Enabling (End-To-End) Encrypted Cloud Mails With Practical Forward Secrecy

S.Akashiya[1], Dr.J.jeyachitra[2]
[1, 2] Dept of Computer Science And Application
[1, 2]Periyar Maniammai Institute Of Science And Technology Vallam, Thanjavur, Tamilnadu, India

Abstract- *Cryptography plays an important role in today and future's confidential data communication. Cryptographic applications provide the secure communication medium to transfer data reliably. It ensures more privacy and ability to communication and other information, gives individual, group and organization to restore personal privacy. Nowadays online users want to register their account to access concern sites such as online tutorial, online purchase, online resource access, hosting services, social networks, etc. However, service provider or authority person ensure the registration and login process with valid conditional, sometime there is a chance to hack the account by third party in regular user access way. With the widespread use of cloud emails and frequent reports on large-scale email leakage events, a security property so-called forward secrecy becomes desirable and indispensable for both individuals and cloud email service providers to strengthen the security of cloud email systems. However, due to the failure to meet the security and practicality requirements of email systems simultaneously. Which enables an email user to perform fine-grained revocation capacity.*

Keywords- Cryptography System, Cloud Mails, Encrypted

I. INTRODUCTION

Email 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 startups to deploy their own cloud email systems, which is 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.

II. LITERATURE REVIEW

Title: Ontological Detection of Phishing Emails

Author: Gilchan Park, Julia Rayz.

Year:7-10 Oct.2018

Description:

Detection of phishing emails is a topic that received a lot of attention both from academia and industry due to the devastating effects of phishing enabled data breaches have on private individual and companies. While the accuracy of phishing detection reported in the papers is impressive, the damage from the attacks continues to grow every year. One of the reasons is the diversity of attacks, especially within spear phishing and whaling. Another reason is that the natural language part of the detectors is usually devoid of semantics. In this paper we present an approach that adds semantics to highly accurate bag of words and part of speech approaches. We show that while the current approach is less accurate as a starting point, it retains its accuracy as a corpus deviates from training.

Title: Implementing PII honeytokens to mitigate against the threat of malicous insiders

Author: Jonathan White, Brajendra Panda.

Year: 8-11June 2009

Description:

In the past several years, extensive research has been performed in various honeypot technologies, including honey nets, honey walls, and honey tokens, primarily to gather information about external threats. Little to no research has been performed on how honey tokens, pieces of digital information designed to attract and trace illicit uses of data, can be implemented to catch one of the most dangerous threats, the trusted insider. The goal of this work is to detect, identify, and confirm insider threats, specifically threats that are after personally identifiable information (PII) data. These insiders are not after the physical system; they are after the information that these systems contain, which is often a significant threat. Malicious insiders are a threat because they are technically skilled, generally highly motivated, and insiders have access to extensive resources. For example, this

threat may be a disgruntled employee who wishes to sell information to an overseas competitor. Or, this threat could be a spy working for a foreign country to compromise national security. Examples of such spies include Robert Hansen, Aldrich Ames, and Anna Montes, all of whom caused extreme harm to their organizations over a long period of time without being detected.

Title: A Vision Based Three-Layer Access Management System with IoT Integration

Author: Nafize Ishtiaque Hossain, Ali Reza Galib, Raihan Bin Mofidul.

Year:19 December 2019

Description:

In developing countries, traditional access management systems ubiquitously use either keypad based password protection or radio frequency identification (RFID) card based protection. With the increased number of threats in recent years, these systems are becoming more vulnerable. If the password or the RFID card is somehow compromised, any unauthorized person can breach the system with ease. Considering and analyzing these issues, a cost-effective prototype of a vision based three-layer access management system with IoT connectivity was developed. In this paper, an access management system architecture is proposed based on the fusion of radio frequency identification, back propagation based face recognition and password protection. The system is also connected to a Node JS based web server. Whenever an access is granted or any unauthorized access is detected, an SMS and an email are sent to both the user and the system administrator.

