



**A NEW DATA-CENTRIC AUTHENTICATION AND AUTHORIZATION
MECHANISM FOR MULTILAYER SYSTEMS**



By CANAN NİYZE SOBA

DECEMBER 2018

A NEW DATA-CENTRIC AUTHENTICATION AND AUTHORIZATION
MECHANISM FOR MULTILAYER SYSTEMS

A THESIS SUBMITTED TO
THE GRADUATE SCHOOL OF NATURAL AND APPLIED
SCIENCES OF
ÇANKAYA UNIVERSITY



BY
CANAN NİYZE SOBA

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE
DEGREE OF
MASTER OF SCIENCE
IN
COMPUTER ENGINEERING
DEPARTMENT

DECEMBER 2018

Title of the Thesis: **A New Data-Centric Authentication And Authorization Mechanism For Multilayer Systems**

Submitted By **Canan Niyaze SOBA**

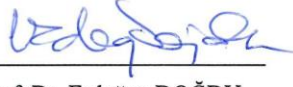
Approval of the Graduate School of Natural and Applied Sciences, Çankaya University.



Prof. Dr. Can ÇOĞUN

Director


I certify that this thesis satisfies all the requirements as a thesis for the degree of Master of Science.



Prof. Dr. Erdoğan DOĞDU

Head of Department

This is to certify that we have read this thesis and that in our opinion it is fully adequate, in scope and quality, as a thesis for the degree of Master of Science.



Dr. A. Nurdan SARAN

Supervisor

Examination Date: 14 December 2018

Examining Committee Members

Dr. Ins. A. Nurdan SARAN (Çankaya Univ.)

Dr. Ins. Murat YILMAZ (Çankaya Univ.)


Dr. Ins. Tülin ERCELEBI AYYILDIZ (Başkent Univ.)



STATEMENT OF NON-PLAGIARISM PAGE

I hereby declare that all information in this document has been obtained and presented in accordance with academic rules and ethical conduct. I also declare that, as required by these rules and conduct, I have fully cited and referenced all material and results that are not original to this work.

Name, Last Name: Canan Niyaze SOBA

Signature: 

Date: 13.12.2018

ABSTRACT

A NEW DATA-CENTRIC AUTHENTICATION AND AUTHORIZATION MECHANISM FOR MULTILAYER SYSTEMS

SOBA, Canan Niyaze
M.Sc., Department of Computer Engineering
Supervisor: Dr. A. Nurdan SARAN
December, 2018, 56 Pages

Since sensitive data is shared by third parties with the rapid progress of the Internet and cloud technologies, there will be a need for encryption to store these data. There are many methods in the literature to prevent unauthorized access of sensitive data. In this study, to provide access control, new multi-layer access control model in which Role-Based and Attribute-Based Access Control models are used together is presented. The suggested system is an approach that is based on secure sharing and storage of data on the network. Identity based encryption (IBE) and identity based signature (IBS) mechanisms are used for user authentication. At the same time, the Ciphertext-policy Attribute-Based Encryption (CP-ABE) mechanism is used for authorization based on the user-specified attributes on the system. The authentication and authorization mechanism is used for smooth start-up, secure data import and secure data sharing. Revocation is used for authority management which is the biggest problem of such systems. This mechanism provides the controls for situations such as changing the user's attributes in the system or revoking of user authorization. However, if same data is encrypted several times by many users causes unnecessary growth of storage space. To prevent this, a whole mechanism has been proposed by using the deduplication, Convergent Encryption method. Thus, it is shown that the system is obtained with lower bandwidth cost.

Keywords: Identity-based Encryption, Identity-based Signature, Ciphertext-policy Attribute-Based Encryption, Convergent Encryption, Revocation Mechanism

ÖZ

ÇOK KATMANLI SİSTEMLER İÇİN VERİ MERKEZLİ YENİ BİR KİMLİK DOĞRULAMA VE YETKİLENDİRME MEKANİZMASI

SOBA, Canan Niyaze
Yüksek Lisans, Bilgisayar Mühendisliği Anabilim Dalı
Tez Yöneticisi: Dr. A. Nurdan SARAN
Aralık, 2018, 56 Sayfa

İnternet ve bulut teknolojilerinin hızlı ilerlemesi ile hassas veriler üçüncü taraflar tarafından paylaşıldığından bu verilerin depolanması için şifrelemek bir ihtiyaç olacaktır. Hassas verilerin yetkisiz erişimini engellemek için literatürde, birçok yöntem bulunmaktadır. Bu çalışmada, erişim denetimini sağlamak için Rol Tabanlı ve Öznitelik Tabanlı Erişim Denetim modellerinin birlikte kullanıldığı yeni çok katmanlı erişim denetim modeli sunulmuştur. Önerilen sistem verilerin ağda güvenli paylaşımı ve saklanması planı üzerine kurulmuş bir yaklaşımdır. Kullanıcı kimlik doğrulama için kimlik tabanlı doğrulama (IBE) ve kimlik tabanlı imza (IBS) mekanizmaları kullanılmıştır. Aynı zamanda Şifreli Metin İlkesi Tabanlı Şifreleme (CP-ABE) mekanizması kullanıcıların sistemde belirlenmiş olan özniteliklerine bağlı yetkilendirme için kullanılmaktadır. Kimlik doğrulama ve yetkilendirme mekanizması sistemi sorunsuz başlatma, güvenli veri alımı ve güvenli veri paylaşımı için kullanılmaktadır. Bu tür sistemlerin en büyük sorunu olan yetki yönetimi için ise İptal Mekanizması kullanılmaktadır, bu mekanizma sistemde kullanıcının özniteliklerinin değişmesi ya da kullanıcının yetki iptali gibi durumlarda kontrolleri sağlamaktadır. Bununla birlikte, aynı verinin birçok kullanıcı tarafından birkaç kez şifrelenmesi depolama alanının gereksiz yere büyümesine neden olmaktadır, bunu engellemek için tekilleştirme, Yakınsak Şifreleme, yöntemi kullanılarak bütüncül bir mekanizma önerilmiştir. Böylece daha düşük bant genişliği maliyetiyle elde edilmiş bir sistem olduğu gösterilmektedir.

Anahtar Kelimeler: Kimlik Tabanlı Doğrulama, Kimlik Tabanlı İmza, Şifreli Metin İlkesi Tabanlı Şifreleme, Yakınsak Şifreleme, İptal Mekanizması

ACKNOWLEDGEMENTS

In the realization of this work, my esteemed counselor, who shared her valuable knowledge with me for two years; Dr. A. Nurdan SARAN, my friends Begüm EROĞLU and Harun KIYMAZARSLAN who has been helping me during my studies, and I offer endless gratitude of valuable my family that supports me in all my difficult moments during the work.



TABLE OF CONTENTS

STATEMENT OF NON-PLAGIARISM PAGE ...	Hata! Yer işareti tanımlanmamış.
ABSTRACT	iv
ÖZ	v
ACKNOWLEDGEMENTS	vi
TABLE OF CONTENTS	vii
LIST OF FIGURES	ix
LIST OF TABLES	x
LIST OF ABBREVIATIONS	xi
1. INTRODUCTION	1
2. LITERATURE REVIEW.....	5
2.1. Preliminaries.....	5
2.1.1. Identity Based Encryption	5
2.1.2. Identity Based Signature.....	6
2.1.3. Pairing-Based Cryptography	7
2.1.4. CP-ABE	7
2.2. Related Work.....	13
3. MULTI-LAYER AUTHORIZATION MODEL SCENARIO AND REQUIREMENTS	16
3.1. System Requirements	16
3.2. Multilayer Authorization Mechanism System Design	17
3.3. System Users	18
3.4. Authorization Module	19
3.4.1. Access to the System	21
3.4.2. Network Administrator Controls	22
3.4.3. Authorization Layer – Data Administrator.....	24

3.4.4. Administrator Controls	25
3.5. File Sharing Module	25
3.5.1. Data Owner File Sharing	26
3.6. A Sample Scenario	29
4. SYSTEM CHARACTERISTICS	33
4.1. Revocation Mechanism	33
4.2. Deduplication	35
5. SECURITY ANALYSIS	37
6. EXPERIMENTAL RESULTS	39
7. CONCLUSION	48
REFERENCES	50
APPENDIX	55

LIST OF FIGURES

Figure 1: Data Sharing Scenario	16
Figure 2: Multilayer Authorization Model	19
Figure 3: Multilayer Authorization	20
Figure 4: Start-up phase	22
Figure 5: User Registration	23
Figure 6: Data Sharing Request	26
Figure 7: File Sharing Steps.....	26
Figure 8: Access Tree Structure.....	29
Figure 9: Data Sharing	35
Figure 10: Key Genearion.....	42
Figure 11: Encryption	43
Figure 12: Decryption	43

LIST OF TABLES

Table 1: Identity-Based Key Created by Network Administrator for Users	23
Table 2: User Attribute Definition	24
Table 3: Access Authority Demonstration	29
Table 4: User List.....	34
Table 5: RBAC Encryption Result.....	40
Table 6: CP-ABE Encryption Result	41
Table 7: CP-ABE Encryption Comparison Results	44
Table 8: Comparison of Algorithm	44

LIST OF ABBREVIATIONS

CE	Convergent Encryption
CP-ABE	Cipher-Text Policy Attribute-Based Encryption
C_T	Cipher-Text
IBE	Identity - Based Encryption
IBS	Identity - Based Signature
MSK	Master Key
N	Number
PriK	Identity - Based Private Key
PubK	Public Key
RS_{ID}	Unique Identifier
SecK	Attribute – Based Private Key
Tag	Tag of Data
U	Attribute Set
Z	Time

CHAPTER 1

INTRODUCTION

Information security is one of the most important issues of present-day. Data sharing is a clear and important problem in information security. Information security is a general sequence of steps taken to protect against attacks, such as unauthorized access and modification. These steps may involve various security mechanisms, regulations or company policies. Security mechanisms are used to prevent attacks such as invalid authentication, illegal changes. According to the importance of data in the system, security mechanisms are changing. Attacks to the system get complicated by the importance of data. The security in the systems should be determined according to the security gap analysis determined in that system and the security vulnerabilities detected. The solutions applied to these problems determine the security level of the system. Security policies should determine the limits of authority of the system. Today, the authentication mechanism precedes the authorization system.

In any security system, the identity of the user must first be verified to prevent alterations. The authentication process is the name given to the information assets in general, the access permission operation by evaluating the user attributes. Unauthorized users can be prevented at this layer of the system. This system is determined as the first layer of authorization for security mechanisms.

In the cases needing higher security, authentication becomes insufficient. For a reliable system, a more complex structure than authentication is needed. Besides controlling who is logged into the system, the authorities of the person in the process should also be assessed.

Authorization mechanisms define the authorities on the source that the authenticated user wants to access. Today, authorization mechanisms must have a secure file sharing mechanism that is trying to provide strong security. The principal feature of this

security mechanism system is the encryption of all data and the dealing with the key distribution.

There are various security controls in security mechanisms. In these security controls, not only the decision of who enters the system but also the evaluation of the user authority in the process is necessary. In security controls, methods such as the flexible authorization mechanism constitute the general security layers of the system. These methods support system reliability over the users and attributes.

An effective authentication mechanism should provide control for the entire system. But only the authentication mechanism is not enough for the security of all data like sensitive data. The authenticated user has extensive authority in the system due to lack of security mechanism. This causes security gaps. It causes the data to be lost or appear as unauthorized. A user who has logged into the system can copy all data in the database. It can reach to the unauthorized users. In addition, users can damage the system. Security vulnerabilities can be observed. It may cause unauthorized use or unauthorized access. In-house threats are generally caused by unauthorized access. In order to prevent the security vulnerabilities that have been seen in companies, a flexible structure that determines user authority is needed.

The flexible authorization mechanism restricts access to data not only to prevent access of unauthorized users but also authorized users according to their authorization levels. The reason for restricting the authority among users is that many of the security vulnerabilities that have arisen in recent years have been realized by internal users, and these attacks are devastating to institutions.

In order to prevent defined security vulnerabilities, both authentication and flexible authorization mechanisms must be used together. In such systems, symmetric or asymmetric encryption can be used for authentication. Identity-based encryption is a good approach for authentication and authorization services. Identity-based encryption advanced version is Ciphertext-policy Attribute-Based Encryption (CP-ABE). It can provide flexible and detailed authorization.

When the system is dynamically changed in the used ABE schemes, the system works successfully unless there is distortion in the source or if the attributes are not changed. However, it is always the case that users abuse their authority and violate the rules. When these malicious users are detected, there is no cancellation mechanism in the systems. The system administrator has to edit the entire system from scratch. This is a huge cost and a waste of time. For this reason, a revocation mechanism should be designed at the beginning of the system.

Recently, data management is very important in systems. Now, in every environment, bigger data is coming out. The big data emerges in online social environments or in data processing systems. For this reason, keeping the data safe and efficient is one of the important problems. Together with outsourcing to companies, saving data management costs and increasing security are important points. To effectively use the storage space, cloud computing has adopted a method of deducing data. Deduplication removes redundant data from the annihilate. A single copy of the data is stored and transmitted to the data owners when necessary. Deduplication is doing a significant savings in disk space and network bandwidth.

