient data access control for cloud storage with blockchains.
3) We analyze the security of our scheme theoretically, which confirms that our scheme meet the requirements mentioned above.
4) We present experimental performance of our scheme, and the result shows that it is feasible and efficient for both owners and users.

2. Problem Formulations

2.1. System Model

The system model is depicted in Figure 1. This system consists of the following entities: user, data owner, KGC (Key Generation Center), and cloud service provider.

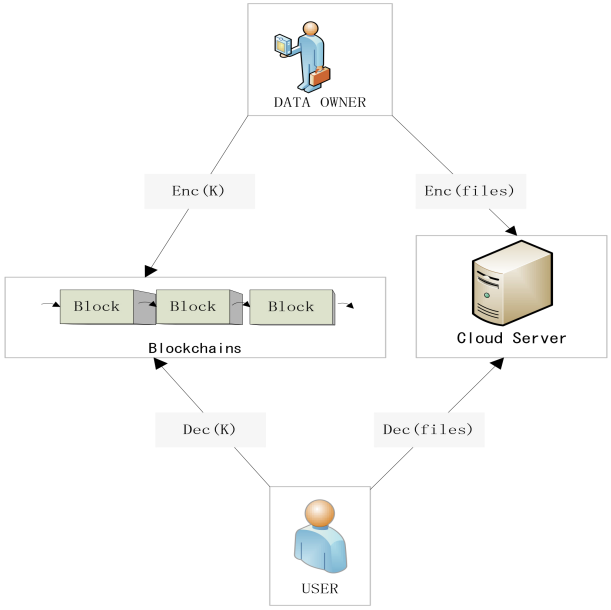


Figure 1. System model

Key Generation Center: To implement Ciphertext-Policy Attribute-Based Encryption, we need a KGC which is in charge of the management and administration of keys, including PK, MSK and SK. Generating, distributing, and revoking SKs to different parties individually are the most essential part of its jobs. When it comes to SKs, the KGC generates and distributes them to users according their attributes, which determine what kind of ciphertext they can decrypt. Generally, the KGC is viewed as honest but curious, which means that it definitely finish the key-assignment tasks without deception, but it may naturally tries to snoop the users information.

Data Owner: its one of the most vital jobs in our scheme to preserve their privacy when data owners are trying to share their sensitive data (in the form of ciphertext) with others remotely via cloud storage system. Besides, the data owner is endowed with the authority to formulate the policy associated with his own files. The idea of owners determining the essential attributes which are indispensable to get access to the files not only provides user-friendly service, but liberates the provider of cloud storage from managing the keys. Apart from that, owners are responsible for generating blocks which record the encrypted Ks using CP-ABE.

User: Users try to get access to the files shared online in the cloud storage system. The first step is to check the conrresponding data items on the blockchains to get the ciphertext of Ks. If their private keys, which are labeled with a set of attributes, are able to pass the access structure formulated by the data owner, they will decrypt the K from the blocks and decrypt the cloud files smoothly. By contrast,

they are not supposed to get the K if their attributes are not in line with the ciphertexts policy.

Cloud Service Provider: Cloud service companies provide remote storing capacity for clients and ease the process of sharing their files online. However, just like the Key Generation Center, they are considered to be honest but curious. In order to preserve the privacy of clients, files are encrypted before uploaded into the storing center. Different from the traditional schemes, Cloud Service Provider is not in charge of controlling the access to stored data any longer to avoid information leakage or destruction.

2.2. Threat Model

The entities in the system may threat the system in the following ways:

Key Generation Center: The KGC, which is in charge of generating and administration of clients secret keys, may cause the leakage of keys given that it learns the encrypted contents as much as possible.

Data Owner: data owners may be involved in some dishonest behaviors: firstly, some owners might want to repudiate the data record in the blockchains; secondly, they may tamper the files stored in the cloud; additionally, some may launch impersonation attacks.

User: as the requestors of the files stored in the cloud server,users may try to decrypt those files which they have no legal access to. In other words, they may collude with others and combine their attributes together. In this way, they might decrypt some files that they don't have enough attributes to pass the access structure on their own.

Cloud Service Provider: Cloud service companies are also viewed as semi-trusted, so clients would suffer from their snooping sensitive data. Whats more, they may try to divulge clients personal information to make profits.

2.3. Design Goals

In order to meet the requirements for CP-ABE based data access control for cloud storage with blockchains and withstand the adversary model which may compromise the performance of our system, the following properties are the pre-requisites for the safe functioning of the data access control scheme:

1) Confidentiality. Our scheme should provide the confidentiality of files in the cloud storage system, because the clients consider the cloud service provider as untrustworthy which may snoop their sensitive information.
2) Decentralization. Utilizing the technology of blockchains, we eliminate the administration center. Different from traditional schemes, we remove the authority of key-management from the cloud service provider and avoid the problems brought by untrustworthy third-party.
3) Fine-grained access control. One of our goals lies in individualized access policy designed by the owners themselves, meanwhile eliminating the need for cloud server to block unauthorized access to sensitive information.
4) Verifiability. Only when the identity of the data owner who created blocks is confirmed can users of the data decrypt the exact files he or she needs without being concerned about the authenticity and integrity of them.
5) Anti-collusion attack. Our scheme should guarantee that collusion attack to attribute-based access control is invalid, which means the colluding users with different attributes cannot decipher additional ciphertext through the combined attribute set.
6) Data integrity. Our scheme should ensure that once the record is formulated in the blockchain, which confers the willingness of the data owner to share the data online, the record cannot be tampered or denied.

3. The Proposed Scheme

In our scheme, we reasonably assume that the files uploaded by data owners are authentic and harmless. According to CP-ABE, private keys of users are identified with a set of attributes. A party that wishes to encrypt a message must specify a policy through an access tree structure. Each interior node of the tree is a threshold gate while the leaf nodes are associated with attributes. A user will be able to decrypt a ciphertext with a given private key only when the attributes from the private key are included by the leaf nodes of the tree. We utilize the same notation as[11] to describe the access structure, though the attributes in our case are used to identify the private keys.

3.1. Initialization

Setup For Key Generation Center, the first step is to Setup for CP-ABE and prepare for the following key-generation and assignment. The setup algorithm[2] takes no input other than the implicit security parameter. It outputs the public parameters PK and a master key MK. The setup algorithm[2] will choose a bilinear group G_0 of prime order p with generator g. Next it will choose two random exponents $\alpha, \beta \in Z_p$. The public key is published as: $PK = G_0, g, h = g^{\beta}, e(g,g)^{\alpha}$, and the master key MK is (β, g^{α}).

Key Generation The core of KGCs tasks is to generate secret keys and assign them to users based on their descriptive attributes. Using the public and secret parameters in the CP-ABE scheme, the KGC grants different access levels to different users (groups) to realize fine-grained access control over the Ks, which further determine the access to the

sensitive files stored in the cloud system. The key generation algorithm [2] will take as input a set of attributes S and output a key that identifies with that set. The algorithm first chooses a random $r \in Z_p$, and then random $r_j \in Z_p$ for each attribute $j \in S$. Then it computes the key as

$$SK = (D = g^{(\alpha+r)/\beta}, \forall j \in S : D_j = g^r \cdot H(j)^{r_j}, D'_j = g^{r_j})$$

3.2. Uploading Files

Encryption of Files Before data owners upload their sensitive files into the cloud storing center, the files should be encrypted using symmetrical encryption algorithms with K as the encryption key. $EncF = Enc_k(Files)$

Encryption of K In this phase, the data owner utilizes CP-ABE for K. The encryption algorithm[2] encrypts K under the tree access structure T. The algorithm first chooses a polynomial q_x for each node x (including the leaves) in the tree T. These polynomials are chosen in the following way in a topdown manner, starting from the root node R. For each node x in the tree, set the degree d_x of the polynomial q_x to be one less than the threshold value k_x of that node, that is, $d_x = k_x - 1$.Starting with the root node R the algorithm chooses a random $s \in Z_p$ and sets $q_R(0) = s$. Then, it chooses d_R other points of the polynomial q_R randomly to define it completely. For any other node x, it sets $q_x(0) = q_{\text{parent}}(x)(index(x))$ and chooses d_x other points randomly to completely define q_x. Let Y be the set of leaf nodes in T. The ciphertext is then constructed by giving the tree access structure T and computing

$$CT = (T, \tilde{C} = K(g,g)^{\alpha s}, C = h^s,$$
$$\forall y \in Y : C_y = g^{q_y(0)}, C'_y = H(\text{att}(y))^{q_y(0)})$$

Record of K After being encrypted with Ciphertext-Policy ABE, K should be recorded in the blockchain in the form of ciphertext. Compared with applying CP-ABE to the files directly, encryption of K, which is much shorter than the whole file, is absolutely more efficient and safe. Figure 2 shows the concrete structure of the blockchain, which includes data owners public key, CT, Hash Value[16], data owners signature[9], [10] and the ID of the corresponding files. When complete the proof-of-work and generate a valid block including the ciphertext of K (CT), the Record phase is finished. The specific realization of digital signature and mining are not the core of our paper, so readers might consult [5], [12], [13], [14], [15]. The items generated in the blocks are closely related to each other.

