isrjournals

International Journal of Advanced Research in Computer Science Engineering and Information Technology

Volume: 6, Issue: 3,Special Issue: 2 ,Apr,2023 ,ISSN_NO: 2321-3337

EFFICIENT MULTI-AUTHORITY ATTRIBUTE BASED SIGNCRYPTION

KIRUTHIGA.M[1],SUVETHA.A.R[2],SWETHA.V[3],SATHYA.S[4]

UG Scholar[1 2 3] - Department of CSE, GRT Institute of Engineering and Technology, Tiruttani.

Associate professor[4] - Department of CSE, GRT Institute of Engineering and Technology, Tiruttani.

kiruthigam48@gmail.com, suvetha25ram@gmail.com,

swethavijaykumar2510@gmail.com,ssathyaind@gmail.com

Abstract **-** Efficient multi-authority attribute-based signcryption (EMABSC) is a cryptographic technique that allows multiple authorities to collaborate in encrypting and signing messages based on certain attributes. In this paper, we propose an improved EMABSC scheme that enhances the security and efficiency of the existing approaches. Our scheme employs a hybrid encryption and signature mechanism to provide confidentiality, integrity, and authenticity of the signed and encrypted messages. It also allows multiple authorities to independently generate partial signatures and encrypt parts of the message basedon specific attributes, without revealing any information to each other. Toimprove the efficiency of the proposed scheme, we utilize a symmetric encryption algorithm in the encryption process, which reduces the computational cost compared to existing asymmetric encryption-based schemes. We also introduce a threshold mechanism that allows for flexible control of the number of authorities needed to decrypt and verify the signature of a message. We conducted a security analysis of the proposed scheme and proved its correctness and security against various attacks. Our performance evaluation results showed that our scheme outperforms existing EMABSC schemes in terms of computational efficiency and communication overhead, making it suitable for use in various applications such as e-commerce, e-government, and cloud computing.

KEYWORDS: Attribute Based Signature, Attribute Based Encryption, Attribute-Based Signcryption, Constant-Size Ciphertext, Multi Authority, Cloud Storage, Authentication, Confidentiality.

1.INTRODUCTION

The encryption technique is a unique process of securing the personal data and information. It is used by social media giants like WhatsApp. The Multi Authority based on signcryption is a huge benefit to the people and also to the industry. Recently, efficient fine-grained access mechanism has been studied as a main concern in cloud storage area for several years. Attribute-based signcryption (ABSC) which is logical combination of attribute-based encryption (ABE) and attribute-based signature (ABS), can provide confidentiality, authenticity for sensitive data and anonymous authentication. At the same time, it is more efficient than previous “encrypt-then-sign” and “sign-then-encrypt” patterns. However, most of the existing ABSC schemes fail to serve for real scenario ofmultiple authorities and have heavy communication overhead and computing overhead. Hence, we construct a novel ABSCscheme realizing multi-authority access control and constant-size ciphertext that does not depend on the number of attributes or authorities. To protect data from compromise and authenticate the sender at the same

time, encryption and digital signing are used together. They are also both used in tandem to fulfill compliance standards for companies. Standards, like the Federal Information Processing Standards (FIPS) or the General Data Protection Regulation (GDPR), require companies to protect data as securely as possible along with authenticating data received from others.

Our Results We resolve this problem in the affirmative. We give an efficient scheme for multiauthority attribute based encryption. We allow the sender to specify for each authorityk a set of attributes monitored by that authority and a number dk so that the message can be decrypted only by a user who has at least dk of the given attributes from every authority. We allow any number of attribute authorities to be corrupted, and guarantee the security of encryptions long as the required attributes cannot be obtained exclusively from those authorities and the trusted authority remains honest.

We also provide several extensions to our basic multiauthority scheme. We describe techniques to allow the encryptor to determine for each ciphertext how many attributes to require from each authority. We also describe a variant of our scheme in which the encryptor can specify a number D such that a user can decrypt if he has sufficient numbers of the given attributes from at least D authorities. It is this variant that would be used to implement the RI example above. In this example, we have 3 authorities, and the ciphertext will include 1 attribute from each. However, we only want to require that a user must have satisfactory attributes from 2 out of the 3 authorities in order to decrypt.