The authenticity of a document depends on the reality of the document's content and its validity inter-institutions. According to the institutional system layout, the document should be established in a reliable manner. A document is valid if appropriate. At the same time, the document should be reliable not only within the organization but also between institutions. Inter-institutional validity is valid if it can be verified by both institutions. If a document is not changed without authorization, the document is valid. The authenticity of the document can be verified by the document maker with digital signature algorithms. But using the cloud computing and large data, this system appears to be inadequate. For this reason it is important to examine the competence of authorization in various conditions for the reliability of the document.

In the multi-layered model proposed by Soğukpınar and Uğur [1], document reliability and authorization problems and solutions have been produced. The shortcomings of authorization in the model have been identified and the solutions have been developed.

In the developed method, user login system is controlled by Kerberos mechanism. User restrictions were created with access control list. Role-based authorization also provides restrictions based on user characteristics.

In the system proposed by Li et al. [2], the authentication and authorization system of large data has been examined. It has been tried to encrypt data on the network and securely store the data. Public key encryption mechanism is used for user login. Data encryption is performed by determining policies through the qualifications with the CP-ABE mechanism. Despite being a more effective policy, there are some identified deficiencies.

In this study, the system is considered for the security of large data proposed by Li et al. with the multi-tier architecture model proposed by Soğukpınar and Uğur together, a multi-layered mechanism for storage and sharing of institutional sensitive data has been considered, and in addition, the deficiencies have been identified and a security mechanism has been developed.

Contributions of the thesis;

- The user input mechanism has been replaced by the system Identity-Based Control (IBE) mechanism, which is controlled by Kerberos.
- The encryption of the data is performed by the attribute-based encryption (CP-ABE) mechanism instead of the role-based encryption (RBAC). For why, Attribute-based access control can adapt to both authority change and user change.
- Apart from these two researches, there are user and attribute revocation mechanisms in the system and the changes of these data are controlled.
- To increase the efficiency and to prevent the same data being encrypted multiple times, it is checked whether there is a copy of the data in the system.
- The security mechanisms that exist as different in the systems are redesigned from a holistic point of view.

CHAPTER 2

LITERATURE REVIEW

2.1. Preliminaries

2.1.1. Identity Based Encryption (IBE)

The identity-based encryption mechanism is a type of general key encryption algorithm. The recipient must get an authenticate key before sending the message. The IBE mechanism is based on the idea that the user public key (*PubK*) is generated based on a unique identifier of the user. When the user sends encrypted text, the recipient must only know the identifier. A trusted users creates a private key (*PriK*) so that users can view encrypted text. This secret key is generated by the user with a unique identifier [1].

Shamir first introduced the Identity Based Encryption (IBE) mechanism in 1984. The purpose of identity-based encryption is certificate management in electronic mail. When the user sends e-mail, the user encrypts the message with the public key. In addition, it has introduced the encryption mechanism as well as the identity based signature mechanism and has accepted that there are similar encryption mechanisms [2].

IBE systems are found to be suitable system for companies or corporate areas. A reliable third party role required in the system is an appropriate structure for such organizational structures.

IBE Algorithms

Setup Algorithm Security-Parameters (P), Master Key (MSK) and User Identifier (ID) are input. Private Key ($PriK$) is provided to the user.

This algorithm is run when the user wants its own private key. Verification of the validity of the requestor and secure transport of the secret key are the problems that IBE protocols do not address.

Encrypt Security parameter (P), Master Key (MSK) and User Identifier (ID) are received. Cipher-text is given as output [1].

2.1.2. Identity Based Signature

Identity-based encryption proposed by Shamir makes it possible to calculate public keys only for the generic parameters and for the entities with entity definitions. The private key generator calculates the user secret key with the master key and then distributes it to the users. Boneh, Franklin and Cocks suggested that the proposed mechanism is not sufficiently safe and efficient. Therefore, they have conducted a number of studies, including an identity-based signature mechanism.

A general approach to the IBS scheme is to use a normal sign mechanism and to sign a document containing the signer's public key. The simplicity of this technique indicates that the IBS schemes are easier than the IBE schemes [3].

Identity-Based Signature Algorithms

Setup A trusted user runs the algorithm. It produces $PubK$ and MSK . $PubK$ users are notified. The master key is hidden.

The user identifier ($UserID$) and MSK are used for the generation of private keys ($PriK$).

Sign Message (M) User's private identifier (ID) and user private key ($PriK$) are received. Secret key is created on the algorithm message.

Verify The signing user validity is checked against the user's identifier. Accordingly, it is rejected [3].

2.1.3. Pairing-Based Cryptography

The main idea of the system is to provide a pairing between two cryptographic groups that allow new encryption schemes based on the problem that is usually reduced to an easier problem. The algorithms applied to this pairing are Weil and Tate pairings. It contains a very complex mathematics. However, they can be abstracted using group structure and mapping properties.

Bilinear Maps

Bilinear Map is a main match-based structure. $G1$ and $G2$ (prime order q) are treated as two different groups. Even though $G1$ and $G2$ group operations are very different from arithmetical addition and multiplication; $G1$ is used for the additive notation, $G2$ is used for the multiplicative notation. We think that $G1$ has two generators as P and Q and

$$aP = P+P+\dots+P$$

Map (e) is thought to be as follows.

Let $G1$, $G2$ and Gt be cyclic groups.

$$e : G1 \times G2 \rightarrow Gt, u \in G1, v \in G2, a, b \in \mathbb{Z}$$

$$e(u^a, v^b) = e(u, v)^{ab} [4]$$

2.1.4. CP-ABE

Access control restricts unauthorized access to a resource. It is also a security service that limits the flow of information. There are mainly three different access control models known. These are Discretionary, Mandatory and Role-Based. Limitations in the discretionary model are determined by the sharing user. The application of the discretionary model is easy. It is a flexible model for the user. This model does not guarantee the information flow in the system. In the mandatory model, information flow is secured in the strict access control environment. The role-based model

combines the advantages of the discretionary and mandatory access model. Roles are defined as the work activity and user responsibilities.

Public-key encryption is a powerful system while storing and sending data for providing privacy. However, this system works effectively when it knows the identity of the encrypted user of the data and also the public key ($PubK$). But in complex systems, the general keys and identities of all users are not known. In such cases, the user cannot form an effective access control policy as to who can resolve the data. This case has brought about an IBE and ABE mechanism. A user who uses attribute-based encryption can determine the access control policy based on attributes. Thus, only those whose attributes are appropriate can resolve the password of the encrypted text. ABE encryption is suitable for the real applications.

There are two types of attribute-based encryption; Key Policy Attribute-Based encryption (KP-ABE) and Cipher-Text-Policy Attribute-Based Encryption (CP-ABE) [5]. The KP-ABE includes the access policy tree and user attributes in the secret key. Decryption occurs when there are attributes that are specified in the user secret key. In the CP-ABE mechanism, the user secret key is associated with attributes. Encrypted text access is provided by this key. CP-ABE can express the complex relationship between sensitive sources. In distributed environments, the CP-ABE mechanism is used for access control. Updating access policies in a sharing system is one of the difficult issues. However, CP-ABE can solve this problem. The CP-ABE needs to provide the necessary attributes to decrypt the text. This system enhances safety and efficiency [6].

CP-ABE SCHEME

Setup: The algorithm takes a security parameter (k). Generate $PubK$ and MSK .

Key Generation: The algorithms takes MSK and Attribute Set (U). Depending on these, it creates a secret key ($SecK$).

Encrypt: The user encrypts the message (M) using the user $PubK$ and Attribute Based Access Policy.

Decrypt: Displays encrypted text with *PubK*, *SecK* and user attributes.

Revocation for CP-ABE

Due to the dynamic change of the system, there is a possibility of error. Once users have received their credentials during the installation phase, violations of these rules may be made using these authorities. After detecting these malicious users, if there is no revocation mechanism in the system, the system administrator has to regulate the system from the beginning. For this reason, the revocation mechanism should be designed from the beginning of the system. It should be considered that the time and cost will decrease after the revocation mechanism is designed in the system.

This section provides an overview of relevant work in the field of authorization mechanisms. In addition, the proposed multilayer model authorization mechanisms in the study [3] are outlined.

Discretionary Access Control (DAC) mechanism is the first method for access control. It is also called 'user requested access control mechanism'. The access rights that users grant for the objects is defined by Discretionary Control mechanism, i.e., based on the specified user identity and authority of the user, the access list for each object provides access control for users. Each access request to reach an object is checked against the specified authority. In certain situations, object access is allowed by the user, and if there is an authorization mechanism in the system the request is rejected and if the user does not have the necessary feature. The objects to be used in the system are defined by the users in this mechanism. Then, the authorization policy on these objects is indicated. And that only person has object dominance. Some models allow the transmission of objects to another user. But, this authorization model is not valid. For instance, imagine that Alice has created an object therefore Alice becomes the owner of that object. If another user Alice wants to read an authorized object; Alice, the owner of the object A, may permits or deny Alice's access to the other object for the A object. Discretionary Access Control mechanism has a drawback that the information flow is not required. For example, an authorized user to read the data may copy that data. He

may then share the data without prior notice to the owner, because there is no restriction [7].

Mandatory Access Control (MAC) mechanism is another developed method. Based on the classification of objects in the system, the Mandatory Access Control mechanism manages the access. A security level is given to each user, subject and object in the system. The security level about the object depends on the sensitivity of the information in the objects. The security level of the user reflects the user's reliability. Sensitive data access is allowed to some users. Based on the security level the requests are taken. There are two different security levels which are; simple security properties and liberal properties. According to this structure, access permissions are evaluated. The system is not sufficient for the areas requiring practical information like commercial areas [7].

Mandatory Access Control is appropriate for multi-layer military applications. Discretionary Access Control is more appropriate system in order to meet the security requirements of the industrial and civilian government. However, relying on Mandatory Access Control and Discretionary Access Control mechanisms is not sufficient. For the secure transaction requirements, a more centralized and role-based access control mechanism (RBAC) has been developed. This mechanism is role-based access control mechanism. Access authorities are granted to roles, not to users. The roles are associated with a set of permissions, which are actions on objects that define the meaning of the events. The users are assigned to a specific role group and the permissions associated with the roles are defined. So, the authorities become independent of the users. Starting from duties and responsibilities, the authorities are created. It is determined which function is associated with which business function. Permissions are given according to the minimum authorization [8].

Role Based Access Control (RBAC) should be restricted because the ever-increasing user concern. A role is assigned to each user. Each role requires a different set of permissions. Then, in the system many roles are defined. Determining the roles takes a long time and that increases the cost. In order to prevent these problems, developers have expanded Role Based Access Control in many ways. This model is Attribute-

Based Access Control (ABAC). A more flexible structured authorization mechanism is provided by Attribute-based access control, where these mechanisms are considered together [7] [9].

Attribute-based access control is a highly flexible method while providing access based on evaluation of qualifications. The Attribute-based access control is a wise access control model. This is a specific feature, because it controls objects' accesses. It can be considered as a property of something that can be defined and assigned value. Attribute-based access control solutions assess qualitative and environmental situations. Then, it comprises basic skills to set the rules between environmental conditions competences. Attribute-based access control can adapt to authority and user change [9]. An access The attribute-based cryptographic mechanism causes large computational costs to the user due to the complexity of encryption and decryption [10]. It has been determined that it requires a more flexible access structure in attribute-based access and two different systems have been developed for this; Cipher-text policy Attribute-Based Encryption (CP-ABE) and Key policy attribute based encryption scheme (KP-ABE) [11]. The CP-ABE mechanism is the developed form of attribute-based access policy. Its main features are flexibility, scalability and detailed access control [12]. CP-ABE mechanism is fine grained, which mechanism very adaptable in complex system. Based on this idea, it was used in open source data distribution [13]. The flexibility of the CP-ABE mechanism in the cloud mechanism data sharing principle is prioritized. CP-ABE mechanism was used in the system [14]. The access tree is assigned to users with attributes. Through this access tree, a private key is defined. Cipher-texts are created based on attributes. The CP-ABE mechanism describes the concept of sensitive data. It analyzes the basic relationships between specific data objects [15]. It introduces sensitive data set. Indicates that the entire system is not affected when the data set changes [16]. It is a new encryption technology that addresses secure data sharing challenges [17]. It is a policy that seeks to prevent violations of both malicious users and authorities [18]. Studies have been conducted in various fields with CP-ABE mechanism [19], complex access control applications in data [20], storing and sharing of data in the cloud system [21] confidentiality of health data [22]. These fields are; development of access control system [19], the security of stored data [23], access control in large data applications by the Cloud