Title: A Review of Computer Vision Methods in Network Security

Author: Jiawei Zhao, Rahat Masood, Suranga Seneviratne

Year: 04 June 2021

Description:

Network security has become an area of significant importance more than ever as highlighted by the eye-opening numbers of data breaches, attacks on critical malware/ransomware/cryptojacker attacks that are reported almost every day. Increasingly, we are relying on networked infrastructure and with the advent of IoT, billions of devices will be connected to the Internet, providing attackers with more opportunities to exploit. Traditional machine learning methods have been frequently used in the context of network security. However, such methods are more based on statistical features extracted from sources such as binaries, emails, and packet flows. On the other hand, recent years witnessed a phenomenal growth in computer vision mainly driven by the advances in the area of convolutional neural networks. At a glance, it is not trivial to see how computer vision methods are related to network security. Nonetheless, there is a significant amount of work that highlighted how methods from computer vision can be applied in network security for detecting attacks or building security solutions.

III. METHODOLOGY

The AES algorithm (also known as the Rijndael algorithm) is a symmetrical block cipher algorithm that takes plain text in blocks of 128 bits and converts them to cipher text using keys of 128, 192, and 256 bits. Since the AES algorithm is considered secure, it is in the worldwide standard

The AES algorithm uses a substitution-permutation, or SP network, with multiple rounds to produce cipher text. The number of rounds depends on the key size being used. A 128-bit key size dictates ten rounds, a 192-bit key size dictates 12 rounds, and a 256-bit key size has 14 rounds. Each of these rounds requires a round key, but since only one key is

inputted into the algorithm, this key needs to be expanded to get keys for each round, including round 0.

- Step 1 − In the step, the bytes of the block text are substituted based on rules dictated by predefined S-box.
- Step 2 − Next comes the permutation step. In this step, all rows except the first are shifted by one.
- Step 3 − In the third step, the Hill cipher is used to jumble up the message more by mixing the block's columns
- Step 4 − In the final step, the message is XORed with the respective round key

IV. MODULE DESCRIPTION

1. Register:

This is the first module in our project. The user update their essential detail to data base for login purpose.

2. Login:

This is module in our project, here symbolizes a unit of work performed within a database management system (or similar system) against a database, and treated in a coherent

and reliable way independent of other transactions. A transaction generally represents any change in database user will transfer the amount to provider.

3. Employee File-View:

In this module is used to help to the employee view the branch manager updated file. The file view form the data base.

4. Employee Request:

In this module the Employee will View the data file. And Request the Head-Office will be responsible for checking your file to Response.

5. Employee File-Download:

In this module the Employee will also download the data file fully analyzed data in category wise view. Employee will be responsible for your file stored in database.

6. Branch-Manager File-Upload:

In this module is used to help to the user to upload the file with the land longitude and the user will update the report along with their opinion and the will be stored the database.

7. Branch Manager File View:

In this module is used to help the manager upload file to the data base. Now the manager need to view his uploaded file. Then he will view the file.

8. Head-Office Request-View:

In this module is used to help to the Head-Office to view the user request to the database. It will show to the head office page.

9. Head-Office Response:

In this module the Head-Office will also view the data file. And analysis the Head-Office will be responsible for your file stored in database. Then head office response the user request

V. TESTING

The software, which has been developed, has to be tested to prove its validity. Testing is considered to be the least creative phase of the whole cycle of system design. In the real sense it is the phase, which helps to bring out the creativity of the other phases makes it shine.