Algorithm 1 Generation of K-record

Input: owner's private key kr, owner's public key kp, $CT(K), EncF, Record_{j-1}$

Output: $Record_j$

owner executes:
$FileID = HASH(CT(K), EncF)$
$HashValue = HASH(kp, CT(K), FileID, Record_{j-1}$
$, timestamp_j)$
$Owner'sSignature = SIG(kr, HashValue)$
$Record_j = kp \| FileID \| HashValue$
$\| Owner'sSignature \| CT(K)$
return $Record_j$

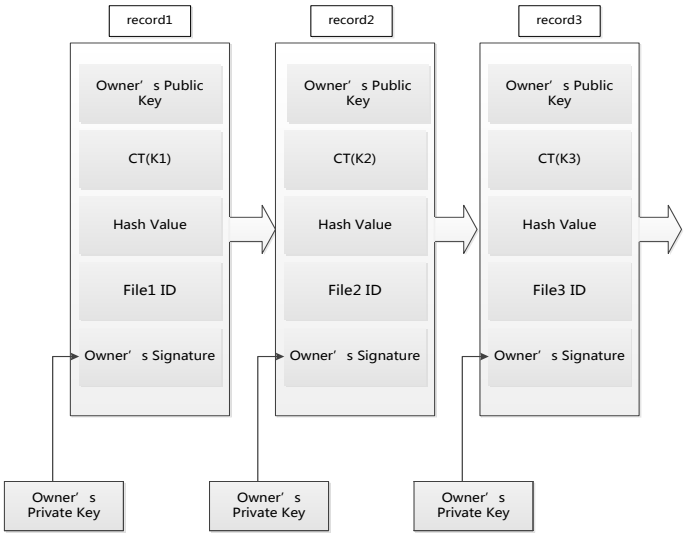


Figure 2. Structure of record-blockchain

3.3. Downloading Files

Decryption of K Let the decryption procedure as a recursive algorithm[2]. For ease of exposition we present the simplest form of the decryption algorithm. We first define a recursive algorithm DecryptNode (CT, SK, x) that takes as input a ciphertext $CT = (T, \tilde{C}, C, \forall y \in Y : C_y, C'_y)$, a private key SK, which is associated with a set S of attributes, and a node x from T. If the node x is a leaf node then we let $i = \text{att}(x)$ and define as follows: If $i \in S$, then

$$\begin{aligned}\text{DecryptNode}(CT, SK, x) &= \frac{e(D_i, C_x)}{e(D'_i, C'_x)} \\ &= \frac{e(g^r \cdot H(i)^r_i, h^{q_x(0)})}{e(g^{r_i}, H(i)^{q_x(0)})} \\ &= e(g,g)^{rq_x(0)}\end{aligned}$$

We now consider the case when x is a non-leaf node. The algorithm DecryptNode(CT, SK, x) then proceeds as

follows: For all nodes z that are children of x, it calls DecryptNode(CT, SK, z) and stores the output as F_z. Let S_x be an arbitrary k_x- sized set of child nodes z.such that $F_z \neq \perp$. If no such set exists then the node was not satisfied and the function returns$\perp$. If $i \neq S$, then we define DecryptNode$(CT, SK, x) = \perp$. Now we can define the decryption algorithm, which begins by simply calling the function on the root node R of the tree T. If the tree is satisfied by S we set $A = DecryptNode(CT, SK, r) = e(g,g)^{rq_R(0)} = e(g,g)^{rs}$. The algorithm now decrypts by computing

$$\widetilde{C}/(e/(C,D)/A) = \widetilde{C}(e(h^s, g^{(\alpha+r)/\beta})/e(g,g)^{rs}) = K.$$

Decryption of Files Finishing the decryption of K, users are able to decrypt the files with it and get the plaintext. Any efficient symmetrical decryption algorithm is acceptable. Cloud service providers may tailor encryption methods to their needs. $Files = Dec_k(EncF)$

3.4. Rekeying

Generally, data owner needs to change the encryption key (K) once in a while for the sake of safety. Additionally, data owner may want to renew the policy based on current situation, and make a change on the data access. In our system, rekeying phase, which is indispensable, is designed to be not only efficient but user-friendly as well. All the work data owner need to finish is to formulate a new block and broadcast it online. In the new block, the only thing that is different from the old one is the CT, which is the ciphertext of the new K. The structure of the block is still the same, which is depicted in Figure 2.

4. Analysis Of Scheme

We now demonstrate that our scheme meets all the requirements below.

4.1. Confidentiality

Even though the cloud server is considered as semi-trusted (both honest and curious), clients don't have to be concerned about their privacy of the stored files. Using symmetrical encryption algorithms guarantees the safety and the working efficiency at the same time. We eliminate the potential problems brought by storing the plaintext in the cloud server directly. As $EncF = Enc_k(Files)$, if the cloud service provider tries to learn the secret information in the server, it will have to get K to perform $Files = Dec_k(EncF)$. However, the premise of getting K is to look up to the record-blocks, and execute DecryptNode (CT, SK, x). In other words, the service provider has to be equipped with corresponding attributes to decrypt the files stored in the cloud, which makes the service provider equivalent to normal users.

4.2. Decentralization

By recording key parameters on the blockchain, which serves as a decentralized and open ledger, we successfully eliminate the problems caused by unreliable third-party. Traditionally, the cloud service providers are in charge of determining the access levels of users and blocking out illegal visits to the cloud server. However, considering their characterisctics–honest but curious, letting the third-party to take on the management of relevant security parameters is clearly not sound. Consequently, we combine the relevant parameters together and generate a genuine and unique record for each pair of K and the file. $Record_j = kp \| FileID \| HashValue \| Owner'sSignature \| CT(K)$. In this way, users enjoy the safety provided by our system when there is no untrustworthy third-party that may snoop clients' data.

4.3. Fine-Grained Access Control

The basic function of our system lies in individualized access policy designed by the owners themselves with CP-ABE. Granted with the right to administrate the access permission to their own files, data owners formulate different policies with different access structures and apply them to different files. Only when a user's set of attributes γ satisfies the access tree T_x, the algorithm will execute $T_x(\gamma) = 1$. Next, this user will execute Decrypt (PK, CT, SK) to get K, which will assist him to decrypt the ciphertext of files $Files = Dec_k(EncF)$. Meanwhile, canceling the authority of the untrustworthy provider of the cloud service to block out illegal visits to sensitive information enhances the reliability of our scheme.

4.4. Verifiability

When generating the records in the blockchain, data owners would execute $Owner'sSignature = SIG(kr, HashValue)$. When the users are suspicious of the identity of the creator of the blocks and the resource of the files, they can confirm the digital signature recorded in the block with the data owners public key. Since the blockchain is fixed and tamper-resistant, the record will win complete trust of users. All in all, users can verify the resource and decrypt the exact files he or she needs without being concerned about the authenticity and integrity of them.

4.5. Anti-Collusion Attack

In the downloading phase, users with eligible attributes can only decrypt certain segments. However, aspiring for other information, they may collude with others in order to enlarge their privileges. Our scheme ensures the collusion attack described above is unfeasible. For example, assuming

that users U_1 and U_2 have the attribute set S_1 and S_2 respectively and they want to collude together. Let U_3 have the attribute set S_3 and $S_3 = S_1 \cup S_2$. In other words, U_1 and U_2 try to obtain U_3s secret key and decrypt his or her information. In our scheme, U_1 and U_2 must recover$e(g,g)^{\alpha s}$ to garner U_3s secret key. During the phase of Encryption, the string s from different users have been already randomized, which means U_1 and U_2 cannot recover $e(g,g)^{\alpha s}$. Consequently, U_3s ciphertext cannot be decrypted merely by combining two sets of attributes. Extended to the situation with more than two users, the collusion attack is also invalid.

