IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁂ Impact Factor 7.39 ⁂ Vol. 11, Issue 6, June 2022

DOI: 10.17148/IJARCCE.2022.11633

Encrypted E-Mails with Practical Forward Secrecy

K.K.Varshaa[1], K.Sajar Nisha[2], A.S.Balaji[3], J.Vinothini[4]

Student, B.E. Computer Science and Engineering, Anand Institute of Higher Technology, Chennai, India[1,2]

Assistant Professor, CSE, Anand Institute of Higher Technology, Chennai, India[3]

Assistant Professor, CSE, Anand Institute of Higher Technology, Chennai, India[4]

Abstract: Cloud computing may be a general term that involves delivering hosted services over the world wide web. These services are divided into three main categories: infrastructure as a service (IaaS), platform as a service (PaaS) and software as a service (SaaS). Cloud infrastructure involves hardware and software components for proper implementation of a model. Cloud computing can be thought of as utility computing or on-demand computing. Cloud computing works by enabling client devices to access data and cloud applications over the web from remote physical servers, databases and computers. With the widespread use of cloud emails and frequent reports on email leakage events, a security property called forward secrecy becomes desirable for both individuals and cloud email service providers to strengthen the protection of cloud email systems. Specifically, forward secrecy can guarantee the confidentiality of these previously encrypted emails whether or not the user's secret key gets exposed. However, thanks to the failure to satisfy the protection requirements of email systems simultaneously, typical methods like Diffie-Hellman key exchange and forward-secure public-key encryption, haven't been widely approved and adopted. To capture forward secrecy of encrypted cloud email systems, we introduced a replacement cryptographic primitive called forward-secure puncture able identity-based encryption (fs-PIBE), which enables the user to perform fine-grained revocation of decryption capacity. in additional detail, the user is allowed to preserve the decryption capacity of unreceived encrypted emails while abolishing that of these received ones. Thus, it provides more practical forward secrecy than typical manners, during which the decryption capacity of received and unreceived encrypted emails is revoked simultaneously. supported such a primitive, we build a framework of encrypted cloud email systems.

Keywords: cloud emails, Forward secrecy, Diffie-Hellman, forward-secure public-key encryption, identity-based encryption, fs-PIBE.

I. INTRODUCTION

Cloud Computing was founded in the year 1950 with the implementation of mainframe computers. The development of the computation ability paved way for the cloud computing to become an important tool for people and enterprises who need computing resources. In the era of cloud computing, various types of data from both academic and industrial communities are constantly subcontracted to public clouds by consumers. Nowadays security and data privacy are key issues for cloud computing and the Internet of Things (IoT) environment. However, in real applications, third-party cloud servers could not be completely trusted for they may be malicious or have some potential threads. Cloud Computing is the delivery of various computing services over the Cloud through Internet. It is better for companies can rent access to anything from applications to storage from a cloud service provider rather than owning their own computing infrastructure or data centers. It is payable. ELECTRONIC mail, e-mail, in short, has been wildly used instead of traditional communication established by pen and paper. Modern e-mail systems transfer not only text but also electronic documents, voice, graphics, animations, and financial transactions via the internet. E-mail has always been one of the main methods for individuals and enterprises to transmit data and exchange information. Moreover, the emergence and commercialization of cloud computing greatly facilitate those small organizations and start-ups to deploy their own cloud email systems, which are much scalable and cheaper than the traditional solution. This further expands the use of emails. The Radicating Group reported that, by 2020, the total number of business and consumer emails sent and received per day will exceed 306 billion, and the number of worldwide email users will top 4.0 billion.

1.1 OBJECTIVE

In this work we systematically explore the problem of providing forward secrecy in asynchronous secure data sharing systems. Our overall goal is to develop private key encryption that allows for fine-grained revocation of decryption capability.