• Various Levels Of Testing

1. White Box Testing
2. Unit Testing
3. Performance Testing
4. Output Testing
5. User Acceptance Testing

• White Box Testing

White-box testing, sometimes called glass-box, is a test case design method that uses the control structure of the procedural design to derive test cases. Using White Box testing methods, we can derive test cases that

• Unit Testing

Unit testing is a method by which individual units of source code, sets of one or more computer program modules together with associated control data, usage procedures, and operating procedures are tested to determine if they are fit for use. Intuitively, one can view a unit as the smallest testable part of an application. In procedural programming, a unit could be an entire module, but it is more commonly an individual function or procedure. In object- oriented programming, a unit is often an entire interface, such as a class, but could be an individual method. Unit tests are short code fragments created by programmers or occasionally by white box testers during the development process.

• Performance Testing

In general testing performed to determine how a system performs in terms of responsiveness and stability under a particular workload. It can also serve to investigate, measure, validate or verify other quality attributes of the system, such as scalability, reliability and resource usage. Performance testing is a subset of performance engineering, an emerging computer science practice which strives to build performance into the implementation, design and architecture of a system. It is also intended to test up to and beyond the bounds defined in the software/hardware requirements specification.

• Output Testing

After performing the validation testing, next step is output testing of the proposed system since no system could

be useful if it does not produce the required output generated or considered in to two ways. One is on screen and another is printed format. The output comes as the specified requirements by the user. Hence output testing does not result in any correction in the system.

• User Acceptance Testing

User acceptance of a system is the factor for the success of any system. The system under consideration is tested for the user acceptance by constantly keeping in touch with the prospective system users at the time of developing and making changes wherever required.

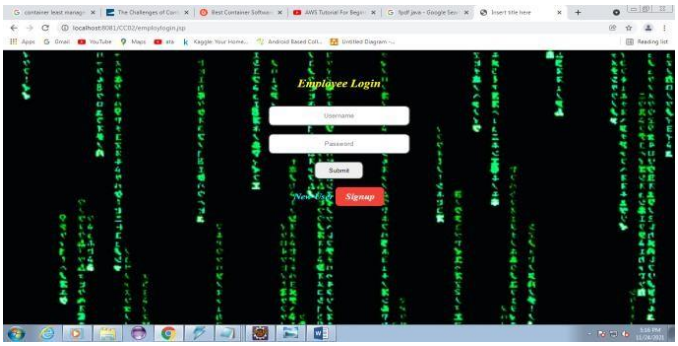
• Input screen design.

• Output screen design.