2. BACKGROUND

To solve cloud storage security issue by constructing multi-authority access control and constant size cipher text. To provide public verifiability of cipher text and privacy protection for the signcryptor. Recently, efficient data access mechanism has been considered as a main concern in cloud storage. Attribute-based signcryption (ABSC) can provide confidentiality, authenticity for sensitive data and anonymous authentication. At the same time, it is more efficient than previous “encrypt-then-sign” and “sign-then-encrypt” patterns. However, most of the existing ABSC

schemes fail to serve for real scenario of multiple authorities and have heavy communication overhead and computing overhead.

2.1.OVER VIEW OF CYBERSECURITY

Cyber Security is the body of technologies, processes, and practices designed to protect networks, devices, programs, and data from attack, theft, damage, modification or unauthorized access. The technique of protecting internet-connected systems such as computers, servers, mobile devices, electronic systems, networks, and data

from malicious attacks is known as cybersecurity. We can divide cybersecurity into two parts one is cyber, and the other is security. Cyber refers to the technology that includes systems, networks.

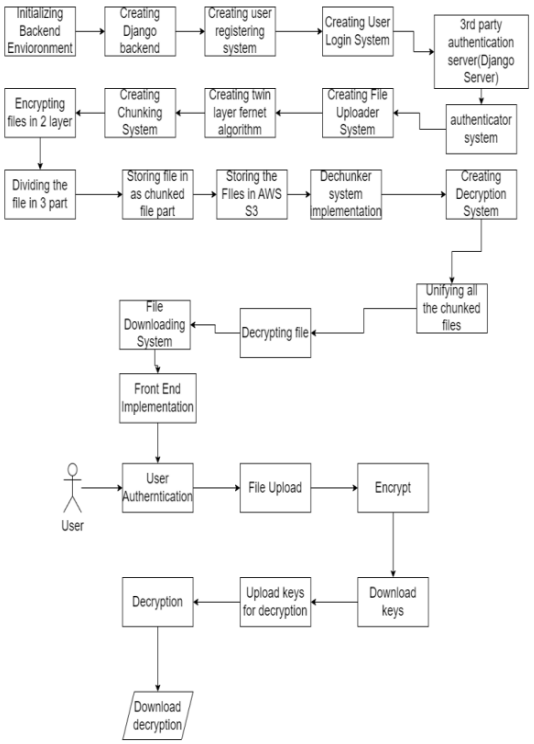

Fig 2:ABSC related to cybersecurity.

2.1Attribute Based Encryption(ABE)

Attribute-based encryption is a generalisation of public-key encryption which enables fine grained access control of encrypted data using authorisation policies. The secret key of a user and the ciphertext are dependent upon attributes (e.g. their email address, the country in which they live, or the kind of subscription they have). In such a system, the decryption of a ciphertext is possible only if the set of attributes of the user key matches the attributes of the ciphertext.A crucial security aspect of attribute-based encryption is collusion-resistance: An adversary that holds multiple keys should only be able to access data if at least one individual key grants access.

2.2Attribute-Based Signature (ABS)

Attribute-based signature (ABS) is a promising cryptographic primitive. It allows the signer to generate a signature with attributes satisfying the predicate without leaking more information, so as to provide message authenticity in an anonymous manner. The kind of authentication required in an attribute-based system differs from that offered by digital signatures, in much the same way public-key encryption does not fit the bill for attribute-based encryption. An attribute-based solution requires a richer semantics, including anonymity requirements, similar to signature variants like group signatures [17], ring signatures [30], and mesh signatures [11]. The common theme in all these signature primitives is that they provide a guarantee of unforgeability and signer anonymity.