Security Alliance (CSA) [24], profile matching used in social networks [25] protection of personal health data and display by authorized persons [26] [27], the security of data sharing systems that depend on multiple authorities [28], encryption and protection of data in cloud computing [29] protection of data without a reliable center in the cloud storage system [30] and encrypted data access control and management of user privileges [31], ensuring data privacy in the cloud system [32], direct provision of data access control in the cloud system [33]. Data access control is considered a difficult issue because cloud storage is not a completely reliable system. The outsourced use of encrypted data in the cloud server is an important issue of today. In addition, the data may contain network access policies, main data, specific information about data owners or data receivers, and the disclosure of some sensitive access policies may result negative publicity or loss of market earning [34]. Users' concerns about data security prevent the widespread use of cloud computing. This is because sensitive data are stored in untrusted public clouds in an unsafe way [35]. Hence, it wants that all users view the data with sensitive access structure. The CP-ABE mechanism is a flexible and data-safe system for the cloud storage environment. These and other reasons highlights the use of the CP-ABE scheme in cloud computing [36]. In the system proposed by Wang et al., The CP-ABE mechanism is considered to be suitable only for providing data security in the cloud storage environment due to the functionality and flexibility of the CP-ABE as well as the correct functioning of the attributes and access policy [37]. In the system proposed by Zhou et al., the design of the completely unreliable cloud structure, with the CP-ABE mechanism, argues that the system can be protected against attacks by the user while providing both forward-looking and backward security [38]. In the fog information system, which is an extension of cloud computing, end-users are assured that the CP-ABE mechanism is a well-known encryption technology to ensure data confidentiality and fine-grained data access control while providing security for computing, storage and application services [39]. Another area where the CP-ABE mechanism is used is the Internet (IoT) systems, that all the things with internet today. The integration of intelligent object-based infrastructures increases the likelihood of the internet being found everywhere. The system that contains large data brings out security and confidentiality issues. In addition, the fine-grained access structure is an important question while maintaining data privacy [40]. The CP-ABE mechanism provides a convenient field of use for

secure storage and encryption of large data and fine-grained access [41]. Supported by fine-grained access control capability, the scheme significantly improves data access efficiency and greatly reduces the cost of key management [42]. The problem of key-authority misuse in CP-ABE mechanisms is a major problem. A mechanism should be added to improve these misuse problems. Such a system formalizes security requirements [43]. The CP-ABE mechanism has been found to be an efficient system in ideal conditions after obtaining the private key associated with user attributes. It is always possible for users to violate the privacy rules by misusing this proprietary information once they have obtained their credentials and authorization from the system administrator [44]. After detecting these malicious users, it is necessary to rebuild the system after the system has no cancellation mechanism. For this reason, a cancellation mechanism must be designed from the very beginning. It is necessary to consider how much this mechanism will reduce the cost when necessary [21]. Another contribution of this technique is that the encryption key size is smaller [45]. Currently changing user data and user rights with health workers should be checked dynamically [46]. In the real world, users' access rights are often dynamic. Therefore, mechanisms need to support the cancellation process [47]. An effective deduplication method should be added to the system in order to reduce the cost and increase the storage space, i.e. to prevent the same data being encrypted many times [48]. In order to eliminate repeated data and improve storage utilization, cloud storage is used for deduplication [49]. After user entry into the system, these controls must be carried out effectively.

KP-ABE is designed for multiple communications. Encrypted text is marked by attributes. The trusted authority give a user own private key. The KP-ABE mechanism is suitable for systems in which certain documents are read by whom [11].

2.2. Related Work

Considering the authentication and authorization mechanism, Uğur and Soğukpınar suggested a model called authorization model in multi-tier architecture [50]. This study is a step in designing of the desired system security. The operation mechanism of this suggested study is as follows; The authorization mechanism determines the attributes

of the users. Users must work depending on the specified attributes. This mechanism is a multilayer authorization model. Functionality and authorization are the basis of layer structure. The first layer of authorization mechanism controls user access to the system through Kerberos authentication. In this method, it is necessary to have an identity and a password. With this method, a short-term ticket is defined to the user. The user access to the system is realized through this ticket. The second layer was created to hold access control lists. In the third layer, access control is performed through roles. In the fourth layer, the situations where the roles are insufficient are checked. However, since this system is not based on encryption, data security is not considered.

Many different studies supporting multi-tier architectural security have been conducted. Multilayer security models are proposed to protect user privacy, reduce storage costs, provide access control, decrease the malicious persons harm to the system, and provide flexible authorization [51]. These security models have been used in studies such as biometric authentication [48], multi-authoritative system design [25], and outsourced data security [49].

Another system aimed at providing data security is proposed by Li et al. [2]. This system is a network authentication and authorization system for large data. This system requires that authenticated publishers share data securely with dynamic users. At the same time, it was tried to keep the data waiting in the cache securely. Threats here generally appear during data caching or when users are receiving data. Attackers try to carry out attack by impersonating system users. Some important points have been identified for system security. These; the unity of the large data should not be changed, secure logging into the system, secure data retrieval from the system, efficient and convenient authorization, and finally the data backed up on the network should be available everywhere. This system met all of the requirements that have been set [52]. The design of the system is as follows; Public key encryption has been used to perform identity based encryption. Instead of CP-ABE and role-based access control, data encryption is performed by specifying policies on attributes. Data access can be restricted by the characteristics of the users and is also flexible. In the system, centralized, reliable users are defined to identify features and users, and to make key

distribution. Authentication with the identity-based encryption mechanism has been made to the users. At the same time, an identity based digital signature mechanism has been defined to these users. This signing mechanism shows the changes that users have made, so the denial problem is considered. The key chain mechanism is coded and stored by the CP-ABE system in order to identify and store the features in the system.



CHAPTER 3

MULTI-LAYER AUTHORIZATION MODEL SCENARIO AND REQUIREMENTS

3.1. System Requirements

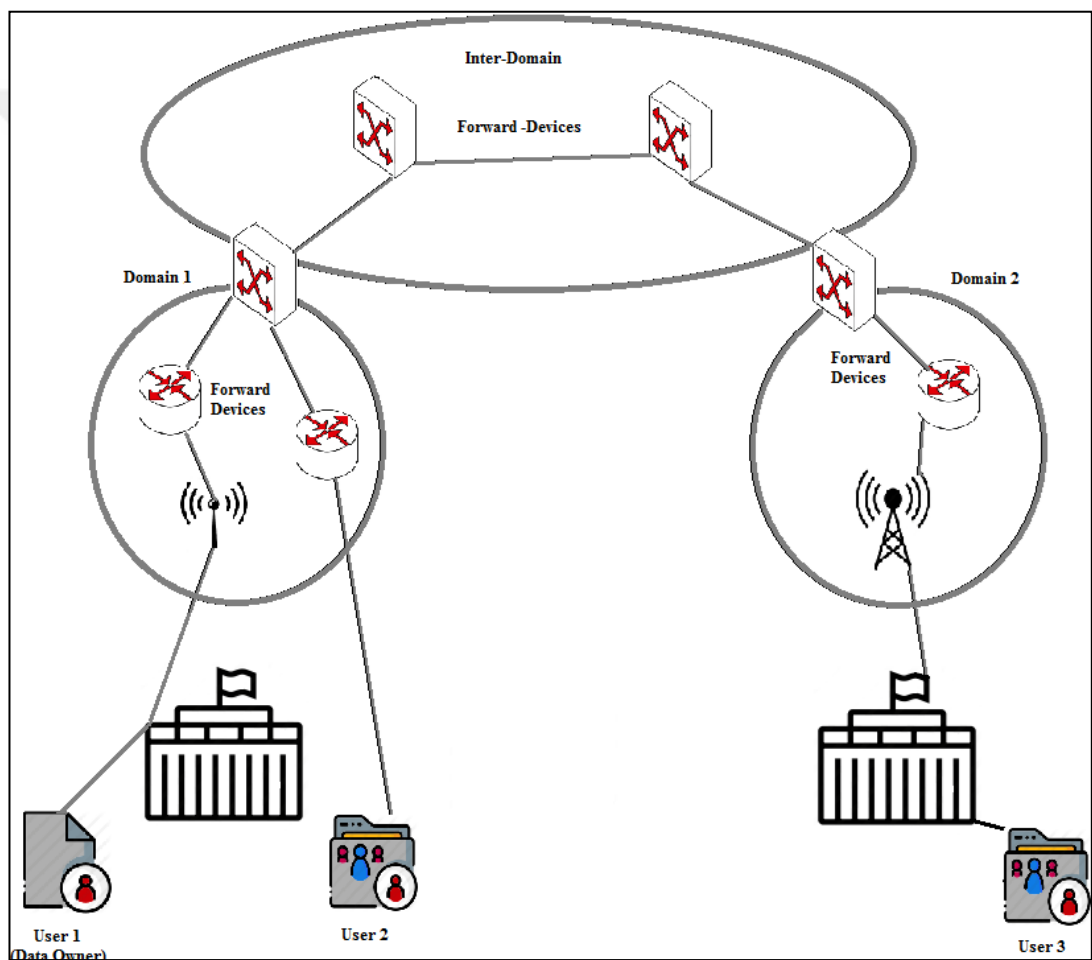


Figure 1: Data Sharing Scenario

In Figure 1, it is obvious that sensitive data need to be securely shared by people who have been authenticated by various restrictions. At the same time, shared data must be secure on the network or cached. Problems in this scenario usually occur when the user receives data or sends data. In other words, this could be defined as phishing attacks.

Identity impersonation attacks can be defined as the substitution of the malicious users to the system users or requests to gain access as an authorized user of unauthorized users in the system.

- Ensuring that users register securely into the system
- Allowing the users to publish in accordance with the system policy of the data and providing to allow data access with flexible authorization.
- Ensuring the restrictions data or authority retrieval.
- Encrypting data according to user characteristics to ensure secure transmission
- Checking that the copy of the data is not in the system
- Ensuring that the data is not altered without authorization
- Undeniability

3.2. Multilayer Authorization Mechanism System Design

The proposed multilayered authorization mechanism is determined by its stages, functions and authorization sensitivity. User authorization filter is performed on each layer.

Two different layer structures are considered for authorization;

1. Authorization Module : The initial module of the system. System users and system attributes are determined. Attribute definition is done for users. The identity-based key ($PriK_{ID\#}$) and the attribute-based key ($SecK_{ID\#}$) are specified for the users
2. File Sharing Module: Encryption operations are performed during file sharing. Data tag, data and user revocation mechanism are designed.

In order to meet the scenario requirements shown in Figure 1, a multi-layer authorization mechanism system is considered. In order to meet these system requirements, a system is used in which a Cipher-text policy-based attribute-based encryption (CP-ABE) mechanism, an identity based encryption mechanism (IBE), and an identity based signature mechanism (IBS) are used together. At the first stage of this system, the user performs access control to the system. To perform these controls, an identity based encryption mechanism (IBE) and an identity based signature

mechanism (IBS) are used. In the other layer, flexible authorization and encryption of the data depending on this authorization are provided in the system. These operations are performed by the CP-ABE mechanism.

3.3. System Users

Network Administrator: It is one of the authorized users in the system. The Network Administrator manages the assets on the network, registers the users into the system, and performs the access control to the system. It determines the private identifiers for the user to be used in the system revocation mechanism. It declares the private identifiers in a public environment with its own signature when the user authority changes or when the user is removed from the system. It keeps this list up to date. The Network Administrator transmits user data and defined identifiers through a trusted channel for user identification to the data administrator.

Data Administrator: One of the authorities in the system is the data Administrator. It defines the attributes to be used in the system and the attributes of the users. It specifies the user authorizations with these attributes. It provides qualification and key generation for flexible authorization.

Users: All people that reaches the data. (Data owner and data user)

Data Owner: It is the person who shares the data. It performs data encryption by specifying attributes.

Data User: Only displays encrypted data if its attributes are compatible with the data it wants to encrypt.

3.4. Authorization Module

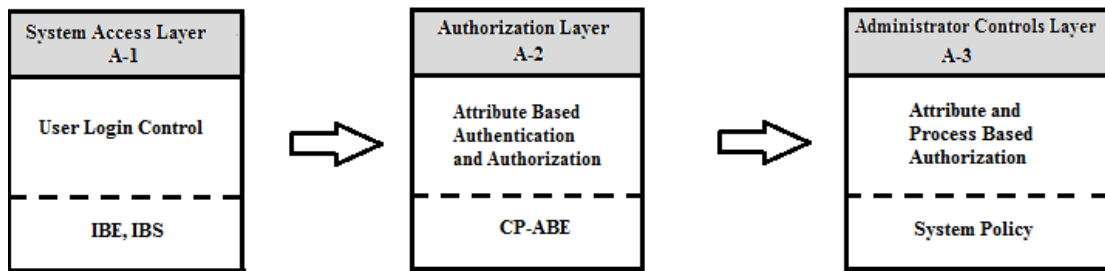


Figure 2: Multilayer Authorization Model

Here is a brief summary of the steps of this architect;

A-1) Access to the System (Startup) Phase: The network administrator and data administrator are specified. The master key is defined for the network administrator and the data administrator. A user-specific identifier is specified with the key. The network administrator performs the necessary key definitions for each user registered to the system. It identifies each user's private identifier. Users are registered securely on the system with routing devices. The data administrator specifies the system's attributes. It performs attribute definition for users who are registered to the system.

A-2) Authorization Layer: All users registered in the system can perform data sharing process. The user has full authority over the file he owns. After logging into the system, it encrypts the data and transmits the data over the network to the user.

Secure Data Retrieval: The user sends the relevant data to the system for verification. After verification, the data is displayed if the necessary attributes are provided to access the encrypted data.

A-3) Administrator Controls Layer: It is required for network administrator which is authorized in the system and data manager control. If the system's trusted authorities change, it is a security step for those users. If the user is removed from the system with special identifiers then authorization should be denied. However, the data that were previously viewed are not taken into account. Processes continue according to the determined system policies.

In this system, a network administrator and a data manager are planned because a data sharing mechanism is considered for an outsource provider of an enterprise network. However, a hierarchical network and data administrator structure can be considered for larger enterprise networks running from multiple centers.

In this study, multi-tier architecture system and data security on the network are analyzed. Data security is taken into account through network communication of an institution system with different locations. The data are posted by users on the system. As shown in Figure 3, the user or data user who wants to share data must be registered to the system. Registration to the system is performed by the Network Administrator. The data administrator defines the attributes for users on the system. In the cloud system, the data owner is stored the data. The Data User accesses the encrypted data over the cloud system. User data or files are stored securely in the cloud system.