4.6. Data Integrity

Given that blockchian is defined as a decentralized and transparent ledger, all users share the exactly same information together and witness the creation of blocks online. Based on $HashValue = HASH(kp, CT(K), FileID, Record_{j-1}$, each block contains the information of the previous block. The deceptive data owner would have to forge all the previous blocks before, which is nearly an impossible mission. That is to say, our scheme ensures that once the record is formulated in the blockchain, which confers the willingness of the data owner to share his or her data online, the record is verifiable and permanent.

5. Performance Evaluation

In this section, we mainly focus on the evaluation of computation overhead of our system. The experiments were conducted on a PC (CPU: Intel(R)Core(TM) i5-7200U CPU @ 2.50GHz 2.71GHz, RAM:8G, OS: Windows 10) based on Java Pairing-Based Cryptography Library (JPBC). We have used packages java security and java crypto to implement symmetrical encryption algorithms.

To begin with, we studied the influence of the number of attributes on the computation cost. The two following experiments were based on AES as the symmetrical encryption algorithm for the encryption of files, so the size of K was fixed to 256bit. Depicted in the Figure 3, the Key-Generation time almost increased with the number of attributes in private key at a near-liner trend, whereas the computation cost of encryption and decryption of K approximately kept steady. Given that we only need to encrypt K, which was comparatively short, the experiment result was acceptable. On the other hand, we found that the number of attributes in policy imposed different impact on the phase of encryption and decryption of K. Figure 4 showed that the computation time increased with the number of attributes in policy at a near-liner trend. Consequently, the more stringent the policy is, the more time it takes to process the ciphertext of K.

Next we conducted an experiment to compare different symmetrical encryption algorithms including DES, 3DES and AES. We used files of different sizes consisting of images and text as input for encryption. Then the encrypted output of each file was saved as a file, which in turn became the input for decryption. For better comparison, we used the same input files for all algorithms with ECB Mode. Figure 5 showed that DES took the highest time for encryption overall, while AES took the least. As the size of files increased, the encryption time of DES and 3DES increased significantly while the encryption time of AES almost stayed the same. Accordingly, AES was the premier choice when encrypting large files. All in all, the performance of our scheme is satisfying in practice, and proves that our scheme features high efficiency with symmetrical encryption for files and CP-ABE for K.

6. Conclusion

We create a blockchain-based secure cloud files sharing scheme with fine-grained access control. Different from traditional schemes, our system not only provides fine-grained data access control, but also enhances working efficiency. In our scheme, data owners are able to share their files online without being concerned about the reliability of the cloud service provider, and make their own decisions about the policy of access level. To prove the security of our scheme, we analyze the relevant properties of the sharing system. In the end, we evaluate the influence of the number of attributes and assess different symmetrical encryption algorithms in the performance experiments.

7. Acknowledgment

This work was supported by National Natural Science Foundation of China (61472310, U1536202).

References

[1] Goyal V, Pandey O, Sahai A, et al. *Attribute-based encryption for fine-grained access control of encrypted data*. ACM Conference on Computer and Communications Security. ACM, 2006:89-98.

[2] Bethencourt J, Sahai A, Waters B. *Ciphertext-Policy Attribute-Based Encryption*.Security and Privacy, 2007. SP '07. IEEE Symposium on. IEEE, 2007:321-334.

[3] Ling C, Newport C. *Provably secure ciphertext policy ABE*. ACM Conference on Computer and Communications Security, 2007:456-465.

[4] Sun G Z, Dong Y, Li Y. *CP-ABE based data access control for cloud storage*. Journal on Communications, 2011, 32(7):146-152.

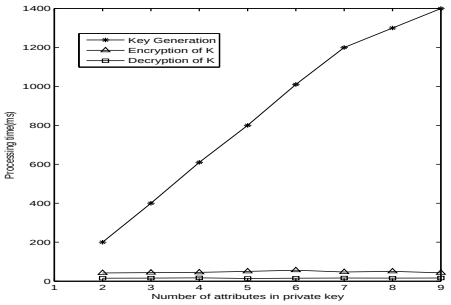


Figure 3. Different number of attributes in private key

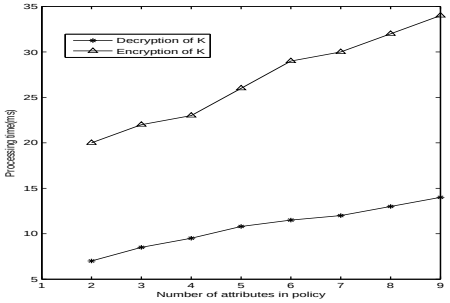


Figure 4. Different number of attributes in policy

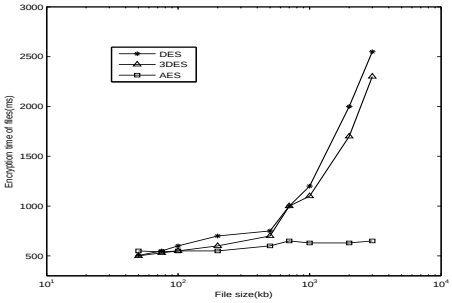


Figure 5. Comparing encryption time of different algorithms

[5] S. Nakamoto.*Bitcoin: A peer-to-peer electronic cash system, Consulted*,2008.

[6] A.J.e.a. Park S, Pietrzak K. *Spacecoin: A cryptocurrency based on proofs of space*.IACR Cryptology ePrint Archive 2015,: 1C26.

[7] Narayanan, Arvind. *Bitcoin and cryptocurrency technologies: A comprehensive introduction*. Princeton University Press ,2016.

[8] Sahai A, Waters B. *Fuzzy Identity-Based Encryption*.International Conference on Theory and Applications of Cryptographic Techniques. Springer-Verlag, 2005:457-473.

[9] J. ZHANG, J. MA, and S. Moon.*Universally composable one-time signature and broadcast authentication*. Science China Information Sciences,vol. 53, no. 3, pp. 567C580, 2010.

[10] X. Dong, H. Qian, and Z. Cao.*Provably secure rsa-type signature based on conic curve*. Wireless Communications and Mobile Computing,vol. 9, no. 2, pp. 217C225, 2009.

[11] Goyal V, Jain A, Pandey O, et al.*Bounded Ciphertext Policy Attribute Based Encryption*. Automata, Languages and Programming. DBLP, 2008:579-591.

[12] M. Swan.*Blockchain: Blueprint for a new economy*. OReilly Media.Inc.2015.

[13] Shamir A.*Identity-Based Cryptosystems and Signature Schemes*. Lect.notes Comput.sci, 1984, 196(2):47-53.

[14] Yuan C, Xu M X, Si X M. *Research on a New Signature Scheme on Blockchain*.2017, 2017(2):1-10.

[15] He D, Tian M, Chen J. *Insecurity of an efficient certificateless aggregate signature with constant pairing computations*. Elsevier Science Inc. 2014.

[16] Hsieh W B, Leu J S. *A dynamic identity user authentication scheme in wireless sensor networks*. Wireless Communications and Mobile Computing Conference. IEEE, 2013:1132-1137.

刘予珂, Welcome to NEEA TOEFL iBT® Online Registration System

NEEA ID: 8576176 **ETS ID:** 13574216 **Account Balance:** RMB¥0.00

Log Out

MY PROFILE
View Profile
Update Login Password
FINANCE
Payments
Request a Refund
TOEFL iBT® VALUE PACKAGE
Purchase Value Package
View Value Package
TOEFL iBT® REGISTRATION
Search Seats
Register for Test
View Orders
TOEFL iBT® POST-TEST
View Score

View Scores

TOEFL scores are valid and posted online for 2 years.

Finished Test

Program	TOEFL iBT®
ETS Registration Number	0000000032701112
Test Date	Saturday, April 21, 2018
Test Center	STN80115A Shaanxi Normal University
Test Status	CHECKED IN

Score

Listening	Speaking	Reading	Writing	Total
30	26	29	29	114

View Scores

Score Recipients View/Add **Valid for two years begin with the test day**

Score Report Mailing

Mailing Address

Address	陕西省西安市西沣路兴隆段266号
Post Code	710126
Mobile Number	18971159579

Status of Score Report Mailing
(Score report will be mailed to the above address by EMS within 8 weeks after your test date. Please check.)