A valid signature can only be generated in particular ways, but the signature does not reveal any further information about which of those ways was actually used to generate it. More specifically, group and ring signatures reveal only the fact that a message was endorsed by one of a list of possible signers. In a ring signature, the list is public, chosen by the signer ad hoc, and given explicitly. In a group signature, the group must be prepared in advance by a group manager, who can revoke the anonymity of any signer. In mesh signatures, a valid signature describes an access structure and a list of pairs (mi , vki), where each vki is the verification key of a standard signature scheme. A valid mesh signature can only be generated by someone in posession of enough standard signatures σi , each valid under vki , to satisfy the given access structure. In this work we introduce attribute-based signatures (ABS). Signatures in an ABS scheme describe a message and a predicate over the universe of attributes. A valid ABS signature attests to the fact that “a single user, whose attributes satisfy the predicate, endorsed the message.” We emphasize the word “single” in this informal security guarantee; ABS signatures, as in most attribute-based systems, require that colluding parties not be able to pool their attributes together.2 Furthermore, attribute signatures do not reveal more than the claim being made regarding the attributes, even in the presence of other signatures.

2.3Attribute-Based Signcryption (ABSC)

Attribute-Based Signcryption (ABSC) is a natural extension of Attribute-Based Encryption (ABE) and Attribute-Based Signature (ABS), where one can have the message confidentiality and authenticity together. Since the signer privacy is captured in security of ABS, it is quite natural to expect that the signer privacy will also be preserved in ABSC. In this paper, first we propose an ABSC scheme which is weak existential unforgeable and IND-CCA secure in adaptive-predicates models and, achieves signer privacy. Then,

by applying strongly unforgeable one-time signature (OTS), the above scheme is lifted to an ABSC scheme to attain strong existential unforgeability in adaptive-predicates model. Both the ABSC schemes are constructed on common setup, i.e the public parameters and key are same for both the encryption and signature modules.

3. SYSTEM DESIGN MODEL

System Design defines a comprehensive solution based on principles, concepts, and properties logically related and consistent with each other. The design has features, properties, and characteristics satisfying, as far as possible, the problem or opportunity expressed by a set of system requirements and life cycle concepts (e.g. operational, support) and is implementable through technologies (e.g., software, services, procedures, human activity). The System Design explores a general solution based on the algorithms and third-party providers. It has multiple modules which protects the data from theft.

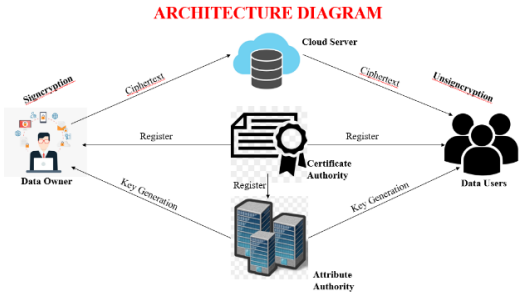

Fig 3:Architecture Diagram.

4. PROPOSED SYSTEM

We propose a Django based web application that uses a third-party authentication system to user authentication and does file encryption decryption using 2-layer fernet model.

¬ **Input :** Any sort of file that you want to encrypt

¬ **Output:** Encrypted file stored in server and decrypted downloadable file

Our scheme can ensure the confidentiality and the integrity of the multicasted messages, allows consumers to authenticate the source of the multicasted messages, achieves and non-repudiation property, and allows prompt revocation. Our security analysis demonstrates that the proposed scheme can thwart various security threats to the system. In order to address the main problems with the current ABSC schemes in cloud storage systems, such as the high communication overhead, the high computing overhead, and incompatibilities in multi-authority scenarios, we intend to propose an ABSC scheme. We create the KP-ABSC as well as the Multi-authority Attribute-based Signcryption with Constant-size Ciphertext (MACSC-ABSC) to combine access control for various authorities. This approach understands that the number of authorities and characteristics increasing in the cloud storage system has no impact on the ciphertext size for the multi-authority scenario. In a nutshell, the ciphertext size does not change. The MACSC-ABSC method also incorporates the public verifiability for all trusted cloud servers and the signer privacy. In particular, the amount of computation needed to produce the ciphertext and decipher the plaintext message is independent of the number of authorities and characteristics.