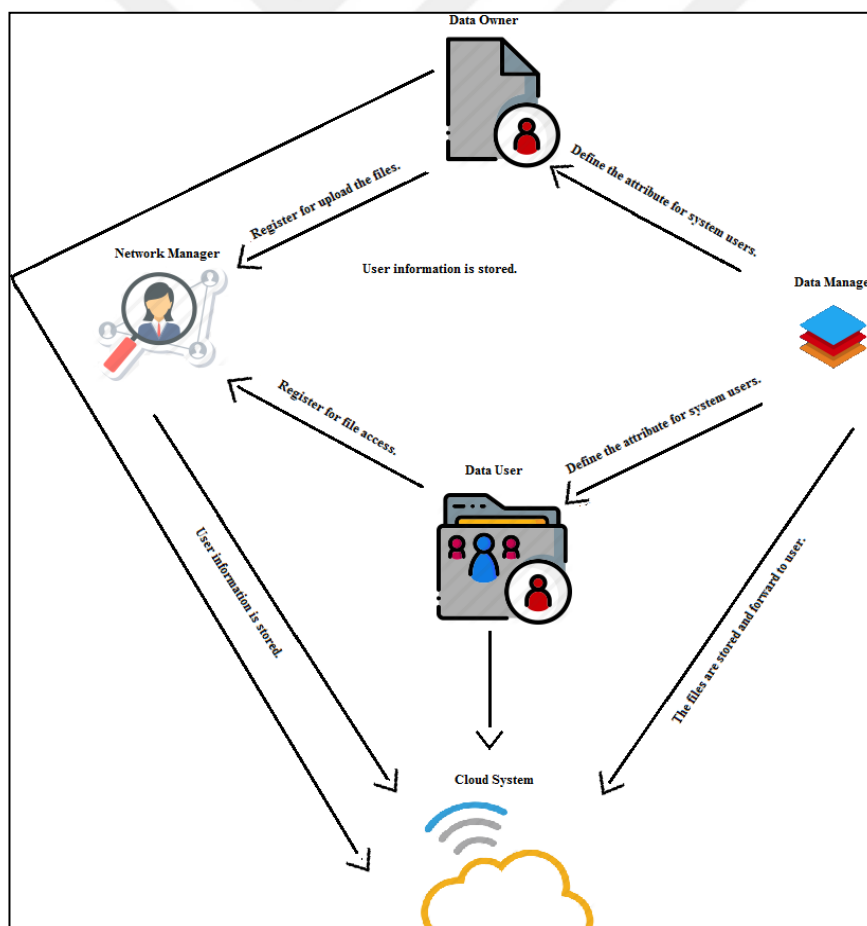


Figure 3: Multilayer Authorization

3.4.1. Access to the System

It is the first (A-1) tier of the multi-tier authorization model. In this layer, Network Administrator and Data Administrator are initiated. The Network Administrator authenticates and verifies users. Data Administrator specifies the system attributes.

The network administrator controls the login process for system users. It registers the newly logged users to the system. The TLS mechanism with IBE is used for authentication. It is necessary to modify and implement the TLS mechanism, in this section we recommend using the algorithm as in [58]. The system creates an Id-Based Key for the users, $PriK_{ID\#}$. It also specifies private identifiers ($RS_{ID\#}$) for users. This private identifier checks the lists and keeps them up to date.

The data manager identifies the attributes to be used on the system, and defines these attributes for system users. It creates an Attribute-Based Key, $SecK_{ID\#}$.

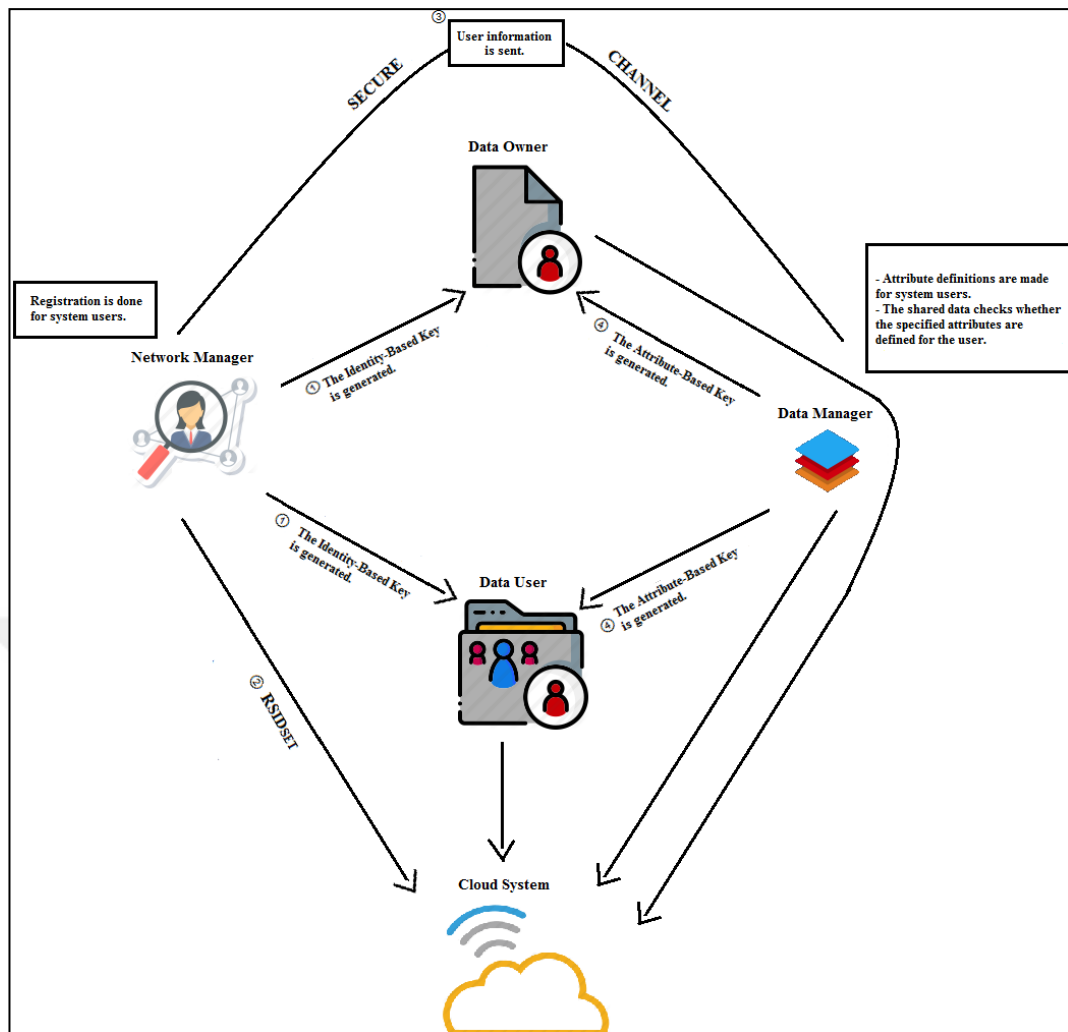


Figure 4: Start-up phase

3.4.1.1. Network Administrator Controls

The Network Administrator first generates a Master-Key (MSK_{AY}). Then, generates the corresponding Public-Key ($PubK_{AY}$) for itself. The network administrator manages and authenticates the identities of other users in the system. It performs ID-based key generation for users. It uses the Identity-Based Authentication (IBE) mechanism. The network administrator specifies private identifiers for the users, and this private identifier ($RSID\#$) is used to check whether the user is authorized in the system. The network manager makes changes to this special identifier set, depending on the user revocation. It stores this special identifier set securely in the document management system by signing with the $MSK_{\#}$, Network Administrator's, MSK_{AY} . It keeps this list constantly updated with its own digital signature.

Network Administrator Setup Algorithm;

- **Setup**(MSK_{AY}): The network administrator master key (MSK_{AY}) and the corresponding public key ($PubK_{AY}$) are generated. A unique identifier ($RS_{ID\#}$) is defined for all users.
- **Key Generation**($MSK_{AY}, ID\#$): The network manager generates the secret key ($PriK_{ID\#}$) for assets on the network using the master key and user identifier
 $PriK_{ID\#} = IBE_{KeyGen}(MSK_{AY}, ID\#)$.
- **Processes**: The user secret key ($PriK_{ID\#}$) is sent over trusted channels. The user's identity-based digital signature is created.

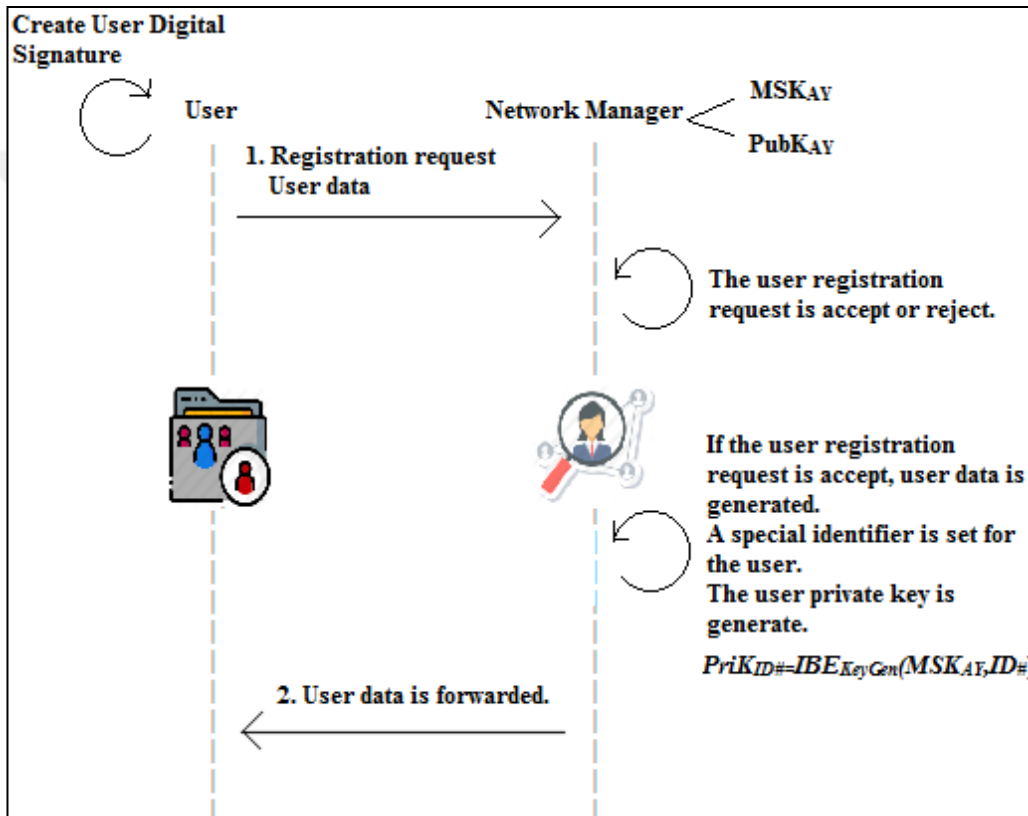


Figure 5: User Registration

In this system, the network administrator is considered as completely reliable. In Figure 5, the network administrator stores MSK_{AY} , announces $PubK_{AY}$. For system assets, the administrator generates the private key with MSK_{AY} and the user identifier.

Table 1: Identity-Based Key Created by Network Administrator for Users

Name/Surname	ID	RS _{ID}	Identity-Based Key
User1	1	RS _{ID1}	PriK _{ID1}
User2	2	RS _{ID2}	PriK _{ID2}
User3	3	RS _{ID3}	PriK _{ID3}
User4	4	RS _{ID4}	PriK _{ID4}

The users created in the system are defined as shown in Table 1, the values written under the $RS_{ID\#}$ column are randomly defined identifiers. The user's unique identifier defined as a RS_{ID} [45]. RS_{ID} is used to monitor the user cancellation in the system. Revoked users are stored in $RS_{ID_{SET}}$ sets. $RS_{ID_{SET}}$ is used to control the authorization changes of system users. Each user private identifier ($RS_{ID\#}$) is signed by the network administrator with a digital signature and is published in an untrusted environment. As it will be described later, the user attribute key is created with these special identifiers. When the user's authority on the system changes, the network administrator adds the user-specific identifier to the $RS_{ID_{SET}}$ set. The $RS_{ID_{SET}}$ set is signed with the Network Manager Master key (MSK_{AY}) and kept in the document management system. The data owners also uses this set when they are associating access policy with encrypted text. Thus unauthorized access control is ensured.

3.4.2. Authorization Layer – Data Administrator

The data manager identifies and manages the system attributes (A-2). It defines the attributes defined in the system on the users. When system attribute values are defined, keeps the following values;

Table 2: User Attribute Definition

	Attribute ₁	Attribute ₂	Attribute ₃	Attribute-Based Key
ID ₁	✓			SecK _{ID1}
ID ₂		✓		SecK _{ID2}
ID ₃	✓		✓	SecK _{ID3}
ID ₄		✓		SecK _{ID4}

As shown in Table 2, the user attributes are defined according to their ID definitions. Depending on the attributes, a secret key is generated for the users. This attribute-based secret key ($SecK_{ID\#}$) is used for data encryption.

The stages of the secret key formation are as follows;

- **Setup** (): Data Manager runs the setup algorithm. MSK_{VY} and $PubK_{VY}$ are produced for the data manager. The System Users' Attributes (*user att.*) are determined. The size of the access structure and its maximum size (n_{max}) are determined.