Mailing Status	Score report has been sent
EMS Tracking Number	1104366093815 Please use the following way to check the status of delivery: EMS website: http://www.ems.com.cn Service hotline: 11183
Delivery Date	20180604

YUKE LIU

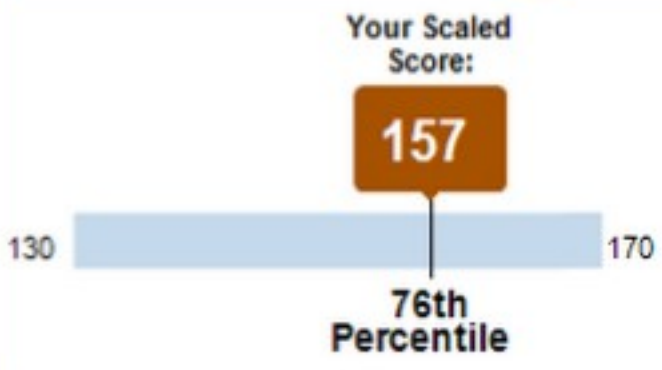
Address: 266 XINGLONG SECTION OF XIFENG, ROAD, XI'AN, SHAANXI, XI'AN, Shaanxi, 710126 China
Email: yukeliu98@163.com
Phone: 86-18971159579
Date of Birth: January 2, 1998
Social Security Number (Last Four Digits):
Gender: Female
Intended Graduate Major: Computer Science (0402)

Most Recent Test Date: March 17,

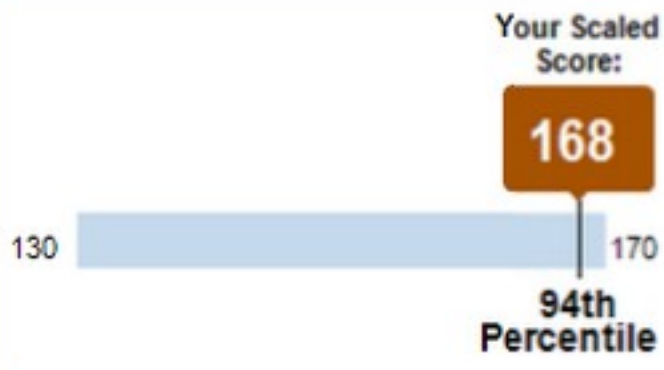
Registration Number: 2810357

Your Scores for the General Test Taken on March 17, 2018

Verbal Reasoning



Quantitative Reasoning



Analytical Writing

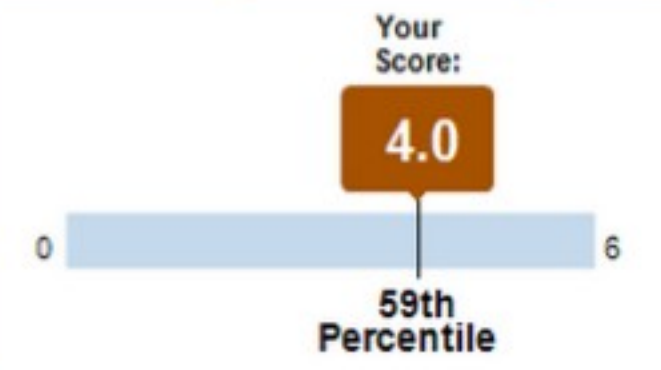


Image graphs of the General Test Taken on March 17, 2018 Graph of verbal reasoning with your scaled score of 157 out of 170 which is the 76th percentile. Graph of quantitative reasoning with your scaled score of 168 out of 170 which is the 94th percentile. Graph of analytical writing with your score of 4.0 out of 6 which is the 59th percentile.

Your Test Score History

General Test Scores

	Verbal Reasoning		Quantitative Reasoning		Analytical Writing	
Test Date	Scaled Score	Percentile	Scaled Score	Percentile	Score	Percentile
March 17, 2018	157	76	168	94	4.0	59
December 3, 2017	157	76	169	96	3.5	41

A Blockchain-based Secure Cloud Files Sharing Scheme with Fine-Grained Access Control

Yuke Liu, Junwei Zhang, Qi Gao
School of Cyber Engineering, Xidian University
Xi'an, China
yukeliu98@163.com, jwzhang@xidian.edu.cn, 392761924@qq.com

Abstract

As cloud services greatly facilitate file sharing online, there's been a growing awareness of the security challenges brought by outsourcing data to a third party. Traditionally, the centralized management of cloud service provider brings about safety issues because the third party is only semi-trusted by clients. Besides, it causes trouble for sharing online data conveniently. In this paper, the blockchain technology is utilized for decentralized safety administration and provide more user-friendly service. Apart from that, Ciphertext-Policy Attribute Based Encryption is introduced as an effective tool to realize fine-grained data access control of the stored files. Meanwhile, the security analysis proves the confidentiality and integrity of the data stored in the cloud server. Finally, we evaluate the performance of computation overhead of our system.

Index Terms

blockchains; cloud storage; CP-ABE; access control; data security

1. Introduction

Nowadays, the rapid development of cloud storage has aroused the awareness of privacy-preserving service provided by enterprises. Therefore, cloud storage system should preserve the integrity and access control of confidential data. However, outsourcing sensitive information to cloud service providers may give rise to privacy issues. To address this problem, the common way is to store the data after encryption instead of plaintext. When users wish to establish a policy defining who can decrypt the sensitive data based on their identities, the traditional method is to implement the access control on a coarse level, like giving your private key to another party. Nevertheless, a fine-grained access control over sensitive data is imperative in many situations. For instance, the Academic Affairs Office need to encrypt exam papers stored in the cloud server so that only certain teachers who are in charge of corresponding subjects can decrypt them. Ciphertext-Policy Attribute-Based Encryption is a great contributor to the fine-grained access control according to the specific knowledge of underlying data. However, the traditional CP-ABE scheme makes it extremely demanding to renew encryption keys particularly for small-sized cloud service providers with limited budgets. Consequently, the blockchain technology is introduced to alleviate this problem. By combining Ciphertext-Policy Attribute-Based Encryption and blockchains, an efficient security solution is realized for cloud storage companies concerning users personal data management on a fine-grained level.

Related works Lots of researchers have been trying to optimize ABE schemes. Bethencourt J et al. [2] proposed CP-ABE (Ciphertext-Policy Attribute-Based Encryption) in 2007. In this system, the users secret key is closely associated with a set of descriptive attributes. Only when those attributes are in line with the policy of the ciphertext can this user decrypt the ciphertext. Given that the construction[1] was proved to be secure solely under the generic group model, Newport et al. [3] presented another one which was secure under the standard model to overcome this weakness. SUN Guo-zi et al. proposed a cloud storage mechanism[4] to achieve the safety and privacy of data during sharing and storage services on the internet.

In 2008, S.Nakamoto[5] proposed blockchain-based Bitcoin, a kind of cryptocurrency, along with a worldwide payment system. In the following years, many blockchain-based cryptocurrency systems[6], [7] have been invented and widely used. Blockchain, based on a peer-to-peer network, records in a verifiable and permanent way.

Data access control for cloud storage The CP-ABE based data access control for cloud storage using blockchain has following properties.

Firstly, confidentiality is the premise of other data management works in our system. On the one hand, adversaries may intentionally compromise the data stored in the cloud server, or even steal sensitive information illegally. Moreover, the service provider is considered to be genuine but curious. In this way, preventing the cloud company from leaking or snooping users personal data for its own benefits

becomes a basic safety requirement.

Secondly, this cloud storage system features fine-grained access control. One can build up a secret-sharing policy for their files, ruling out the vexation brought by confirming identity then giving out secret keys individually. For some special occasions, fine-grained access control is a must when visitors are labeled with a set of attributes that indeed determine the access levels of them.

Thirdly, our scheme guarantees the decentralized management of the data that is related with the secret keys. Utilizing blockchain technology, all the owners of data shared online must sign the ciphertext and record on the blocks.

Our contributions Nowadays, the cloud storage system begins to serve as an efficient resource-sharing platform. However, traditional authority management such as the reference monitor[8] is proved to be inefficient and inflexible considering the massive requests for the online resources in the cloud nowadays. Despite the fact that CP-ABE scheme ensures fine-grained access control over users data, we cannot neglect how complex it is for data centers to generate and renew secret keys while checking the authority of visitors. This paper proposes a privacy-preserving scheme to realize the fine-grained access control when sharing the files stored in the cloud by combining CP-ABE and blockchain technology. Its both safe and efficient for owners to record encrypted keys of the files on blockchains and for visitors to decrypt them from the records. Whats more, generating a new block would be the quickest way to inform others that the keys have been changed. Our contributions in this paper are listed below.