VI. RESULT

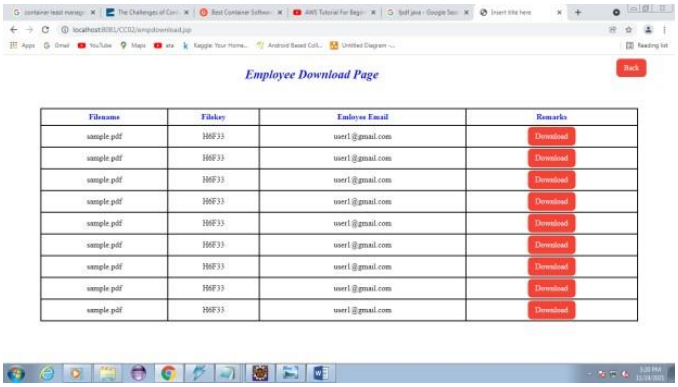
Home Page

Employee Login Page

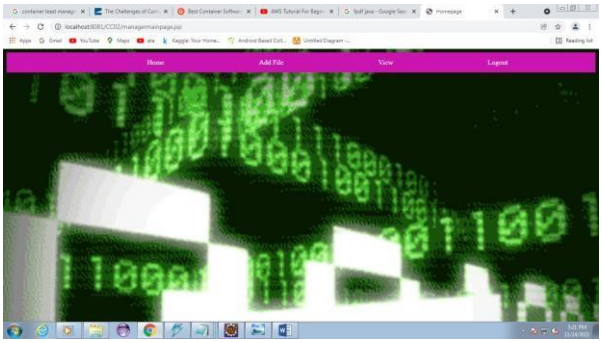


Employee-Register-Page

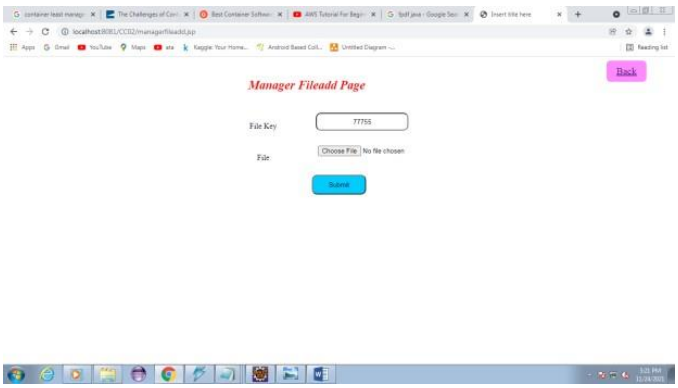
Employee Download Page



Branch-Manager Home Page



File Add Page



Admin Response Page

VII. FUTURE ENHANCEMENT

In future implementation will add some algorithm to implement the project very secure .And add some module or states to improve more options to implementation. Safe and Secure. Analysis the file request.

VIII. CONCLUSION

In this paper, to clutch pragmatic ahead secret of cloud email structures, we present another cryptographic rough named forward-pleasant puncturable conspicuous evidence generally based encryption plot, what segment never again need the assistance of PKIs and the synchronization of the email source and authority. More unequivocally, we at first formalize the sentence construction and prosperity conviction of AES, considering which we further gift a construction of encoded cloud email structures. Then, we present a significant improvement of AES plan to fire up the construction. Particularly, the proposed AES plot features of predictable length of cipher text, provable prosperity without subjective prophets and help of more than one cipher text marks. Also, to vanquish the unpreventable trouble of key-escrow in IBE and decay the estimation charge of end clients, we become the proposed AES plan to guide give up to-give up prosperity and once again appropriated unscrambling, independently. Finally, we do the proposed AES and present different preparation results to reveal its practicability In this paper, to clutch reasonable ahead secret of cloud email structures, we present another cryptographic unrefined named forward-pleasing puncturable ID basically based encryption plot, what segment never again need the assistance of PKIs and the synchronization of the email transporter and recipient. More unequivocally, we at first formalize the sentence design and security conviction of AES, considering which we further gift a design of encoded cloud email structures. Then, we present a significant improvement of AES plan to fire up the framework. Particularly, the proposed AES contrive features of steady length of cipher text, provable security without sporadic prophets and help of more than one cipher ext marks. Additionally, to conquer the certain trouble of key-escrow in IBE and decrease the computation cost of end clients, we stretch out the proposed AES plan to guide give up to-give up security and reexamined disentangling, independently. Finally, we execute the proposed AES and present different preparation results to reveal its practicability.

REFERENCES

[1] The Radicati Group Inc., "Cloud Email and Collaboration-Market Quadrant 2019," https://www.radicati.com/wp/wp-content/uploads/2019/ 03/Cloud-Email-and- Collaboration-Market-Quadrant-2019-Brochure. pdf, March 2019, accessed April 8, 2019.

[2] Tim Sadler, "The Year of Email Data Breaches," https://www.infosecurity magazine.com/opinions/2017-email-data-breaches/, January 2018, accessed September 11,2019.

[3] Wikileaks, "Hillary Clinton Email Archive," https://wikileaks.org/clinton-emails/, March 2016, accessed April 8, 2019.

[4] "The Podesta Emails," https://wikileaks.org/ podesta-emails/, March 2016, accessed April 8,2019.

[5] J. Callas, L. Don nerhacke, H. Finney, D. Shaw, and R. Thayer, "OpenPGP Message Format," https://tools.ietf.org/html/ rfc4880, November 2007, RFC 4880 (Proposed Standard