- **Key Generation** (MSK_{VY} , $user\ att.$, $RSID\ \#$): For each user, the secret key $SecK_{ID\#}$ is generated using MSK_{VY} , $user\ att.$, and $RSID$
 $SecK_{ID\#} = CP\text{-}ABE_{KeyGen}(MSK, user\ att., RSID\#)$
- **Process:** The secret key defined for the user is delivered to the user through the secure channels.

3.4.3. Administrator Controls

Attribute and Process Based Authorization (A-3) is the phase in which network and data admin controls are performed.

In this designed mechanism, detailed controls on the users and the operations they perform are provided. Regulations on organizational roles are carried out in the system but no checks on sensitive reliable centers are made. For this reason some changes may be needed on these roles. Decision mechanisms for these people are the constraints defined in the regulations. When there is a user change, it is revoked with unique identifiers again in the revocation of the system users. This layer defined in the system is provided to support authorization checks. The decision mechanisms is consider regulations when determining constraints. This layer emphasizes that the system is controlled by reliable people. It is a section used for verifying the authentication. It is considered as a necessary layer for dynamically changing systems.

3.5. File Sharing Module

At this stage, users perform encryption for secure file sharing.

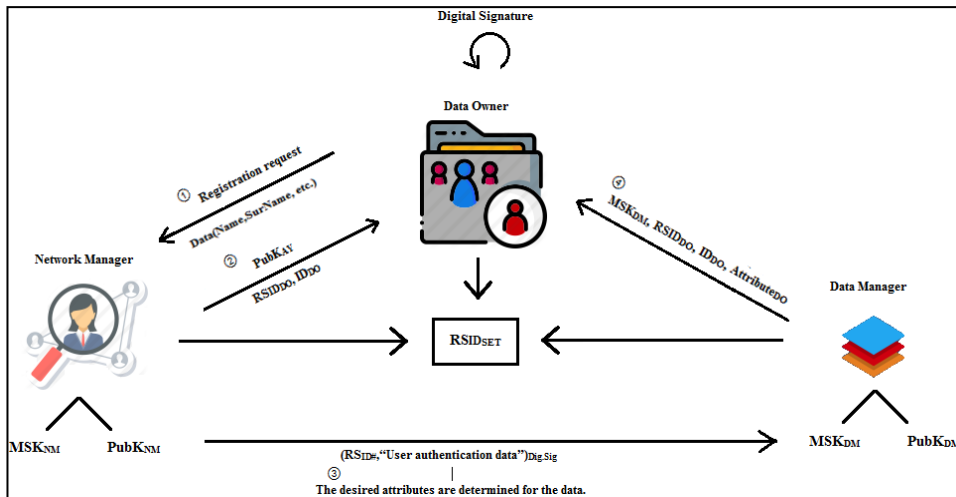


Figure 6: Data Sharing Request

As shown in Figure 6, the user must first register to the network administrator for data sharing. The user forms login credentials to the system. A key ($PriK_{ID\#}$) linked to the ID is provided and it is transmitted to the user through a secure channel. For a user in the system, the identity details are verified. After the identity details are created for a user who is logged into the system for the first time, the attributes are determined by the data manager.

A key ($SecK_{ID\#}$) related to the attributes is also created for the user. According to these attributes, the authority of the user in the system is checked. Once the data owner received the key related to the identity and the key related to the attribute, it performs data encryption and data sharing.

3.5.1. Data Owner File Sharing

Data owner is any user who shares the sensitive data in the system. It has full authority over the data it has. Other users in the system can only read data and cannot make any changes. Data encryption is performed by the data owner.

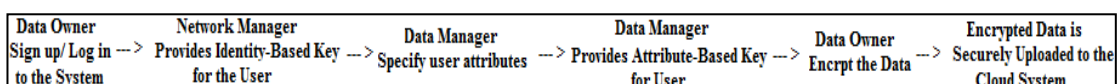


Figure 7: File Sharing Steps

The steps of user data sharing phase are shown in Figure 7. Once the user logs into the system and provides the required verification, and after the attributes are specified, data sharing and encryption can be performed. User data encryption is performed as follows. The data encryption process is described below.

Data Encryption

Before encryption data owner login to system using his/her own ID-Based key. Then, data owner prepares the tag of a data to control whether the data is encrypted before. The calculation of the data tag value is as follows;

The calculation of tag value is consists of three stages.

- The data encryption key is created.

$$Key = H(data)$$

(H is the hash function.)

- Cipher-text is generated using the symmetric encryption mechanism.

$$Text (T) = AES (data, Key)$$

- Data Tag Value;

$$Tag = H(T)$$

The data tag value is generated by the convergent encryption method [48]. The hash value of the data is used as an encryption key. Data is encrypted with the encryption key specified by the AES algorithm. The hash value of this encrypted data is the data tag. Therefore, check for duplication when load the data into the system. If the data copy is present in the system which is not need to be encrypt. It is described in the deduplication article in detail [48].

After, preparing the tag of the data, data owner starts encryption of the data as following. Since symmetric key encryption is faster, it is used to speed up the key encryption. Data encryption starts with a random session key (s), s is a random number.

The data is encrypted with the AES algorithm using s . The data policy associated with the data is generated by data owner. Then, session key is encrypted by ciphertext policy attribute based encryption using attribute based secret key of data owner with data policy and actual $RSID_{SET}$.

$$C_T = AES(data, s)$$

$$SessionKey = CP-ABE(s, accesspolicy., RSID_{SET}, T, N, SecK_{ID\#})$$

$$\{C_T, SessionKey, user\ att.\} // Tag$$

The data is encrypted depending on the key chain mechanism. A random encryption key s is created. The data is encrypted with the key s by the AES algorithm. A policy should be determined for this data. Then, The $RSID$ set must be check which is prepared by the network admin. This session key is encrypted according to the attribute-based encryption method using the $SecK_{ID\#}$ of the owner of data. Time (T) and random number (N) in data encryption are used to prevent replay attacks.

Revocation sets ($RSID_{SET}$) are stored in the document management system signed by the network administrator in the system. This revocation set can be accessed by everyone, but cannot be changed. The revocation set is generated with time stamp.

The user who shares the data in the system is the owner of the data. The data is updated by the data owners. When the data owner is removed from the system or when there is authority change, he / she has no authority on the data. The data is exported by the data admin.

Data Decryption

Data user also logins to system using IBE keys then if the attributes of data user is defined in the ciphertext policy then he/she decrypts the data(C_T) using, $SessionKey$.

If the user identifier $RS_{ID\#}$ is not in $RSID_{SET}$, in other words if he/she is not in the revocation list, or his attributes are not compatible with data policy, his $SecK_{ID\#}$ will not decrypt the session key.

3.6. A Sample Scenario

In this section, we will examine the system. Let's consider the situation where we have a secret document. This document can be accessed by the Instructor, Chief and staff with A-X, A-Y, A-Z attributes. We redesign the access policy as follows:

$$((Chief \wedge Instructor) \wedge (1-Attribute \{A-X, A-Y, A-Z\}))$$

The access structure representation may can also tree:

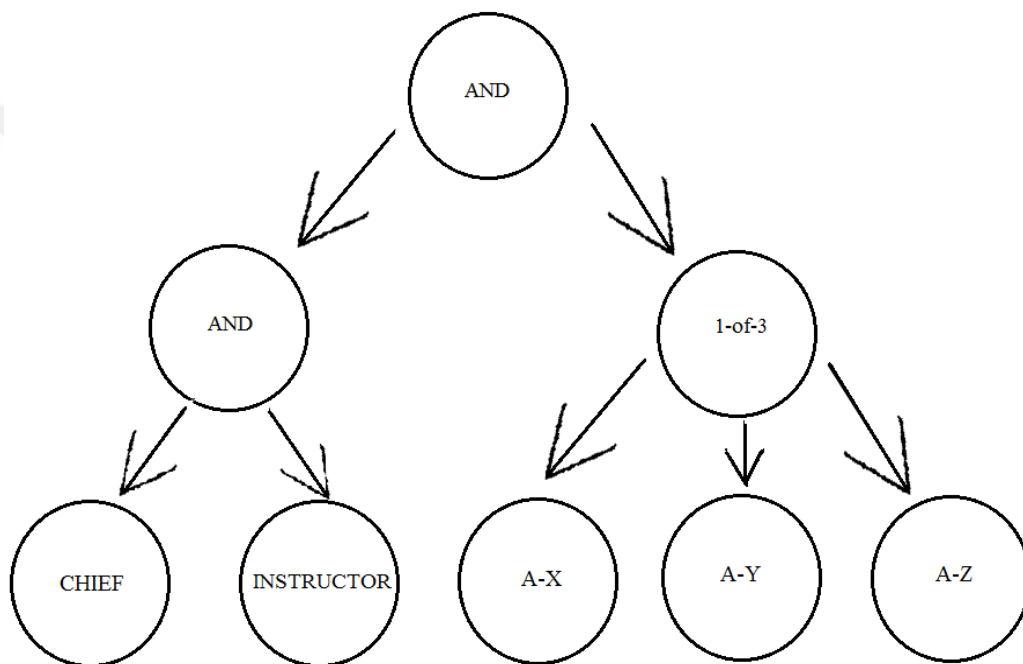


Figure 8: Access Tree Structure

In this part, for four types of user each with different attributes, we will examine the access rights according to user attributes with an example access structure.

Table 3: Access Authority Demonstration

	User 1	User 2	User 3	User 4
Instructor	✓	✓		✓
Chief	✓	✓	✓	
A-X			✓	
A-Y		✓		✓
A-ZZ	✓			

Table 3 shows the users attributes. This table shows that two users provide the required attribute policy and the other two do not have the required attributes. Encryption mechanism for the user is shown in the following part.

Setup

Network Admin generates

- The master key (MSK_{NA}), public key ($PubK_{NA}$)
- ID and RSID for each user.
- The secret key ($PriK_{\#}$) (using IBS method with MSK_{NM} and $ID_{User\#}$)

$PriK_{\#} = KeyGen(MSK_{NA}, ID_{User\#})$, is delivered to the users via secure channels.

Creates a revocation set ($RSID_{SET}$). $RSID_{SET}$ is stored in the document management system in such a way as to provide user access by signing it with the master key. It will be updated if necessary.

Data Admin generates

- The master key (MSK_{DA}), the public key ($PubK_{DM}$)
- The attribute table based on the user IDs.
- The attribute based key for each user

$SecKey_{User\#} = KeyGen(MSK_{DA}, user\ att.\ User\#, RSID_{User\#})$, is delivered to the user via reliable channels.

Encrypting a Message

The data owner checks the revocation set before performing the encryption process. The data is encrypted accordingly to the access policy. And also, the data owner should check the tag whether the data has been uploaded to the system.

Data owner generates a random key (s). It uses s to encrypt the data that it has produced.

$$C_T = AES(s, data)$$

Attribute-based encryption is performed by the user through this key.

$$Enc(CPABE(s, access\ policy, RSID_{SET}, T, N, SecK_{ID\#}))$$

$$\{C_T, SessionKey, user\ att.\} || Tag$$



Decrypting the Ciphertext

If the data user whom will decrypt this encrypted text is in the RSID set and his/her attributes satisfies access policy, U. He may decrypt and check integrity of the ciphertext.

$$(AES(s, data), CP-ABE(s, RSID_{SET}, T, N)) || Tag$$

In the specified scenario, $((Chief \wedge Instructor) \wedge (1-Attribute \{D-X, D-Y, D-Z\}))$, users who is provide the rule perform the decryption process. Table 3 is show the user access authority. According to this table only user1 and user2 can perform the decryption process.

CHAPTER 4

SYSTEM CHARACTERISTICS

4.1. Revocation Mechanism

Only few algorithms addressed both user and attribute revocation. In attribute revocation, the schemes only addressed the problem of updating new attributes, but did not address the addition and deletion of attributes.

Authentication mechanisms aim to protect data confidence against unauthorized users. However in such a system revocation is another challenging task. In most of the systems, attribute revocation is considered. However both user and attribute revocation should be considered. Moreover, most of the schemes only address the problem of updating new attributes, but did not address the addition and deletion of attributes. Here, we analyze the possible situations, taking into account the revocation of a data reader or its access privileges.

1. Revocation of the user through the system
2. Revocation of all features of the user on the system
3. Revocation of user attribute (crud-create, read, update, delete operations)

In the conventional CP-ABE mechanism, the discretionary user revocation cannot be made. For this, the revocation mechanism suggested by Li et al. [41] is adapted to the designed system. A multi-layer authorization model developed in system security is proposed. In this proposed mechanism, authorization control is made together with unique identifiers. The user revocation sets are contained in the encrypted text, and the user secret keys are created with these unique identifiers. Thus, when the user authority is revoked, it will be defined in the encrypted text. The revocation set must be updated when the user authorization on the system is revoked. The encrypted text to be formed is created according to the new cancellation set.

The cancellation mechanism is added to the system from the beginning. The network manager adds private identifiers for all users who register to the system. The network administrator adds the private identifier of each user who has been revoked in the system to the private identifier set. The network administrator keeps this set constantly updated. User revocations are also realized with these identifiers. User private identifiers are sent to the data admin. User attribute based keys are created with these private identifiers. The user also encrypts the encrypted text with a private identifiers set. Thus, it can be checked whether the user private key opens the encrypted text.