1) We define the required characteristics of our scheme including confidentiality of files in the cloud storage system, fine-grained access control policy designed by the owners themselves, verifiability of the identity of the owners, anti-collusion attack to attribute based access control and data integrity.
2) We propose the formal scheme of CP-ABE based efficient data access control for cloud storage with blockchains.
3) We analyze the security of our scheme theoretically, which confirms that our scheme meet the requirements mentioned above.
4) We present experimental performance of our scheme, and the result shows that it is feasible and efficient for both owners and users.

2. Problem Formulations

2.1. System Model

The system model is depicted in Figure 1. This system consists of the following entities: user, data owner, KGC (Key Generation Center), and cloud service provider.

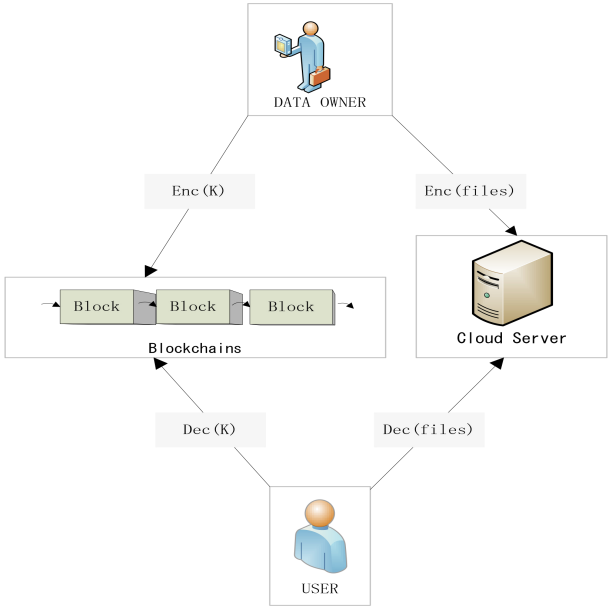


Figure 1. System model

Key Generation Center: To implement Ciphertext-Policy Attribute-Based Encryption, we need a KGC which is in charge of the management and administration of keys, including PK, MSK and SK. Generating, distributing, and revoking SKs to different parties individually are the most essential part of its jobs. When it comes to SKs, the KGC generates and distributes them to users according their attributes, which determine what kind of ciphertext they can decrypt. Generally, the KGC is viewed as honest but curious, which means that it definitely finish the key-assignment tasks without deception, but it may naturally tries to snoop the users information.

Data Owner: its one of the most vital jobs in our scheme to preserve their privacy when data owners are trying to share their sensitive data (in the form of ciphertext) with others remotely via cloud storage system. Besides, the data owner is endowed with the authority to formulate the policy associated with his own files. The idea of owners determining the essential attributes which are indispensable to get access to the files not only provides user-friendly service, but liberates the provider of cloud storage from managing the keys. Apart from that, owners are responsible for generating blocks which record the encrypted Ks using CP-ABE.

User: Users try to get access to the files shared online in the cloud storage system. The first step is to check the conrresponding data items on the blockchains to get the ciphertext of Ks. If their private keys, which are labeled with a set of attributes, are able to pass the access structure formulated by the data owner, they will decrypt the K from the blocks and decrypt the cloud files smoothly. By contrast,

they are not supposed to get the K if their attributes are not in line with the ciphertexts policy.

Cloud Service Provider: Cloud service companies provide remote storing capacity for clients and ease the process of sharing their files online. However, just like the Key Generation Center, they are considered to be honest but curious. In order to preserve the privacy of clients, files are encrypted before uploaded into the storing center. Different from the traditional schemes, Cloud Service Provider is not in charge of controlling the access to stored data any longer to avoid information leakage or destruction.

2.2. Threat Model

The entities in the system may threat the system in the following ways:

Key Generation Center: The KGC, which is in charge of generating and administration of clients secret keys, may cause the leakage of keys given that it learns the encrypted contents as much as possible.

Data Owner: data owners may be involved in some dishonest behaviors: firstly, some owners might want to repudiate the data record in the blockchains; secondly, they may tamper the files stored in the cloud; additionally, some may launch impersonation attacks.

User: as the requestors of the files stored in the cloud server,users may try to decrypt those files which they have no legal access to. In other words, they may collude with others and combine their attributes together. In this way, they might decrypt some files that they don't have enough attributes to pass the access structure on their own.

Cloud Service Provider: Cloud service companies are also viewed as semi-trusted, so clients would suffer from their snooping sensitive data. Whats more, they may try to divulge clients personal information to make profits.

2.3. Design Goals

In order to meet the requirements for CP-ABE based data access control for cloud storage with blockchains and withstand the adversary model which may compromise the performance of our system, the following properties are the pre-requisites for the safe functioning of the data access control scheme:

1) Confidentiality. Our scheme should provide the confidentiality of files in the cloud storage system, because the clients consider the cloud service provider as untrustworthy which may snoop their sensitive information.
2) Decentralization. Utilizing the technology of blockchains, we eliminate the administration center. Different from traditional schemes, we remove the authority of key-management from the cloud service provider and avoid the problems brought by untrustworthy third-party.
3) Fine-grained access control. One of our goals lies in individualized access policy designed by the owners themselves, meanwhile eliminating the need for cloud server to block unauthorized access to sensitive information.
4) Verifiability. Only when the identity of the data owner who created blocks is confirmed can users of the data decrypt the exact files he or she needs without being concerned about the authenticity and integrity of them.
5) Anti-collusion attack. Our scheme should guarantee that collusion attack to attribute-based access control is invalid, which means the colluding users with different attributes cannot decipher additional ciphertext through the combined attribute set.
6) Data integrity. Our scheme should ensure that once the record is formulated in the blockchain, which confers the willingness of the data owner to share the data online, the record cannot be tampered or denied.

3. The Proposed Scheme

In our scheme, we reasonably assume that the files uploaded by data owners are authentic and harmless. According to CP-ABE, private keys of users are identified with a set of attributes. A party that wishes to encrypt a message must specify a policy through an access tree structure. Each interior node of the tree is a threshold gate while the leaf nodes are associated with attributes. A user will be able to decrypt a ciphertext with a given private key only when the attributes from the private key are included by the leaf nodes of the tree. We utilize the same notation as[11] to describe the access structure, though the attributes in our case are used to identify the private keys.

3.1. Initialization

Setup For Key Generation Center, the first step is to Setup for CP-ABE and prepare for the following key-generation and assignment. The setup algorithm[2] takes no input other than the implicit security parameter. It outputs the public parameters PK and a master key MK. The setup algorithm[2] will choose a bilinear group G_0 of prime order p with generator g. Next it will choose two random exponents $\alpha, \beta \in Z_p$. The public key is published as: $PK = G_0, g, h = g^{\beta}, e(g,g)^{\alpha}$, and the master key MK is (β, g^{α}).

Key Generation The core of KGCs tasks is to generate secret keys and assign them to users based on their descriptive attributes. Using the public and secret parameters in the CP-ABE scheme, the KGC grants different access levels to different users (groups) to realize fine-grained access control over the Ks, which further determine the access to the

sensitive files stored in the cloud system. The key generation algorithm [2] will take as input a set of attributes S and output a key that identifies with that set. The algorithm first chooses a random $r \in Z_p$, and then random $r_j \in Z_p$ for each attribute $j \in S$. Then it computes the key as

$$SK = (D = g^{(\alpha+r)/\beta}, \forall j \in S : D_j = g^r \cdot H(j)^{r_j}, D'_j = g^{r_j})$$

3.2. Uploading Files

Encryption of Files Before data owners upload their sensitive files into the cloud storing center, the files should be encrypted using symmetrical encryption algorithms with K as the encryption key. $EncF = Enc_k(Files)$

Encryption of K In this phase, the data owner utilizes CP-ABE for K. The encryption algorithm[2] encrypts K under the tree access structure T. The algorithm first chooses a polynomial q_x for each node x (including the leaves) in the tree T. These polynomials are chosen in the following way in a topdown manner, starting from the root node R. For each node x in the tree, set the degree d_x of the polynomial q_x to be one less than the threshold value k_x of that node, that is, $d_x = k_x - 1$.Starting with the root node R the algorithm chooses a random $s \in Z_p$ and sets $q_R(0) = s$. Then, it chooses d_R other points of the polynomial q_R randomly to define it completely. For any other node x, it sets $q_x(0) = q_{\text{parent}}(x)(index(x))$ and chooses d_x other points randomly to completely define q_x. Let Y be the set of leaf nodes in T. The ciphertext is then constructed by giving the tree access structure T and computing

$$CT = (T, \tilde{C} = K(g,g)^{\alpha s}, C = h^s,$$
$$\forall y \in Y : C_y = g^{q_y(0)}, C'_y = H(\text{att}(y))^{q_y(0)})$$

Record of K After being encrypted with Ciphertext-Policy ABE, K should be recorded in the blockchain in the form of ciphertext. Compared with applying CP-ABE to the files directly, encryption of K, which is much shorter than the whole file, is absolutely more efficient and safe. Figure 2 shows the concrete structure of the blockchain, which includes data owners public key, CT, Hash Value[16], data owners signature[9], [10] and the ID of the corresponding files. When complete the proof-of-work and generate a valid block including the ciphertext of K (CT), the Record phase is finished. The specific realization of digital signature and mining are not the core of our paper, so readers might consult [5], [12], [13], [14], [15]. The items generated in the blocks are closely related to each other.