4.1. METHODOLOGIES

THIRD PARTY AUTHENTICATION

Input the given file (any file) to the front-end. The data which is sent must be legit. The given data undergoes third party authentication. This third party is created by us using Django environment.

ENCRYPTION AND DECRYPTION

Encryption and decryption are done using Fernet algorithm which is an advancement of AES algorithm. It has better salting and hashing method.

4.2 ENVIRONMENTAL REQUIREMENTS

- VS Code
- Python
- Django

4.2.1VS CODE

Visual Studio Code, also commonly referred to as VS Code,[9] is a source-code editor made by Microsoft with the Electron Framework, for Windows, Linux and macOS.[10] Features include support for debugging, syntax highlighting, intelligent code completion, snippets, code refactoring, and embedded Git. Users can change the theme, keyboard shortcuts, preferences, and install extensions that add functionality. Visual Studio Code is a lightweight but powerful source code editor which runs on your desktop and is available for Windows, macOS and Linux. It comes with built-in support for JavaScript, TypeScript and Node.js and has a rich ecosystem of extensions for other languages and runtimes (such as C++, C#, Java, Python, PHP, Go, .NET).

4.2.2PYTHON

Python is a high-level, general-purpose programming language. Its design philosophy emphasizes code readability with the use of significant indentation via the off-side rule. Python is dynamically typed and garbage-collected. It supports multiple programming paradigms, including structured (particularly procedural), object-oriented and functional programming. It is often described as a "batteries

included" language due to its comprehensive standard library.

Guido van Rossum began working on Python in the late 1980s as a successor to the ABC programming language and first released it in 1991 as Python 0.9.0. Python 2.0 was released in 2000. Python 3.0, released in 2008, was a major revision not completely backward-compatible with earlier versions. Python 2.7.18, released in 2020, was the last release of Python 2

4.2.3Django

Django is a high-level Python web framework that enables rapid development of secure and maintainable websites. Built by experienced developers, Django takes care of much of the hassle of web development, so you can focus on writing your app without needing to reinvent the wheel. It is free and open source, has a thriving and active community, great documentation, and many options for free and paid-for support.

5. MODULE DESCRIPTION

5.1 INITIALIZING BACKEND USING DJANGO

Following the completion of the project's basic setup and the addition of the first
app, you may use the name utility to create a new directory or add a new python package to your app. Create a duplicate of the init.py file and transfer it to the utilities folder. Create a new textdocument in the utilities folder and name it encryption util.py. Build a new feature that encryptsthe supplied data. Protect the ENCRYPT KEY. Keep it in the production.py file of settings, and don't add it to git. Due to the possibility of needing to send encoded data via a URL, we are additionally converting the encoded text to a URL-safe base64 format. Return null if an erroroccurred, and log the error message. We can decrypt any encrypted text by just doing the opposite of what was done to encrypt it.

5.2 MODEL IMPLEMENTATION

The fernet recipe is part of the cryptography package, and it's a method for encrypting and authenticating data that you can use. It is not too difficult to implement, and it removes a significant amount of the element of uncertainty that is inherent in cryptography. A message that has been encrypted and authenticated with fernet cannot be read by an adversary nor can it be tampered with when it has been correctly implemented. In addition to an initialization vector that is selected at random, fernet requires three critical inputs, which are as follows:

- A message in plaintext that was entered by the user. This is the information that the user wishes to have encrypted, and it is presented in the form of a byte string that can be chosenat random.

- A key that was generated by the user and has 256 bits of length.

- The time at the moment.

After being processed by the fernet formula, these inputs will result in the production of a token. This has both the message in an encrypted form as well as an HMAC that authenticates the message (we will explain what an HMAC is further down the page).

Together, they make it impossible to view the message or make any changes to it if thekey is not there. We will use a twin fernet layer for this encryption decryption thing. So we willcreate two fernet cipher pipeline to pass our file from that pipeline and create ciphered file.