The cancellation mechanism in our system works as follows. System users and special identifiers of users are stored by the network administrator. A sample user definitions is shown in the Table 6.

Table 4: User List

ID	Name	Surname	RS _{ID}
1	User1	U1	RS ₁
2	User2	U2	RS ₂
3	User3	U3	RS ₃
4	User4	U4	RS ₄
5	User5	U5	RS ₅

When the user is removed from the system, the network administrator creates a revocation (RS_{ID}) set or the existing revocation set is updated. This revocation set is stored by the Network Administrator in an signed form for the access of users in the document management system.

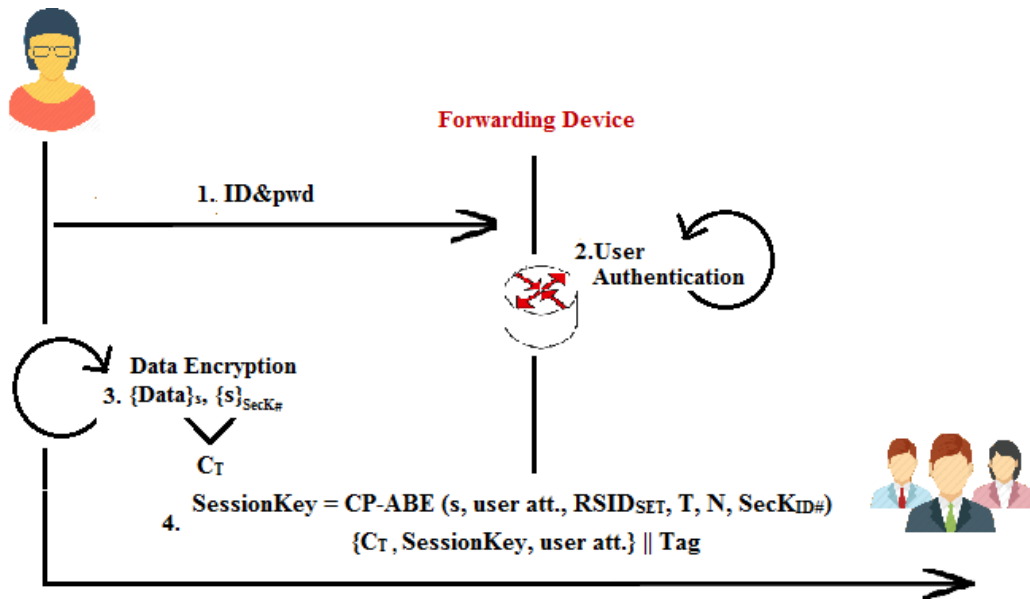


Figure 9: Data Sharing

The user performs data encryption according to the attributes it specified.

$$C_T = AES(s, data)$$

$$\{ CP-ABE(s, AccessPolicyID_4, RSID_{SET}, N_1, Z_1) || Tag(data) \}$$

According to this encryption, only those who have the Attribute3 attribute and do not have an identifier in the RSID set can display the data. Attribute 3 can be displayed by all users according to Table 5. However, User 1 in the user revocation table in Table 4 has been removed from the system. And the user can not view the data because it cannot provide all the features to decrypt the data.

4.2. Deduplication

Data deduplication is a technology that is used to significantly increase storage efficiency. Data deduplication is used to remove the same data in the storage. It is a technique used to reduce the amount of storage space required to record data. Most organizations include copies of many data pieces in storage. For example, the same file can be saved in different places by different users, or non-identical files can be in similar contents. On singulation, a copy of the record is saved and the others are removed. The same data is directed to this file.

Data deduplication has many benefits; first of all it reduces the costs by reducing disk space that organizations must purchase. Removing extra copies of data does not only reduce the cost of disk hardware, but also reduces the costs such as electricity, cooling and maintenance. Data deduplication prevents data increase and increases storage and backup efficiency. Data recovery can also be accelerated.

In traditional encryption, the data under the different key makes the deduplication process impossible. In addition, random encryption results in different encrypted data even when the same data is encrypted with the same key. We can summarize the deduplication used in the system as follows;

The deduplication is performed with the Dekey system in the mechanism used. In the mechanism, the hash value of the data is generated and the data encryption is done by this generated value. Data is not explicitly present in the system. The hash value is checked with the deduplication process. In hashing, small modifications in data will result with different hash and this may cause many extra copies with small modifications, in this case partitions of the text may be hashed.

CHAPTER 5

SECURITY ANALYSIS

The methods used in the system measure the accuracy of the authorization. User identity information is checked in the first layer. In the upper layers, the authorization information is updated via the attributes. The authorization control on the first layer is for access to the system. There are constraints on data management in the other layer.

CP-ABE, which is an authentication mechanism based on identity, identity-based signature and flexible authorization mechanism, is used for authentication and data security. In order to verify the data sent over the network, an identity based signature mechanism is used. A reliable registration and network manager manifest has been used to use this signature effectively. It has been determined at what time interval the data in the system is used for reliable recording. A random number must also be added to this data. Since this number is not always the same, replay is considered as a preventive system for attacks. At the same time, the network performs the authentication of the network administrator. In addition, the hash is used in the system also controls data integrity.

The CP-ABE mechanism works to provide an attribute for flexible authorization. To calculate the available attributes, the information is found and an Id-based signature is added for verification. The CP-ABE mechanism access control is ensured based on the attributes and key chain mechanism determined. This adds the signature of the user who made the encryption. The Id-based signature algorithm is used to provide authenticity. The data hash value is used for the deduplication process.

The proposed multi-layer security mechanism meets the following requirements:

- The Identity-based Authentication mechanism (IBE) and the Attribute-based encryption mechanism (CP-ABE) are used together. Thus, a multi-layer security mechanism is proposed.
- The slow working state of the CP-ABE mechanism is inhibited by the AES algorithm.
- The revocation mechanism is proposed in the system. Set of attributes and a unique identifier are assigned each user in the system. The user can be revoked efficiently using this identifier. In addition, this technique has two important contributions.
 - The designed key size is small.
 - Encryption/decryption with the revoked user cannot be affected.

Revocation information is embedded in encrypted text for more flexible access control [45].

- The deduplication mechanism is proposed in the system. Data tag values are used for singularization. The tag value is used to identify unnecessary copies. If the data copy is in the system which is not again performed the encryption. This situation is reduces the cost of storage. In addition, time loss is prevented.

The deduplication on the encrypted data is solves the conflict problem [48].

CHAPTER 6

EXPERIMENTAL RESULTS

In this section, the results are presented for the evaluation of the performances of RBAC and ABAC algorithms. The RBAC algorithm always assigns roles to the users and performs the encryption over them. The ABAC algorithm defines attributes for the users and performs the encryption over them. We have defined the users and their roles in the RBAC algorithm for the operation of these algorithms. We have examined the encryption speeds on text files with different sizes. We have determined the users and their attributes for the ABAC algorithm and compared the encryption speeds for the same files. The algorithms run times were tested with 4 GB RAM, Intel Core i7, 2.40 GHz.

When performing tests, the classic CP-ABE algorithm implemented in [53] and classic RBAC algorithm implemented in [54] are modified to compare these concepts.

Evaluation of the RBAC algorithm: It is a simple and easy to use model. Roles are assigned statically by the system administrator for the user. The operations that the user can do without changing the role remain unchanged. With role definition, the system works fast. The actions that people can take are determined. It causes too many role definitions for large systems. Role rush occurs. In some cases more roles are produced than the users. When people's tasks change, the roles need to be set from the beginning. On the other hand, it cannot be used efficiently in dynamically changing systems. It cannot provide flexibility for changing environments.

Table 5: RBAC Encryption Result

Text File	Roles	Encryption Time	Decryption Time
2 ⁴ Bayt	3	10ms	3ms
2 ⁴ Bayt	4	11ms	3,71ms
2 ⁴ Bayt	5	13,24ms	5,13ms
2 ¹⁰ Bayt	3	640ms	192ms
2 ¹⁰ Bayt	4	701,4ms	234,42ms
2 ¹⁰ Bayt	5	847,36ms	328,01ms

The test results are given in Table 5 with the RBAC algorithm. Multiple roles are define for a user. For these defined roles, file encryption and decryption rates/times are evaluate in the system. Depending on the number of user roles, the rate/time of encryption and decryption are increase. The text file size increases the encryption and decryption time.

Evaluation of the ABAC algorithm: The ABAC mechanism solves the role assignment problems experienced with the RBAC mechanism. It evaluates the users with their attributes, not with their roles. It is a dynamic and flexible model. However, it also brings the complexity with it. The users' attributes should be known in inter-institutional communication. The operations should be made accordingly. ABAC is flexible and applicable in the systems with too many users systems and in the systems where the roles of users are not specified.

Table 6: CP-ABE Encryption Result

System Att.	User Att.	2 Attributes			4 Attributes			8 Attributes			16 Attributes			32 Attributes		
	File Size	Enc	KeyGen	Dec	Enc	KeyGen	Dec	Enc	KeyGen	Dec	Enc	KeyGen	Dec	Enc	KeyGen	Dec
4 Attributes	2 ⁴	1312	203	165	1504	325	175	-	-	-	-	-	-	-	-	-
	2 ¹⁰	1401	222	185	1665	333	196	-	-	-	-	-	-	-	-	-
	2 ¹⁰⁰	2523	236	1206	2576	392	1274	-	-	-	-	-	-	-	-	-
8 Attributes	2 ⁴	1498	235	167	1500	334	195	1525	402	209	-	-	-	-	-	-
	2 ¹⁰	1752	247	191	1797	342	246	1880	391	311	-	-	-	-	-	-
	2 ¹⁰⁰	2726	270	1264	2778	398	1274	2824	492	1282	-	-	-	-	-	-
32 Attributes	2 ⁴	2664	288	193	2808	386	199	2830	466	215	2903	848	250	3664	1566	325
	2 ¹⁰	2803	297	195	2845	391	248	2897	487	258	2927	877	263	3948	1580	331
	2 ¹⁰⁰	3015	401	1004	3986	411	1991	4023	496	1286	4923	932	1333	5019	1586	1883

The values in Table 6 are given milliseconds. System policy and user attributes are manually specified in the code. Time changes are according to the increase of system attributes, user attributes and file size.

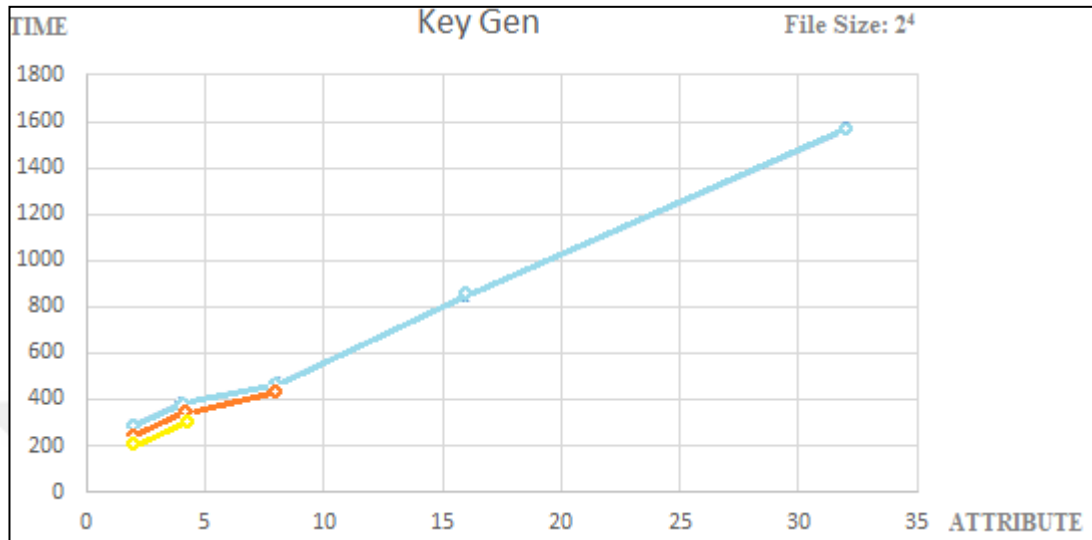


Figure 10: Key Generation

When Table 6 and Figure 10 is examined, the key generation times increase linearly when the number of user attributes increases. The user secret key is created with attributes. Therefore, as the number of attributes increases, user secret key generation times increase ($keygen(attr, PKFileName, SKFileName)$). Also, the key generation times vary when the number of user attributes is kept constant. This is because user secret keys are written to a file. Then, the keys are read through this file. The size of the file is increasing in each new key formation. Accordingly, the key generation time increases.