Algorithm 1 Generation of K-record

Input: owner's private key kr, owner's public key kp, $CT(K), EncF, Record_{j-1}$

Output: $Record_j$

owner executes:
$FileID = HASH(CT(K), EncF)$
$HashValue = HASH(kp, CT(K), FileID, Record_{j-1}$
$, timestamp_j)$
$Owner'sSignature = SIG(kr, HashValue)$
$Record_j = kp \| FileID \| HashValue$
$\| Owner'sSignature \| CT(K)$
return $Record_j$

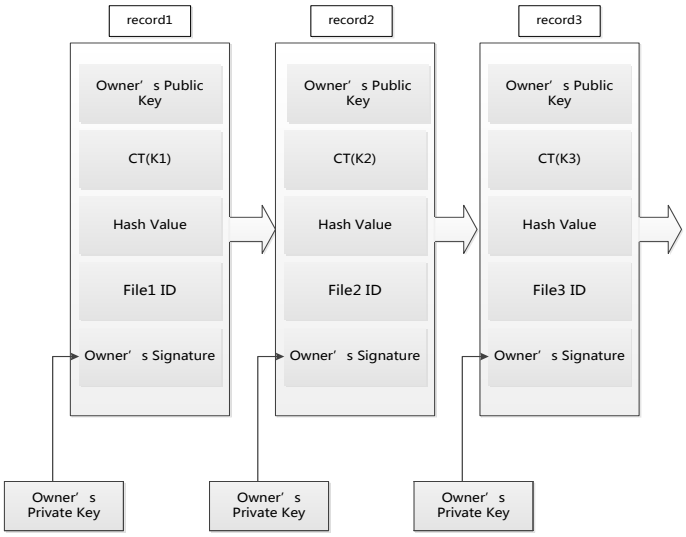


Figure 2. Structure of record-blockchain

3.3. Downloading Files

Decryption of K Let the decryption procedure as a recursive algorithm[2]. For ease of exposition we present the simplest form of the decryption algorithm. We first define a recursive algorithm DecryptNode (CT, SK, x) that takes as input a ciphertext $CT = (T, \tilde{C}, C, \forall y \in Y : C_y, C'_y)$, a private key SK, which is associated with a set S of attributes, and a node x from T. If the node x is a leaf node then we let $i = \text{att}(x)$ and define as follows: If $i \in S$, then

$$\begin{aligned}\text{DecryptNode}(CT, SK, x) &= \frac{e(D_i, C_x)}{e(D'_i, C'_x)} \\ &= \frac{e(g^r \cdot H(i)^r_i, h^{q_x(0)})}{e(g^{r_i}, H(i)^{q_x(0)})} \\ &= e(g,g)^{rq_x(0)}\end{aligned}$$

We now consider the case when x is a non-leaf node. The algorithm DecryptNode(CT, SK, x) then proceeds as

follows: For all nodes z that are children of x, it calls DecryptNode(CT, SK, z) and stores the output as F_z. Let S_x be an arbitrary k_x- sized set of child nodes z.such that $F_z \neq \perp$. If no such set exists then the node was not satisfied and the function returns$\perp$. If $i \neq S$, then we define DecryptNode$(CT, SK, x) = \perp$. Now we can define the decryption algorithm, which begins by simply calling the function on the root node R of the tree T. If the tree is satisfied by S we set $A = DecryptNode(CT, SK, r) = e(g,g)^{rq_R(0)} = e(g,g)^{rs}$. The algorithm now decrypts by computing

$$\widetilde{C}/(e/(C,D)/A) = \widetilde{C}(e(h^s, g^{(\alpha+r)/\beta})/e(g,g)^{rs}) = K.$$

Decryption of Files Finishing the decryption of K, users are able to decrypt the files with it and get the plaintext. Any efficient symmetrical decryption algorithm is acceptable. Cloud service providers may tailor encryption methods to their needs. $Files = Dec_k(EncF)$

3.4. Rekeying

Generally, data owner needs to change the encryption key (K) once in a while for the sake of safety. Additionally, data owner may want to renew the policy based on current situation, and make a change on the data access. In our system, rekeying phase, which is indispensable, is designed to be not only efficient but user-friendly as well. All the work data owner need to finish is to formulate a new block and broadcast it online. In the new block, the only thing that is different from the old one is the CT, which is the ciphertext of the new K. The structure of the block is still the same, which is depicted in Figure 2.

4. Analysis Of Scheme

We now demonstrate that our scheme meets all the requirements below.

4.1. Confidentiality

Even though the cloud server is considered as semi-trusted (both honest and curious), clients don't have to be concerned about their privacy of the stored files. Using symmetrical encryption algorithms guarantees the safety and the working efficiency at the same time. We eliminate the potential problems brought by storing the plaintext in the cloud server directly. As $EncF = Enc_k(Files)$, if the cloud service provider tries to learn the secret information in the server, it will have to get K to perform $Files = Dec_k(EncF)$. However, the premise of getting K is to look up to the record-blocks, and execute DecryptNode (CT, SK, x). In other words, the service provider has to be equipped with corresponding attributes to decrypt the files stored in the cloud, which makes the service provider equivalent to normal users.

4.2. Decentralization

By recording key parameters on the blockchain, which serves as a decentralized and open ledger, we successfully eliminate the problems caused by unreliable third-party. Traditionally, the cloud service providers are in charge of determining the access levels of users and blocking out illegal visits to the cloud server. However, considering their characterisctics–honest but curious, letting the third-party to take on the management of relevant security parameters is clearly not sound. Consequently, we combine the relevant parameters together and generate a genuine and unique record for each pair of K and the file. $Record_j = kp \| FileID \| HashValue \| Owner'sSignature \| CT(K)$. In this way, users enjoy the safety provided by our system when there is no untrustworthy third-party that may snoop clients' data.

4.3. Fine-Grained Access Control

The basic function of our system lies in individualized access policy designed by the owners themselves with CP-ABE. Granted with the right to administrate the access permission to their own files, data owners formulate different policies with different access structures and apply them to different files. Only when a user's set of attributes γ satisfies the access tree T_x, the algorithm will execute $T_x(\gamma) = 1$. Next, this user will execute Decrypt (PK, CT, SK) to get K, which will assist him to decrypt the ciphertext of files $Files = Dec_k(EncF)$. Meanwhile, canceling the authority of the untrustworthy provider of the cloud service to block out illegal visits to sensitive information enhances the reliability of our scheme.

4.4. Verifiability

When generating the records in the blockchain, data owners would execute $Owner'sSignature = SIG(kr, HashValue)$. When the users are suspicious of the identity of the creator of the blocks and the resource of the files, they can confirm the digital signature recorded in the block with the data owners public key. Since the blockchain is fixed and tamper-resistant, the record will win complete trust of users. All in all, users can verify the resource and decrypt the exact files he or she needs without being concerned about the authenticity and integrity of them.

4.5. Anti-Collusion Attack

In the downloading phase, users with eligible attributes can only decrypt certain segments. However, aspiring for other information, they may collude with others in order to enlarge their privileges. Our scheme ensures the collusion attack described above is unfeasible. For example, assuming

that users U_1 and U_2 have the attribute set S_1 and S_2 respectively and they want to collude together. Let U_3 have the attribute set S_3 and $S_3 = S_1 \cup S_2$. In other words, U_1 and U_2 try to obtain U_3s secret key and decrypt his or her information. In our scheme, U_1 and U_2 must recover$e(g,g)^{\alpha s}$ to garner U_3s secret key. During the phase of Encryption, the string s from different users have been already randomized, which means U_1 and U_2 cannot recover $e(g,g)^{\alpha s}$. Consequently, U_3s ciphertext cannot be decrypted merely by combining two sets of attributes. Extended to the situation with more than two users, the collusion attack is also invalid.