This work is licensed under a Creative Commons Attribution 4.0 International License

DOI: 10.17148/IJARCCE.2022.11633

1.2 SCOPE

- The main objective of this project is to include Various types of employee decision support systems include specialist support such as mail and request, alerts and reminders based on head office systems that use computer representations of employee guidelines.
- By defining a set of goals and objectives for the development of a CDS intervention, a practice can make use of the five rights to determine the what (information), who (management), how (intervention), where (format), and when (workflow) for a proposed intervention.
- Organizations for sharing file within the organizations or from one organization to another.
- Government to share most confidential data.
- Educational institutions.

II. ANALYSIS

2.1 SYSTEM ANALYSIS

System Analysis is a combined process dissection the system responsibilities that are based on problem domain characteristics and user requirement.

2.1.1 Problem Definition

The manufacturing and assembly process for our email ID is as efficient as possible. (Ideal) Currently, Most of the companies did not share the data through their official website. All the using the data via third party applications such as gmail, Outlook etc. (Reality) To reduce the third party applications uses, We are using our own company website to share the data more securely. We are Using some Cryptography technique secure the data(Proposal).

2.1.2 Existing System

Users or customers details protection is major things to provide authorized services. There is number of user or customer possess the access with their mail ids. Unless security procedures unavailable, unknown users can get access with valid user data.

ALGORITHM USED

Fs-PIBE algorithm - Forward-secure puncturable identity-based encryption (fs-PIBE) is employed for enhancing security and privacy. This primitive enables to individually revoke the decryption capacity. It provides more practical forward secrecy than traditional forward-secure public key encryption, during which the decryption capacity of these received and unreceived emails are revoked simultaneously.

DISADVANTAGES

- It is not stable for network level sharing data.
- Hackers can easily deceive by providing them with a visually similar site.
- It is necessary to establish much larger and more recent security datasets.
- when dedicated server for this access management system will be developed.

2.1.3 Proposed system

Authentication procedures primarily protect the resource access. Service provider want to provide authorization services to users or customers after receiving their registration details depends on their wishes.

ALGORITHM USED

AES algorithm - The AES encryption algorithm is a symmetric block cipher algorithm that has a block size of 128 bits. It converts these individual blocks using keys of 128, 192, and 256 bits. When it encrypts these blocks, it joins them together to create the ciphertext. It's supported by a substitution-permutation network, also mentioned as an SP network. It consists of a series of operations, including replacing

DOI: 10.17148/IJARCCE.2022.11633

the inputs with specific outputs and bit shuffling.

ADVANTAGES

- It has standard procedure to share data for communication.
- The main advantage of the proposed technique lies in it has an ability to defend against several types of attacks.
- And add some module or states to improve more options to implementation.