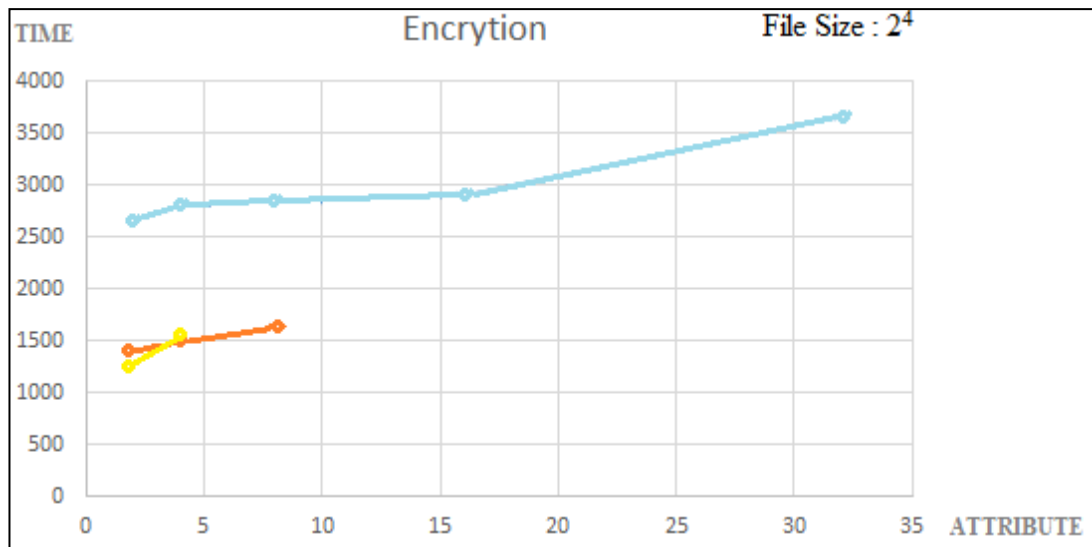


Figure 11: Encryption

(Enc (encFileName, policy, cipherTextFileName, PKFileName))

Table 6 and Figure 11 is examined, the data encryption time is varies according to the number of policy. As the number of attributes is increases which is the encryption time increases. At the same time, the secret key file size is effect the encryption time. Encryption time is increases when the ciphertext file size increases.

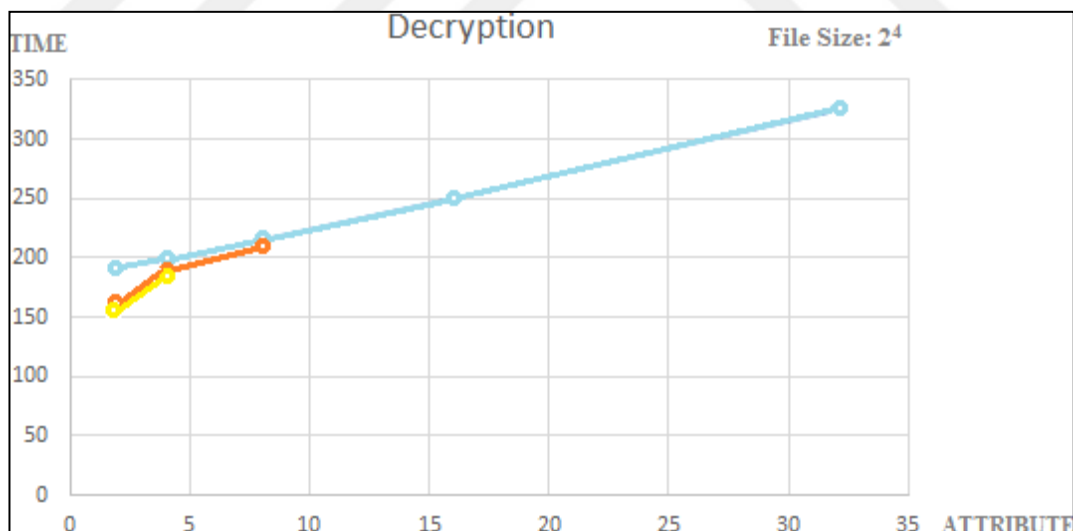


Figure 12: Decryption

(Dec (cipherTextFileName, PKFileName, SKFileName))

Table 6 and Figure 12 is examined, increases the decryption time when the user attributes is increase. Because, the user secret key is composed of attributes. At the

same time, the secret key file size is effect the encryption time. Decryption time is increases when the ciphertext file size increases.

Table 7: CP-ABE Encryption Comparison Results

8 Att. Number of Attributes Defined the System	System Users	User1			User2			User3		
	User Attributes Number	2 Attribute			3 Attribute			5 Attribute		
	Transactions	Enc.	Key Gen.	Dec	Enc.	Key Gen	Dec.	Enc.	Key Gen	Dec.
File Size	2^{10}	1748	243	196	1763	320	222	1792	353	348
	2^{100}	3121	400	1066	3174	404	1302	4038	486	1966

The values in the Table 7 are in milliseconds. Eight system attributes are defined. Three different users are defined in the system. Different number of attributes have been determined for each user. The change in the system was examined depending on the number of these attributes.

The changes observed in Table 6 are also observed in Table 7 Depending on the number of user attributes and file size, encryption and decryption times are increasing.

Comparison of Algorithms

Table 8: Comparison of Algorithm

File Size 2^{10}			Enc. Time	Dec. Time
			ABAC	2 Attr.
	RBAC	2 Role	427	128

Algorithms are compared in Table 8. The RBAC Algorithm encryption and decryption times are faster than the ABAC algorithm. The reason why the RBAC algorithm works faster is to determine the roles directly. This is confirm in the "Comparative analysis of Role Base and Attribute Base Access Control Model in Semantic Web" article comparing the ABAC and RBAC algorithm [55].

The RBAC mechanism runs faster than the ABAC mechanism. However, ABAC provides more effective results in complex access control mechanisms. RBAC makes pre-work for user roles in the installation. The action that each user will take is clear.

But the ABAC mechanism prioritizes the flexibility and dynamism. The access control matrix needs to evaluate the policy determined in each cell. Considering that the policy assesses attributes located in multiple and different locations; the performance of this approach becomes lower.

Comparison the ABAC and RBAC algorithm;

The ABAC algorithm is flexible than RBAC algorithm.

The ABAC algorithm is flexible, dynamic and changeable.

However, the ABAC algorithm is more complex than the RBAC algorithm.

The ABAC algorithm uses attributes for the encryption.

However, the attributes must be standard. Attributes must be valid between organizations.

The revocation mechanism can be applied to the ABAC algorithm. However, the RBAC algorithm is not enabled for revocation cases. Roles need to be rearranged.

The RBAC algorithms uses roles for the encryption. The roles are static. Therefore, systems installed with RBAC are not dynamic.

The RBAC algorithm is controllable and manageable.

With the RBAC algorithm, many roles may be required in the system. This will cause the role explosion.

User access rights are determined by roles. Changes in access rights in the RBAC algorithm are performed with user roles.

When we think of large organizations, as there are too many users, there are too many permission assignments; therefore security management becomes more difficult in the RBAC mechanism. It is necessary to define a complete role to implement this system. Also, management gets more difficult in the circumstances when the users are removed from the system or user authorities change. Installation for this user needs to be done from the beginning.

Today, technology is widely used. User needs change dynamically. The systems have high amounts of control requirements such as flexible authorization, fine grained access, privacy, user control.

Only one access control is provided in the RBAC mechanism. Access to the system continues until the session is over after the user logs in. No ongoing permission check is performed during the session.

Fine grained access refers to situations where data sensitivity means great importance. The roles are determined while the system is being installed in the RBAC mechanism. The roles determined by a general assumption can sometimes cause unauthorized access. This is an indication that the RBAC mechanism is not able to provide fine-grained access.

RBAC is not an effective mechanism in the situations where user identities change dynamically. It is useful for static roles. When the roles change, the system must be set from the beginning. Redesigning the system increases the cost. It causes a loss of time. In such cases, the RBAC mechanism runs slower and the bandwidth cost increases.

Threats To Validity

Information is an asset for today's organizations. The improper modification or disclosure may incur expenses for the organization. Therefore, authorization and authentication mechanisms have a vital role in information security. The security of sensitive data is important in companies with a continuous renewal of authority, such as employee dismissal. The proposed system have not been tested in such a company. In this study, role-based access control algorithm has been compared with attribute based access control system with the limited experiment set.

- The data set used for the test is insufficient. However, there are studies using similar data sets. Similar results are encountered [56]. The CP-ABE mechanism is run faster for the large data set which is mentioned in "The Importance of ABAC: Attribute-Based Access Control to Big Data: Privacy and Context" paper [57].

- When there is an authorization change in the system. The replaced user cannot access the old data. However, this is not a deficiency of our system. CP-ABE mechanism is constructed in this manner. All encrypted text must be re-encrypted before the new user can see it.
- The speed problem in the CPABE mechanism has been solved using AES algorithm [52].
- The user revocation and attribute revocation mechanism should be used together. Revocation of the attribute and user should be checked in the systems. In our system, both are used together.
- Thanks to the deduplication mechanism, storage costs and processing overhead has been precluded by eliminating duplicate copies of repeating data [48].



CHAPTER 7

CONCLUSION

This thesis proposes a security mechanism for data sharing in large organizations. Our goal is to securely share and store data on the network. Depending on our goal, previous studies have been examined. The weaknesses and limitations of these systems are listed. Aim of the study is eliminate the identified weaknesses and limitations.

In daily life, information security has been moved to an important dimension in many areas. It is necessary to work hard to prevent information theft. For this reason, work in this area should be made more intensive. Different algorithms should be developed. The security measures of the systems must be increased.

For this reason, a multi-layer authorization model is recommended. This model is designed for unauthorized access, data stack, and illegal changes in data sharing or sharing environment and user identity impersonation attacks. The network administrator contributes to the system in order to provide user authenticity and to meet the initial security requirements of the system. In addition, a cancellation mechanism has been proposed that is controlled by the network administrator to check user validity. The data administrator identifies system attributes and stores them in secure storage areas. It also realizes the attribute definitions for system and users. The data administrator also provides attribute validity to ensure data validity. With the CP-ABE based encryption mechanism, data security is achieved through user roles and provided with attributes. It has been found that bandwidth cost can be reduced by data deduplication.

Five different mechanisms have been used in the system. Identity-Based Authentication, Digital Signature, CP-ABE, Revocation, Deduplication. Identity Based Authentication controls user login credentials. The Digital Signature shows the changes that the user made on the data. It prevents the denial problem. CP-ABE

provides encryption of data through the attributes. The revocation mechanism controls the user privileges. This mechanism limits the access of data for the unauthorized users. It has removed the threat of unauthorized access. The deduplication mechanism has many benefits.

- The loss of time by blocking prevent the re-encryption
- Storage space is reduced
- The cost is reduced

In this developed mechanism, security vulnerabilities encountered in systems are examined. Then, the solutions based on these vulnerabilities have been produced. The project can be applied to the real system. The main contribution of our study is the addition of revocation mechanism without harming the security and without redesigning the system. When we compare the system with the relevant studies, our system has the following advantages.

- The proposed schema combines the authorization and authentication mechanism with secure file. This method provides efficient data and user controls.
- Two different key managers is proposed in the system. They are network and data manager. The network manager performs the user controls and user verification. It also manages the revoked user and revocation set. The data manager performs attribute checks.
- Encryption is done with the data policy that is defined by data owner according to the attributes of other users in the system. Thus, the system provides flexible authorization. It is not necessary to know in previously who will display the data. Targeted user group can display data with the own attributes.
- In companies, the signatory must be an authorized user. The user's authority should be controlled. Therefore, the identity-based signature mechanism is used instead of the digital signature. Authentication and integrity check is achieved by this signature.
- The key chain mechanism is used for the data encryption. This mechanism increases the process efficiency.
- The encryption process is combined with the deduplication mechanism. Thus, the cost of data storage is reduced.
- The IBE mechanism used for authentication is update with the TLS system.

REFERENCES

- [1] D. Oswald, *Identity Based Encryption*, Ruhr-Universitat Bochum, 2008.
- [2] D. Boneh ve M. Franklin, «Identity-Based Encryption from the Weil Pairing,» *Springer*, cilt 32, no. 3, pp. 586-615, 2003.
- [3] K. G. Paterson ve J. C. Schuldt, *Efficient Identity-based Signatures in the Standart Model*, London: Information Security Group, 2006.
- [4] B. Adida, *Pairing-Based Cryptography*, 2004.
- [5] S. Venugopalan, *ABE Scheme*, 2010.
- [6] W. Cui, C. Du ve J. Chen, *CP-ABE Based Privacy-Preserving User Profile Matching in Mobile Social Networks*, PLOS, 2016.
- [7] X. JIN, *ATTRIBUTE-BASED ACCESS CONTROL MODELS AND IMPLEMENTATION IN CLOUD INFRASTRUCTURE AS A SERVICE*, Texas, San Antonio: THE UNIVERSITY OF TEXAS AT SAN ANTONIO, 2014.
- [8] M. ÖZEN, «mustafaozen,» wordpress, 10 Şubat 2016. [Çevrimiçi]. Available: <https://mustafaozen.wordpress.com/2016/02/10/erisim-kontrol-sistemleri/>. [Erişildi: 22 Şubat 2017].
- [9] "ATTRIBUTE BASED ACCESS CONTROL(ABAC)," 17 July 2013. [Online]. Available: <http://csrc.nist.gov/projects/abac/index.html>.
- [10] J. Li, X. Li, L. Wang, D. He, H. Ahmad ve X. Niu, «Fuzzy encryption in cloud computation: efficient verifiable outsourced attribute-based encryption,» *SpringerLink*, cilt 22, no. 3, pp. 707-714, 2018.
- [11] P. V. Kumar ve R. Aluvalu, «Key Policy Attribute Based Encryption (KP-ABE): A Review,» *International Journal of Innovative and Emerging Reseach in Engineering*, 2015.
- [12] M. Ion ve J. Zhang, *Attribute based encryption and routing*, 3rd ACM SIGCOMM Workshop on Information-centric Networking, 2013.