Developing a system for file chunking and dechunking: In this step, we will develop asystem that, given a given file, will either chunk it or dechunk it before saving it on the server. During the process of decryption, we will combine all of the files and then send the merged setto the pipeline for decryption.

Introducing a Second Element Auth: After generating an authentication token, we willsend it to the user's email address using Amazon Simple Email Service (SES). The secondary Django server will have API endpoints to store user data together with the authentication token.

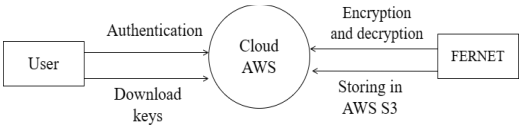

Fig 5.1 model implementation

5.3 CREATING FRONTEND

We have designed a web-based application in order to provide the authorised users of the programme with the ability to communicate with one another and share data with one another. The user is required to give their information in a form for Owner Registration, and then as a verification step, he is required to provide an image as a captcha.

The form may be found on the user's dashboard. On the internet, you may find this particular form. After that, the administrator examines the user's profile and, once they are satisfied with the information, provides the user with their credentials. The next thing that needsto be done in the procedure is for the user to upload the file into the system while concurrentlyproviding a title and description that are acceptable.

After that step, the twin layer Fernet method that was utilised in the model is applied tothe text files and processed using those files. A response is given to the acceptance of the user-key request. After a protracted period of time, the user finally acquires the key that is requiredto download encrypted information in the form of information that is valuable.

A front-end developer creates websites and applications using web languages such as HTML, CSS, and JavaScript that allow users to access and interact with the site or app. Whenyou visit a website, the design elements you see were created by a front-end developer.

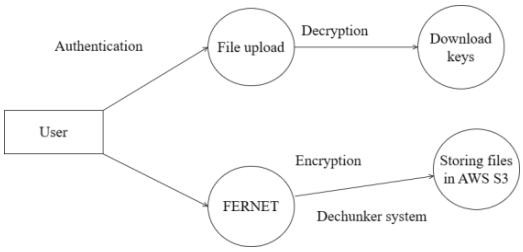

Fig 5.2 creating frontend.

6. EXPERIMENTAL RESULTS

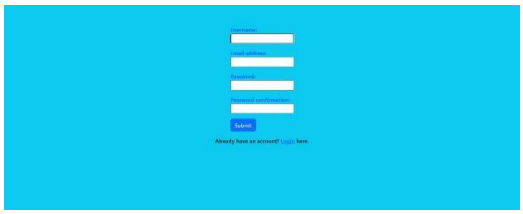

Fig 6.1 Register process

Fig 6.2Login process

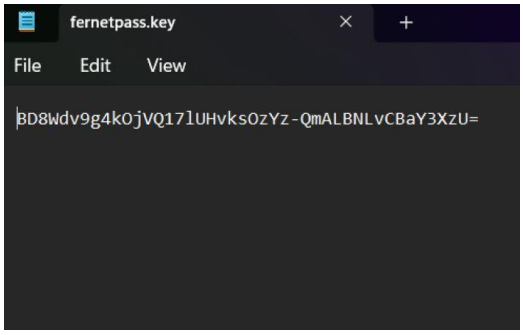

Fig 6.3 File to Upload

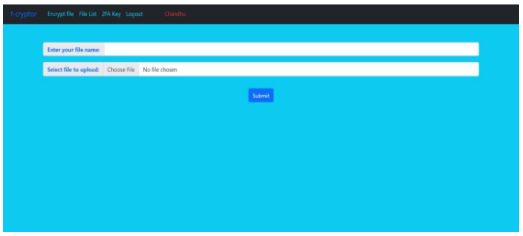

Fig 6.4 Uploading File Process.