III. SYSTEM DESIGN

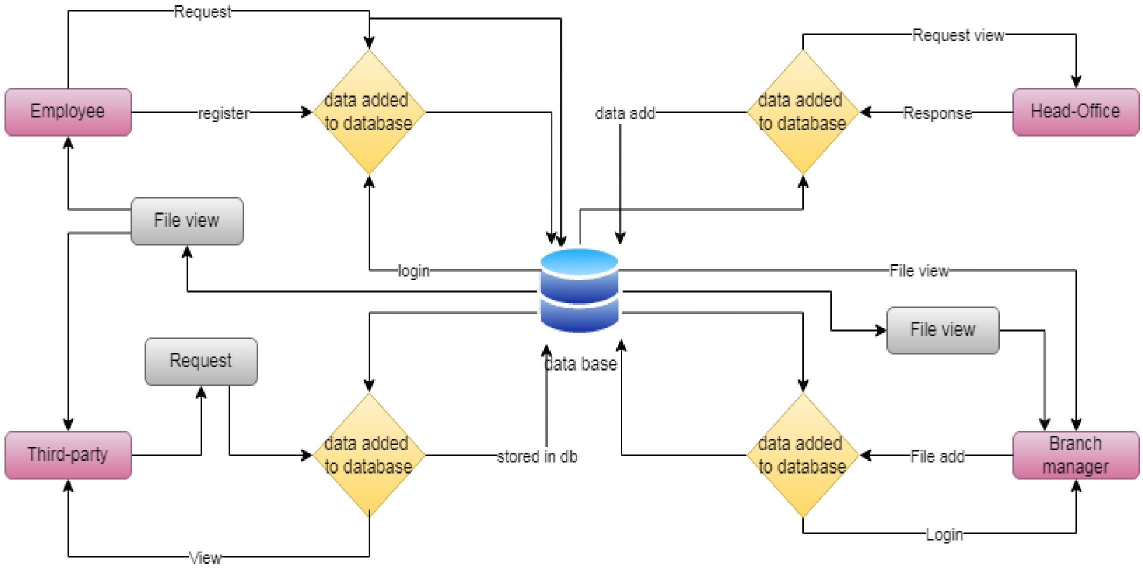

Figure 1.Overall Architecture Design

IV. MODULES

4.1 File management
4.2 File sharing
4.3 Request analysis
4.4 Theft management

4.1 FILE MANAGEMENT :

This module is used to upload, download and organize files of an organization. File management is done by the manager. The manager can upload the document for the employees to view. File management is fulfilled using an encryption technique. The file is protected using three levels of security that include Password protection, Authentication using QR code, and also by Encrypting the data in the file using the AES Algorithm. The manager has the sole authority to approve the employer's request to view the document.

4.2 FILE SHARING:

In the File sharing module, the manager permits the user to view and download the file. The file-sharing process starts with the manager uploading the document that has to be used by the employers. The employers will view the list of available Documents. They will send a request to view the necessary documents. The manager has to authenticate and approve the employee's request. once the request gets approved by the manager QR code, a secret key is given to the user through which the employer will authenticate their identity and view the document. In turn if an hacker requests to view the document the manager can turn down the request, if the manager approves the request and the hacker tries to view the data the secret key is not provided to the hacker in order to protect the file.

DOI: 10.17148/IJARCCE.2022.11633

4.3 REQUEST ANALYSIS:

While the administrator approves the new employer's registration, the manager has to authorize the access to file within the organization. The administrator will approve the registration of the firm's employers. When a hacker registers with the system the admin can review and deny the request and in Manager end the manager can deny the Hacker request from accessing the organization's data.

4.4 THEFT MANAGEMENT

Theft management is carried out in three stages, These include the administrator approval of employer accounts, manager approving the file view request. If the hacker manages to break these two stages the third stage provides file protection in three further more stages like secret key, QR code and the content of the file being encrypted.

V. RESULTS AND DISCUSSION

In this paper, to capture the forward secrecy of encrypted cloud email systems, we introduce a new cryptographic primitive named forward-secure puncture-able identity-based encryption (fs-PIBE), which enables an email user to perform fine-grained revocation of decryption capacity. Based on such a primitive, we build a framework of encrypted cloud email systems.

VI. CONCLUSION

In this paper, We offer a novel cryptographic fundamental called forward-secure puncturable identity-based encryption technique to capture practical forward secrecy of cloud email systems, which does not require the assistance of PKIs or the synchronisation of the email sender and receiver. To be more specific, we clarify the syntax and security concept of fs-PIBE before presenting a framework for encrypted cloud email systems.

REFERENCES

[1]. Ali Reza Galib, Nafize Ishtiaque Hossain, Raihan Bin Mofidul, 19 December 2019, A Vision Based Three-Layer Access Management System withIoT Integration.

[2]. Brajendra Panda, Jonathan White, 8-11 June 2009, Implementing PII honey tokens to mitigate against the threat of malicious insiders.

[3]. Gilchan Park, Julia Rayz, 7-10 Oct. 2018, Ontological Detection of Phishing Emails.

[4]. Guanyu Yan , Qinlong Huang, 03 September 2021, Privacy-Preserving Traceable Attribute-Based Keyword … Search in Multi-Authority Medical Cloud.

[5]. Jiawei Zhao, Rahat Masood, Suranga Seneviratne, 04 June 2021, A Review of Computer Vision Methods in Network Security.

© IJARCCE This work is licensed under a Creative Commons Attribution 4.0 International License