Define the text content here...
keys need to be issued by a fully trusted key authority (KA). This brings a security risk that is known as key escrow problem. By knowing the secret key of a system user, the KA can decrypt all the user's cipher texts, which stands in total against to the will of the user. Secondly, the expressiveness of attribute set is another concern. As far as we know, most of the existing CP-ABE schemes can only describe binary state over attribute, for example, “1 - satisfying” and “0 - not-satisfying”, but not dealing with arbitrary-state attribute. In this paper, the weighted attribute is introduced to not only extend attribute expression from binary to arbitrary state, but also to simplify access policy. Thus, the storage cost and encryption cost for a cipher text can be relieved.

**EXISTING SYSTEM**

Existing CP-ABE schemes cannot support attribute with arbitrary state. In this paper, we revisit attribute-based data sharing scheme in order to solve the key escrow issue but also improve the expressiveness of attribute.

**EXISTING SYSTEM DISADVANTAGES**

- Low resilience
- Data is not secured

**PROPOSED SYSTEM**

We presented the performance and security analyses for the proposed scheme, in which the results demonstrate high efficiency and security of our scheme. Which can not only extend the expression from binary to arbitrary state, but also lighten the complexity of access policy? Therefore, both storage cost and encryption complexity for a cipher text are relieved.

**PROPOSED SYSTEM ADVANTAGES**

- Achieve a high resilience.
- Data is secured

**PROJECT DESCRIPTION GENERAL**

We analyze the problem of detecting misbehaviors based on the system performances we should avoid by using fair share detector. In this project we are sharing data with weighted attribute.

**PROBLEM DEFINITION**

To overcome the problem of existing system we are following attribute-based data sharing scheme used. By using this we can share data easily and securely…

**METHODOLOGIES**

Methodologies are the process of analyzing the principles or procedure for enabling secure external auditing process against data integrity and preventing key exposure in public cloud environment.

**MODULES**

- Authentication
- User
- Store the data into Cloud
- Access Control List
- Manager Sign Generation, Key Generation
- Verifier
ALGORITHM USED

Cipher text-policy attribute-based encryption

1. **KA.Setup**(1κ) → (PP1,MSK1). It is executed by KA. The probabilistic operation inputs a security parameter κ. It returns a public parameter PP1 and a master secret key MSK1.

2. **CSP.Setup**(1κ) → (PP2,MSK2). This algorithm is run by CSP. It inputs a security parameter κ and generates PP2 and MSK2. The public parameter and master secret key of system are denoted as PP = {PP1, PP2} and MSK = {MSK1, MSK2}, where MSK1 and MSK2 are stored by KA and CSP, respectively.

**Phase 2 (Data Encryption):** To improve efficiency of encryption, DO first encrypts file M with content key ck by using simple symmetric encryption algorithm, where file ciphertext is denoted as Eck(M). Then, the content key ck is encrypted by the following operation.

**DO. Encrypt**(PP, ck, A) → (CT). DO inputs PP, ck, and an access policy A. It encrypts ck and outputs content key ciphertext CT which implicitly contains A. Then, DO delivers Eck(M) and CT to CSP.

**Phase 3 (User Key Generation):**

This phase consists of **KA.KeyGen** and **CSP.KeyGen**.

1. **KA.KeyGen**(MSK1, S) → (SK1). KA inputs MSK1 and a set of weighted attributes S. It creates secret key SK1 described by S.

2. In **CSP.KeyGen**, we propose an improved two-party key issuing protocol to remove escrow. KA and CSP perform the improved protocol with master secret keys of their own. Thus, none of them can create the whole set of secret keys of users individually. Meanwhile, we assume that KA does not collude with CSP since they are honest (otherwise, they can obtain the secret keys of each user by sharing their master secret keys).

**CSP.KeyGen**(MSK2) → (SK2). CSP inputs MSK2 and the required information. It produces secret key SK2 by executing the following key issuing protocol.

SYSTEM DESIGN

Design Engineering deals with the various UML [Unified Modeling language] diagrams for the implementation of project. Design is a meaningful engineering representation of a thing that is to be built. Software design is a process through which the requirements are translated into representation of the software. Design is the place where quality is rendered in software engineering. Design is the means to accurately translate customer requirements into finished product.

![System model of CP-WBE-RE scheme in cloud computing.](image)

INTRODUCTION TO DOTNET

Microsoft .NET is a set of Microsoft software technologies for rapidly building and integrating
XML Web services, Microsoft Windows-based applications, and Web solutions. The .NET Framework is a language-neutral platform for writing programs that can easily and securely interoperate. There’s no language barrier with .NET: there are numerous languages available to the developer including Managed C++, C#, Visual Basic and Java Script. The .NET framework provides the foundation for components to interact seamlessly, whether locally or remotely on different platforms. It standardizes common data types and communications protocols so that components created in different languages can easily interoperate. “.NET” is also the collective name given to various software components built upon the .NET platform. These will be both products (Visual Studio.NET and Windows.NET Server, for instance) and services (like Passport, .NET My Services, and soon).

LANGUAGES SUPPORTED BY .NET

The multi-language capability of the .NET Framework and Visual Studio .NET enables developers to use their existing programming skills to build all types of applications and XML Web services. The .NET framework supports new versions of Microsoft’s old favorites Visual Basic and C++ (as VB.NET and Managed C++), but there are also a number of new additions to the family. Visual Basic .NET has been updated to include many new and improved language features that make it a powerful object-oriented programming language. These features include inheritance, interfaces, and overloading, among others. Visual Basic also now supports structured exception handling, custom attributes and also supports multi-threading. Visual Basic .NET is also CLS compliant, which means that any CLS-compliant language can use the classes, objects, and components you create in Visual Basic .NET. 36 Managed Extensions for C++ and attributed programming are just some of the enhancements made to the C++ language. Managed Extensions simplify the task of migrating existing C++ applications to the new .NET Framework.

ASP.NET OVERVIEW

ASP.Net is a web development platform, which provides a programming model, a comprehensive software infrastructure and various services required to build up robust web application for PC, as well as mobile devices. ASP.Net works on top of the HTTP protocol and uses the HTTP commands and policies to set a browser-to- server two-way communication and cooperation.

APPLICATION

It can be applied to the following areas

- Economic Related Application.
- Outsourcing Based Applications.
- Cloud Based Application.

FUTURE ENHANCEMENT

- Future system we focus on protection the privacy of outsourcing data and preventing player abuse in file syncing and sharing services in the cloud. We highlight the development of a group-oriented cryptosystem with especially for tracing and revoking methods that can ensure the security of player/editor.
In our future work, we are planning to introduce a comprehensive anomaly detection, using audit, pattern matching, and risk assessment, for identifying the suspected players.

**CONCLUSION**

We redesigned an attribute-based data sharing scheme in cloud computing. The improved key issuing protocol was presented to resolve the key escrow problem. It enhances data confidentiality and privacy in cloud system against the managers of KA and CSP as well as malicious system outsiders, where KA and CSP are semi-trusted. In addition, the weighted attribute was proposed to improve the expression of attribute, which can not only describe arbitrary state attributes, but also reduce the complexity of access policy, so that the storage cost of ciphertext and time cost in encryption can be saved. Finally, we presented the performance and security analyses for the proposed scheme, in which the results demonstrate high efficiency and security of our scheme.

**REFERENCES**