Fig6.5Download after Signcryption

7.CONCLUSION

In conclusion, we have proposed an efficient multi-authority attribute-based signcryption (EMABSC) scheme that enhances the security and efficiency of existing approaches. Our scheme provides confidentiality, integrity, and authenticity of the signed andencrypted messages and allows multiple authorities to independently generate partial signatures and encrypt parts of the message based on specific attributes without revealing anyinformation to each other. We have utilized a hybrid encryption and signature mechanism to provide a secure and efficient solution for multi-authority signcryption. By using a symmetric encryption algorithm, we have reduced the computational cost of the scheme while introducinga threshold mechanism that allows for flexible control of the number of authorities needed to decrypt and verify the signature of a message. Our security analysis shows that our scheme is resistant to various attacks, and our performance evaluation results demonstrate that our scheme outperforms existing EMABSC schemes in terms of computational efficiency and communication overhead. Overall, our proposed scheme provides a practical solution for secure communication in various applications such as e-commerce, e-government, and cloud computing. It can also be extended to support dynamic policies and efficient revocation mechanisms, making it a promising solution for future research in this field.

8. REFERENCE

[1] L. Wang, Z. Guan, Z. Chen and M. Hu, "Multi-receiver signcryption scheme with multiple key generation centres through public channel in edge computing," in China Communications, vol. 19, no. 4, pp. 177-198, April 2022

[2] Y. Zhao, A. Ruan, G. Dan, J. Huang and Y. Ding, "Efficient Multi-Authority Attribute-based Signcryption with Constant-Size Ciphertext," *2021 IEEE Conference on Dependable and Secure Computing (DSC)*, 2021

[3] L. Shuquan and Z. Huiqi, "Online/Offline Attribute-Based Encryptioin with Multi-Authority Access Control," 2021 18th International Computer Conference on Wavelet Active Media Technology and Information Processing (ICCWAMTIP), 2021

[4] Y. Ming, B. He and C. Wang, "Efficient Revocable Multi-Authority Attribute-Based Encryption forCloud Storage," in IEEE Access, vol. 9, pp. 42593-42603, 2021

[5] Y. Li et al., "SDABS: A Flexible and Efficient Multi-Authority Hybrid Attribute-Based Signature Scheme in Edge Environment," in IEEE Transactions on Intelligent Transportation Systems, vol. 22, no. 3, pp. 1892-1906, March 2021

[6] K. Huang, "Revocable Large Universe Decentralized Multi-Authority Attribute-Based Encryption Without Key Abuse for Cloud-Aided IoT," in IEEE Access,2021.

[7] X. Liu, W. Chen, Y. Xia and R. Shen, "TRAMS: A Secure Vehicular Crowdsensing Scheme Based on Multi-Authority Attribute-Based Signature," in IEEE Transactions on Intelligent Transportation Systems 2020.

[8] J. Priyanka, K. R. Rajeshwari and M. Ramakrishnan, "Operative Access Regulator for Attribute Based Generalized Signcryption Using Rough Set Theory," 2020 International Conference on Electronics and Sustainable Communication Systems (ICESC), 2020.

[9] X. Yang, R. Liu, G. Chen, M. Wang and C. Wang, "Security analysis of a certificateless signcryption mechanism without bilinear mapping," 2020 IEEE 4th Information Technology, Networking, Electronic and Automation Control Conference (ITNEC), 2020.

[10] Q. Xu, C. Tan, Z. Fan, W. 8Zhu, Y. Xiao and F. Cheng, "Secure Multi-Authority Data Access Control Scheme in Cloud Storage System Based on Attribute-Based Signcryption," in *IEEE Access*, 2018.

ABOUT THE AUTHOR

MS KIRUTHIGA.M is studying BE., in computer science and engineering from GRTIET in Anna University. Her interested area is cybersecurity and android applications.

MS SUVETHA.A.R is studying BE., in computer science and engineering from GRTIET in Anna University. Her interested area is cybersecurity and Data Mining.

MS SWETHA.V is studying BE., in computer science and engineering from GRTIET in Anna University. Her interested area is cybersecurity and Data Science.

DR SATHYA.S ASSOCIATE PROFESSOR
Computer Science and Engineering in GRTIET
In Anna University. Her interested area is Data Mining, Data Science and Big Data.