4.6. Data Integrity

Given that blockchian is defined as a decentralized and transparent ledger, all users share the exactly same information together and witness the creation of blocks online. Based on $HashValue = HASH(kp, CT(K), FileID, Record_{j-1}$, each block contains the information of the previous block. The deceptive data owner would have to forge all the previous blocks before, which is nearly an impossible mission. That is to say, our scheme ensures that once the record is formulated in the blockchain, which confers the willingness of the data owner to share his or her data online, the record is verifiable and permanent.

5. Performance Evaluation

In this section, we mainly focus on the evaluation of computation overhead of our system. The experiments were conducted on a PC (CPU: Intel(R)Core(TM) i5-7200U CPU @ 2.50GHz 2.71GHz, RAM:8G, OS: Windows 10) based on Java Pairing-Based Cryptography Library (JPBC). We have used packages java security and java crypto to implement symmetrical encryption algorithms.

To begin with, we studied the influence of the number of attributes on the computation cost. The two following experiments were based on AES as the symmetrical encryption algorithm for the encryption of files, so the size of K was fixed to 256bit. Depicted in the Figure 3, the Key-Generation time almost increased with the number of attributes in private key at a near-liner trend, whereas the computation cost of encryption and decryption of K approximately kept steady. Given that we only need to encrypt K, which was comparatively short, the experiment result was acceptable. On the other hand, we found that the number of attributes in policy imposed different impact on the phase of encryption and decryption of K. Figure 4 showed that the computation time increased with the number of attributes in policy at a near-liner trend. Consequently, the more stringent the policy is, the more time it takes to process the ciphertext of K.

Next we conducted an experiment to compare different symmetrical encryption algorithms including DES, 3DES and AES. We used files of different sizes consisting of images and text as input for encryption. Then the encrypted output of each file was saved as a file, which in turn became the input for decryption. For better comparison, we used the same input files for all algorithms with ECB Mode. Figure 5 showed that DES took the highest time for encryption overall, while AES took the least. As the size of files increased, the encryption time of DES and 3DES increased significantly while the encryption time of AES almost stayed the same. Accordingly, AES was the premier choice when encrypting large files. All in all, the performance of our scheme is satisfying in practice, and proves that our scheme features high efficiency with symmetrical encryption for files and CP-ABE for K.

6. Conclusion

We create a blockchain-based secure cloud files sharing scheme with fine-grained access control. Different from traditional schemes, our system not only provides fine-grained data access control, but also enhances working efficiency. In our scheme, data owners are able to share their files online without being concerned about the reliability of the cloud service provider, and make their own decisions about the policy of access level. To prove the security of our scheme, we analyze the relevant properties of the sharing system. In the end, we evaluate the influence of the number of attributes and assess different symmetrical encryption algorithms in the performance experiments.

7. Acknowledgment

This work was supported by National Natural Science Foundation of China (61472310, U1536202).

References

[1] Goyal V, Pandey O, Sahai A, et al. *Attribute-based encryption for fine-grained access control of encrypted data*. ACM Conference on Computer and Communications Security. ACM, 2006:89-98.

[2] Bethencourt J, Sahai A, Waters B. *Ciphertext-Policy Attribute-Based Encryption*.Security and Privacy, 2007. SP '07. IEEE Symposium on. IEEE, 2007:321-334.

[3] Ling C, Newport C. *Provably secure ciphertext policy ABE*. ACM Conference on Computer and Communications Security, 2007:456-465.

[4] Sun G Z, Dong Y, Li Y. *CP-ABE based data access control for cloud storage*. Journal on Communications, 2011, 32(7):146-152.

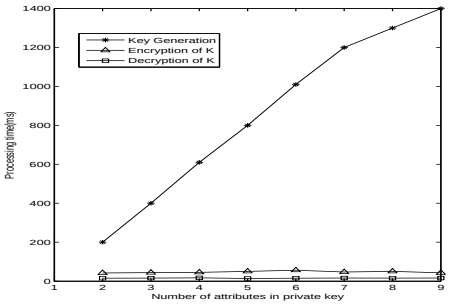


Figure 3. Different number of attributes in private key

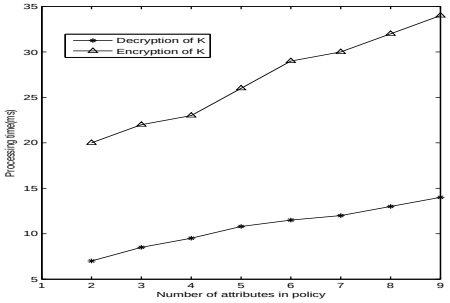


Figure 4. Different number of attributes in policy

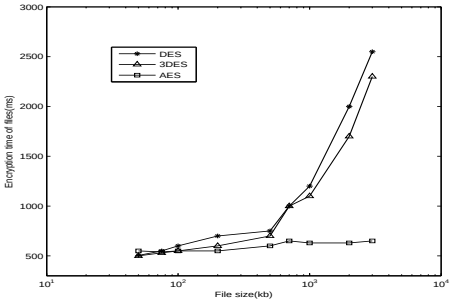


Figure 5. Comparing encryption time of different algorithms

[5] S. Nakamoto.*Bitcoin: A peer-to-peer electronic cash system, Consulted*,2008.

[6] A.J.e.a. Park S, Pietrzak K. *Spacecoin: A cryptocurrency based on proofs of space*.IACR Cryptology ePrint Archive 2015,: 1C26.

[7] Narayanan, Arvind. *Bitcoin and cryptocurrency technologies: A comprehensive introduction*. Princeton University Press ,2016.

[8] Sahai A, Waters B. *Fuzzy Identity-Based Encryption*.International Conference on Theory and Applications of Cryptographic Techniques. Springer-Verlag, 2005:457-473.

[9] J. ZHANG, J. MA, and S. Moon.*Universally composable one-time signature and broadcast authentication*. Science China Information Sciences,vol. 53, no. 3, pp. 567C580, 2010.

[10] X. Dong, H. Qian, and Z. Cao.*Provably secure rsa-type signature based on conic curve*. Wireless Communications and Mobile Computing,vol. 9, no. 2, pp. 217C225, 2009.

[11] Goyal V, Jain A, Pandey O, et al.*Bounded Ciphertext Policy Attribute Based Encryption*. Automata, Languages and Programming. DBLP, 2008:579-591.

[12] M. Swan.*Blockchain: Blueprint for a new economy*. OReilly Media.Inc.2015.

[13] Shamir A.*Identity-Based Cryptosystems and Signature Schemes*. Lect.notes Comput.sci, 1984, 196(2):47-53.

[14] Yuan C, Xu M X, Si X M. *Research on a New Signature Scheme on Blockchain*.2017, 2017(2):1-10.

[15] He D, Tian M, Chen J. *Insecurity of an efficient certificateless aggregate signature with constant pairing computations*. Elsevier Science Inc. 2014.

[16] Hsieh W B, Leu J S. *A dynamic identity user authentication scheme in wireless sensor networks*. Wireless Communications and Mobile Computing Conference. IEEE, 2013:1132-1137.

西安电子科技大学
XIDIAN UNIVERSITY

地址：中国陕西省西安市西沣路兴隆段266号.710126
电话：+86-29-81891850
传真：+86-29-81891850
网址：http://www.xidian.edu.cn/
邮箱：dag@mail.xidian.edu.cn

Add：No.266.Xinglong Section of Xifeng Road.Xi' an China.710126
Tel：+86-29-81891850
Fax：+86-29-81891850
Web：http://www.xidian.edu.cn/
E-mail：dag@mail.xidian.edu.cn

证 明

刘予珂，女，1998年1月生，学号：15180110044。该生自2015年8月至今在我校网络与信息安全学院信息安全专业学习，在前三年本专业成绩总排名中排第5名（专业总人数为158人）。

特此证明。

西安电子科技大学档案馆
2018年9月

CERTIFICATE

Liu Yuke, female, born in January, 1998. Her student ID: 15180110044. She has been majoring in Information Security in the School of Cyber Engineering from August, 2015 to present. For the first 3 years, she has ranked the 5th among total 158 students in her major.

XIDIAN University Archives

September, 2018

Northwestern | THE GRADUATE SCHOOL

Recommendation Form

The Graduate School Northwestern University Evanston, IL 60208-1113

Applicant Name: **Yuke Liu**

Program: **Computer Science: MS**

Applicant Waived Rights*: **This applicant has waived the right to view their recommendation.**

Recommender Name: **Junwei Zhang**

Organization Name: **Xidian University**

Title: **Associate Professor**

E-mail Address: **jwzhang@xidian.edu.cn**

Telephone Number: **+86 13609184562**

Relationship to Applicant: **teacher and mentor**

Certification (Date): **10-11-2018**

*"Public Law 93-380, Educational Amendments Act of 1974, grants students the right to have access to letters of recommendation in their placement files. By selecting the "Waive access" option you are waiving access to these letters."