- [13] B. Li, A. Verleker, D. Huang, Z. Wang ve Y. Zhu, «Attribute-based access control for ICN naming scheme,» *IEEE Conference on Communications and Network Security*, pp. 391-399, Oct. 2014.
- [14] H. Cui, R. H. Deng, H. Lai, X. Yi ve S. Nepal, «An efficient and expressive ciphertext-policy attribute-based encryption scheme with partially hidden access structures, revisited,» *ELSEVIER*, cilt 133, pp. 157-165, 2018.
- [15] N. Helil ve K. Rahman, «CP-ABE Access Control Scheme for Sensitive Data Set Constraint with Hidden Access Policy and Constraint Policy,» *Security and Communication Networks*, 2017.
- [16] S. Wang, J. Ye ve Y. Zhang, *A keyword searchable attribute-based encryption scheme with attribute update for cloud storage*, PLOS ONE, 2018.
- [17] S. Porwal ve S. Mittal, «Implementation of Ciphertext Policy-Attribute Based Encryption (CP-ABE) for fine grained access control of university data,» *IEEE*, pp. 1-7, 2017.
- [18] G. Yu, X. Ma, Z. Cao, G. Zeng ve W. Han, *Accountable CP-ABE with Public Verifiability: How to Effectively Protect the Outsourced Data in Cloud*, Research Gate, 2017.
- [19] R. Sadikin, Y. H. Park ve K. H. Park, «Secure Attribute-Based Access Control with a Ciphertext-Policy Attribute-Based Encryption Scheme,» *J Korea Industr Inf Syst Res*, cilt 19, no. 1, 2014.
- [20] J. Bethencourt, A. Sahai ve B. Waters, *Ciphertext-Policy Attribute-Based Encryption*.
- [21] Z.-y. W. J. M. J.-j. W. S.-z. M. J.-c. R. Yong CHENG†, *Efficient revocation in ciphertext-policy attribute-based encryption based cryptographic cloud storage*, Journal of Zhejiang University, 2013.
- [22] H. Hong, D. Chen ve Z. Sun, «A practical application of CP-ABE for mobile PHR system: a study on the user accountability,» *Springer Open*, no. 1320, pp. 1-8, 2016.
- [23] S. Venugopalan, *Efficient Multi-level Threshold Attribute Based Encryption*, UT Computer Science.
- [24] Z. Wang, C. Cao, N. Yang ve V. Chang, «ABE with improved auxiliary input for big data security,» *ELSEVIER*, cilt 89, pp. 41-50, 2017.
- [25] W. Cui, C. Du ve J. Chen, *CP-ABE Based Privacy-Preserving User Profile Matching in Mobile Social Networks*, PLOS ONE, 2016.

- [26] Q. W. Y. M. J. Z. Leyou Zhang, *Privacy-Preserving and Secure Sharing of PHR in the Cloud*, CrossMark, 2016.
- [27] D. C. Z. S. Hanshu Hong, *A practical application of CP-ABE for mobile PHR system: a study on the user accountability*, SpringerPlus, 2016.
- [28] B. Waters ve A. Lewko, *Decentralizing Attribute-Based Encryption*, Texas: University of Texas at Austin.
- [29] L. Cao, J. Zhang, X. Dong , C. Xi, Y. Wang, Y. Zhang, X. Guo ve T. Feng, « based on blinded CP-ABE searchable encryption cloud storage service scheme: A Based on blinded CP-ABE searchable encr cloud stor serv mech,» *International Journal of Communication Systems*, cilt 31, no. 10, 2018.
- [30] X. Xiao-long, Z. Qi-tong ve Z. Jing-lan, «NC-MACPABE: Non-centered multi-authority proxy re-encryption based on CP-ABE for cloud storage systems,» *Journal of Central South University: Science & Technology of Mining and Metallurgy*, cilt 24, no. 4, pp. 807-819, 2018.
- [31] L. Wen-Win, L. Xue-Lei, W. Qiao-Yan, Z. Shuo ve Z. Hua , «Flexible CP-ABE Based Access Control on Encrypted Data for Mobile Users in Hybrid Cloud System,» *Journal of Computer Science and Technology*, cilt 32, no. 5, pp. 974-991, 2017.
- [32] J. Zhang, X. Dong, C. Xi, Y. Wang, Y. Zhang, X. Guo ve T. Feng, «A based on blinded CP-ABE searchable encryption cloud storage service scheme,» *International Journal of Communication Systems*, cilt 31, no. 10, pp. 1-15, 2018.
- [33] W. Hao, Z. Zhihua, W. Lei ve H. Debiao, «New large-universe multi-authority ciphertext-policy ABE scheme and its application in cloud storage systems,» *Journal of High Speed Networks*, cilt 22, no. 2, pp. 153-167, 2016.
- [34] Z. Wang ve M. He, *CP-ABE with Hidden Policy from Waters Efficient Construction*, SAGE journals, 2016.
- [35] Z. Zhou ve D. Huang, *Efficient and Secure Data Storage Operations for Mobile Cloud Computing*, Arizona: Arizona State University, 2016.
- [36] J. Li, Y. Shi ve Y. Zhang, «Searchable ciphertext- policy attribute- based encryption with revocation in cloud storage,» *International Journal of Communication Systems*, cilt 30, no. 1, 2017.

- [37] Z. Z. L. W. P. L. Hao Wang, «New directly revocable attribute-based encryption scheme and its application in cloud storage environment,» *Springer Link*, cilt 20, no. 3, pp. 2385-2392, 2017.
- [38] J. Zhou, H. Duan, K. Liang, Q. Yan, F. Chen, F. R. Yu, J. Wu ve J. Chen, «Securing Outsourced Data in the Multi-Authority Cloud with Fine-Grained Access Control and Efficient Attribute Revocation,» *OXFORD ACADEMIC*, cilt 60, no. 8, pp. 1210-1222, 2017.
- [39] P. Zhang, Z. Chen, J. K. Liu ve K. Liang, «An efficient access control scheme with outsourcing capability and attribute update for fog computing,» *ELSEVIER*, cilt 78, no. 2, pp. 753-762, 2018.
- [40] Q. Han, Y. Zhang ve H. Li, «Efficient and robust attribute-based encryption supporting access policy hiding in Internet of Things,» *ELSEVIER*, cilt 83, pp. 269-277, 2018.
- [41] F. K, W. J, W. X, L. H ve Y. Y, *A Secure and Verifiable Outsourced Access Control Scheme in Fog-Cloud Computing*, US: PubMed, 2017.
- [42] M. Xiao, J. Zhou, X. Liu ve M. Jiang, *A Hybrid Scheme for Fine-Grained Search and Access Authorization in Fog Computing Environment*, MDPI, 2017.
- [43] Y. Jiang, W. Susilo, Y. Mu ve F. Guo, «Ciphertext-policy attribute-based encryption against key-delegation abuse in fog computing,» *ELSEVIER*, cilt 78, no. 2, pp. 720-729, 2018.
- [44] D. K. N. Junbeom Hur, «Attribute-Based Access Control with Efficient Revocation in Data Outsourcing Systems,» *IEEE*, cilt 22, no. 7, pp. 1214-1221, 2011.
- [45] Y. Li, J. Zhu, X. Wang , Y. Chai ve S. Shao, *Optimized Ciphertext-Policy Attribute-Based Encryption with Efficient Revocation*, International Journal of Security and Its Applications Vol.7 No.6 pp385-394, 2013.
- [46] S. Yu, Y. Zheng, K. Ren ve W. Lou, *Scalable and Secure Sharing of Personal Health Records in Cloud Computing using Attribute-based Encryption*, IEEE, 2012.
- [47] H. Wang, D. He, J. Shen, Z. Zheng, X. Yang ve M. H. Au, «Fuzzy matching and direct revocation: a new CP-ABE scheme from multilinear maps,» *Springer Link*, cilt 22, no. 7, pp. 2267-2274, 2017.
- [48] H. Kwon, C. Hahn, D. Kim ve J. Hur, «Secure deduplication for multimedia data with user revocation in cloud storage,» *Springer Science+Business Median*, pp. 5889-5903, 13 March 2015.

- [49] W. DING, R. DENG ve Z. YAN, *Secure encrypted data deduplication with ownership proof and user revocation*, Singapore: Singapore Management University, 2017.
- [50] A. UĞUR ve İ. SOĞUKPINAR, *Multilayer Authorization Model and Analysis of Authorization Methods*, TÜBİTAK, 2016.
- [51] F. Yundong, W. Xiaoping ve W. Jiasheng, «Multi-authority Attribute-Based Encryption Access Control Scheme with Hidden Policy and Constant Length Ciphertext for Cloud Storage,» *IEEE Second International Conference*, 2017.
- [52] R. Li, H. Asaeda, J. Li ve X. Fu, «A distributed authentication and authorization scheme for in-network big,» *ELSEVIER*, pp. 1-10, 2017.
- [53] «github,» 2013. [Çevrimiçi]. Available: <https://github.com/junwei-wang/cpabe>. [Erişildi: 2018].
- [54] «github,» 2018. [Çevrimiçi]. Available: <https://github.com/kawasima/rbac-example>. [Erişildi: 2018].
- [55] S. Verma, M. Singh ve S. Kumar, «Comparative analysis of Role Base and Attribute Base Access Control Model in Semantic Web,» *International Journal of Computer Applications*, 18 5 2012.
- [56] Z. Xu ve S. D. Stoller, *Mining Attribute-based Access Control Policies*, Stony Brook University, 2014.
- [57] A. Cavoukian, M. Chibba, G. Williamson ve A. Ferguson, *The Importance of ABAC: Attribute-Based Access Control to Big Data: Privacy and Context*, RYERSON UNIVERSITY, 2015.
- [58] S. Roschke, L. Ibraimi, F. Cheng ve Meinel Christoph, *Secure Communication using Identity Based Encryption*, Germany: University of Potsdam, 2014.

APPENDIX

```
public static void main(String[] args) {  
    CPABEImpl.debug = true;  
    String encF_N = "210.docx";  
    String encF_N2 = "TEZ.docx";  
    String cipher_F_N = "test.cpabe";  
    String PK_F_Name = "PK_F";  
    String PK_F_Name2 = "PK_F2";  
    String PK_F_Name3 = "PK_F3";  
    String MK_F_Name = "MK_F";  
    String MK_F_Name2 = "MK_F2";  
    String MK_F_Name3 = "MK_F3";  
    String SK_F_Name = "SK_F";  
    String SK_F_Name2 = "SK_F2";  
    String SK_F_Name3 = "SK_F3";  
    String u = "2 of (arastirmaGorevlisi,asistan,dekan)";  
    String[] user_attr = new String[]{"arastirmaGorevlisi", "asistan"};  
    setup(PK_F_Name, MK_F_Name);  
    long startEnc = System.currentTimeMillis();  
    enc(encF_N, u, cipherF_N, PK_F_Name);  
    long finishEnc = System.currentTimeMillis();  
    long StartKeyGen = System.currentTimeMillis();  
    keygen(user_attr, PK_F_Name, MK_F_Name, SK_F_Name);  
}
```

```

        long FinishKeyGen = System.currentTimeMillis();
        long startDec = System.currentTimeMillis();
        dec(cipherF_N, PK_F_Name, SK_F_Name);
        long finishDec = System.currentTimeMillis();
        long startEnc = System.currentTimeMillis();
        enc(encF_N2, u, cipherF_N, PK_F_Name2);
        long finishEnc = System.currentTimeMillis();
        long StartKeyGen = System.currentTimeMillis();
        keygen(user_attr, PK_F_Name2, MK_F_Name2, SK_F_Name2);
        long FinishKeyGen = System.currentTimeMillis();
        long startDec = System.currentTimeMillis();
        dec(cipherF_N, PK_F_Name2, SK_F_Name2);
        long finishDec = System.currentTimeMillis();
    }
    public static void setup(String PKFileName, String MKFileName){
        File PKFile = new File(PKFileName);
        File MKFile = new File(MKFileName);
        if(!PKFile.exists()){
            try {
                PKFile.createNewFile();
            } catch (IOException e) {
                e.printStackTrace();
            }
        }
        if(!MKFile.exists()){
            try {
                MKFile.createNewFile();
            } catch (IOException e) {
                e.printStackTrace();
            }
        }
    }
}

```

```

}
PublicKey PK = new PublicKey();
PublicKey PK1 = new PublicKey1();
PublicKey PK2 = new PublicKey2();
MasterKey MK = new MasterKey();
Element alpha = pairing.getZr().newElement().setToRandom();
PK.g      = pairing.getG1().newElement().setToRandom();
PK.gp     = pairing.getG2().newElement().setToRandom();
PK1.g     = pairing.getG1().newElement().setToRandom();
PK1.gp    = pairing.getG2().newElement().setToRandom();
PK2.g     = pairing.getG1().newElement().setToRandom();
PK2.gp    = pairing.getG2().newElement().setToRandom();
MK.beta   = pairing.getZr().newElement().setToRandom();
MK.g_alpha = PK.gp.duplicate().powZn(alpha);
PK.h      = PK.g.duplicate().powZn(MK.beta);
PK.g_hat_alpha = pairing.pairing(PK.g, MK.g_alpha);
PK1.h     = PK1.g.duplicate().powZn(MK.beta);
PK1.g_hat_alpha = pairing.pairing(PK1.g, MK.g_alpha);
PK2.h     = PK2.g.duplicate().powZn(MK.beta);
PK2.g_hat_alpha = pairing.pairing(PK2.g, MK.g_alpha);
SerializeUtils.serialize(PK, PKFile);
SerializeUtils.serialize(MK, MKFile);
}

```