西安电子科技大学
XIDIAN UNIVERSITY

地址：中国陕西省西安市西沣路兴隆段266号.710126
电话：+86-29-81891850
传真：+86-29-81891850
网址：http://www.xidian.edu.cn/
邮箱：dag@mail.xidian.edu.cn

Add：No.266.Xinglong Section of Xifeng Road.Xi'an China.710126
Tel：+86-29-81891850
Fax：+86-29-81891850
Web：http://www.xidian.edu.cn/
E-mail：dag@mail.xidian.edu.cn

October 6, 2018

To whom it may concern:

It's my pleasure to provide strong recommendation for Yuke Liu as she applies for the graduate program at your distinguished university. She was once a student in my course of Network Security Theory and Technology. Checking my publications in advance, Yuke contacted me for guidance of networks research. Her eagerness to learn was impressive, and her grade (95) in my theoretical course was outstanding as well. Thus, I offered her a chance to work with me. Something uppermost about Yuke Liu was that she demonstrated her passion, efficiency and meticulousness during the time working with me.

Indeed, her work was highly productive. She was supposed to write an academic paper about our project of designing a blockchain-based scheme for secure cloud file-sharing with fine-grained access control. At first, she was asked to read extensively about relevant topics. To my surprise, she submitted a detailed reading report illustrating her accurate understanding of the core algorithm within just 10 days. Then, she conducted a simulation experiment about the system's performance evaluation independently. Providing timely feedback to my suggestions, she eventually finished writing an innovative paper and published it later.

Besides, Yuke has a keen eye for minute details. In my lecture about IPsec protocols, I explained that when two layers of SAs were used to protect IP packets, Encapsulating Security Payload would encrypt the new IP packet. In effect, the ESP only encrypts the payload of IP packets. Nevertheless, I mistakenly said that the new IP header would also be encrypted. The next day, Yuke came to my office to point it out after consulting reference books. She was the only one that was conscious of my mistake in a class of 120 students. It was a fantastic example of her critical thinking.

Yuke distinguishes herself as an exceptional learner with her curiosity, diligence and endless questioning. I strongly support her decision to go further study in graduate program. Please contact me at jwzhang@xidian.edu.cn or +86 13609184562 if you have any further questions concerning Yuke's qualifications.

Sincerely,

Junwei Zhang
Associate Professor
Xidian University
School of Cyber Engineering

Northwestern | THE GRADUATE SCHOOL

Recommendation Form

The Graduate School Northwestern University Evanston, IL 60208-1113

Applicant Name: **Yuke Liu**

Program: **Computer Science: MS**

Applicant Waived Rights*: **This applicant has waived the right to view their recommendation.**

Recommender Name: **Yueyu Zhang**

Organization Name: **Xidian University**

Title: **Associate Professor**

E-mail Address: **yyzhang@xidian.edu.cn**

Telephone Number: **+86 18192393376.**

Relationship to Applicant: **Teachers of many courses; research advisor**

Certification (Date): **10-08-2018**

*"Public Law 93-380, Educational Amendments Act of 1974, grants students the right to have access to letters of recommendation in their placement files. By selecting the "Waive access" option you are waiving access to these letters."

西安电子科技大学
XIDIAN UNIVERSITY

地址：中国陕西省西安市西沣路兴隆段266号.710126
电话：+86-29-81891850
传真：+86-29-81891850
网址：http://www.xidian.edu.cn/
邮箱：dag@mail.xidian.edu.cn

Add：No.266.Xinglong Section of Xifeng Road.Xi'an China.710126
Tel：+86-29-81891850
Fax：+86-29-81891850
Web：http://www.xidian.edu.cn/
E-mail：dag@mail.xidian.edu.cn

October 2, 2018
Dear Graduate Admissions Officer:

I am writing on behalf of Yuke Liu's application for the graduate program at your university. As a student in my courses of Linear Algebra and Wireless Communication Security, she stood out to me because of her strong motivation, task commitment and collaborative nature. I believe she will thrive as an excellent student in the graduate program.

Yuke always has an ambition to undertake a graduate study in USA. In fact, knowing my experience in Michigan State University as a visiting scholar, she came to me for a talk about her dream of studying overseas. Also, she has a definite plan to achieve it by pursuing a tight schedule every day.

Her work ethic and reasoning ability are major contributors to her high grades in my courses. She had impressive powers of concentration in class. Always sitting at the front row, she never got distracted. She was good at generalizing the key ideas. Her insightful notes was shared and admired by her peers.

As a teaching assistant in my courses, Yuke demonstrated good communication skills and an optimistic attitude. I once assigned a task of completing seven relevant experiments in one day, including GPS spoofing, FM signal simulation and so on, which turned out to be quite demanding for my students. The next day, she came to my office and listed some specific difficulties in conducting the project in a very polite way. Later, she held a seminar to provide possible solutions to her fellow students with my help. Instead of complaining, she always seeks a positive outlook when confronting with hardships.

I'm certain that Yuke has a sound intellectual background for her further study. I enthusiastically support her application for this graduate program to go after her career dream. If further details on my work with Yuke would be helpful, do contact me at yyzhang@xidian.edu.cn, or at +86 18192393376.

Sincerely,

Yueyu Zhang

Yueyu Zhang
Associate Professor
School of Cyber Engineering
Xidian University

Northwestern | THE GRADUATE SCHOOL

Recommendation Form

The Graduate School Northwestern University Evanston, IL 60208-1113

Applicant Name: **Yuke Liu**

Program: **Computer Science: MS**

Applicant Waived Rights*: **This applicant has waived the right to view their recommendation.**

Recommender Name: **Shiyang He**

Organization Name: **Xidian University**

Title: **Assistant Professor**

E-mail Address: **syhe@xidian.edu.cn**

Telephone Number: **+86 18192129285**

Relationship to Applicant: **Teacher; research advisor**

Certification (Date): **10-09-2018**

*"Public Law 93-380, Educational Amendments Act of 1974, grants students the right to have access to letters of recommendation in their placement files. By selecting the "Waive access" option you are waiving access to these letters."

西安电子科技大学
XIDIAN UNIVERSITY

地址：中国陕西省西安市西沣路兴隆段266号.710126
电话：+86-29-81891850
传真：+86-29-81891850
网址：http://www.xidian.edu.cn/
邮箱：dag@mail.xidian.edu.cn

Add：No.266.Xinglong Section of Xifeng Road.Xi' an China.710126
Tel：+86-29-81891850
Fax：+86-29-81891850
Web：http://www.xidian.edu.cn/
E-mail：dag@mail.xidian.edu.cn

October 8,2018

Dear Admissions Committee:

I am delighted to write this recommendation letter in strong support of Yuke Liu. As an assistant professor in School of Cyber Engineering at Xidian University, I offer two courses for undergraduates, namely Java Programming and Software Inverse Engineering. Yuke was a tremendous student in both of my challenging courses.

She was a vigorous eager learner. She always sat in the front row to get more concentrated. Sometimes, she raised insightful questions like "how to realize the string function from C language using assembly language?" after class, indicating her devotion to coursework. Eventually, she got an incredibly high score of 96/100 in SIE.

Yuke was not afraid of confronting challenges. SIE covers a wide range of topics, including windows program development, microcomputer and assembly language, which baffled the students initially. Yuke tried to modify the code to realize new Dll injection after I demonstrated Windows API hooking, which impressed me. In Java class, she told me she had moments of panic when her code couldn't run and her partners were not cooperative. Under my guidance, she divided the complex project into small modules, and conquered them one by one. Finally, she fulfilled the task exceptionally well with her sheer tenacity.

Also, Yuke provided valuable help as my teaching assistant. She would arrange available classrooms for our course seminars, collect and distribute students' homework, and grade students' assignments for me. Meanwhile, she often came to my office to discuss the students' feedbacks on my courses with me, which helped me adjust my teaching plan accordingly.

Maybe Yuke is not outlandishly more intelligent than her peers, but she is clearly the most industrious one in my class. And she is very dependable and responsible as a workmate. I believe she is a qualified applicant for your graduate program.

Sincerely,

Shiyang He

Shiyang He
Assistant professor
Xidian University
School of Cyber Engineering
syhe@xidian.edu.cn
+86 18192129285