INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

www.ijprems.com
editor@ijprems.com

Vol. 03, Issue 04, April 2023, pp : 175-181

e-ISSN : 2583-1062

Impact Factor : 5.725

# ENABLING (END-TO-END) ENCRYPTED CLOUD EMAIL WITH PRACTICAL FORWARD SECRECY

**M.J. Shashidharan[1], S. Arun Raj[2], Ms. Sarika Jain[3], Dr. S. Geetha[4]**

[1]M.Sc – CFIS, Department of Computer Science and Engineering, Dr. M.G.R Educational and Research Institute, Chennai 600 095, Tamilnadu, India

[2,3]Center of Excellence in Digital Forensics, Perungudi, Chennai 600 089, Tamilnadu, India

[4]Head of the Department, Department of Computer Science and Engineering, Dr. M.G.R Educational and Research Institute, Chennai 600 095, Tamilnadu, India

## ABSTRACT

Encryption plays an important role in the communication of personal information today and will continue to play an important role in the future. Cryptographic applications provide the ability to securely transfer information to a robust compliant medium. Strengthen the security and capacity of communications and other data, enabling individuals, gatherings and institutions to restore personal protection. Online customers today need to register files and access locations. B. Online Education, Online Purchasing, Online Property Access, Facilitating Management, Informal Organizations, etc. Regardless of whether a professional cooperative or government individual has ensured the registration and login process with legal restrictions, it is possible that at some point an outsider may hack records through normal methods of customer access. I have. With the widespread adoption of cloud messaging and the constant reports of large-scale email breaches, both enterprises and cloud email specialists have come up against the assumptions of security to ensure cloud email security and harden their frameworks. Secrets become intriguing and indispensable. Regardless of this, the security and rationality requirements of an email framework cannot be met at the same time. This allows email clients to enforce fine-grained rejection limits.

**Keywords-** Email encryption, DES algorithm, encryption**.**

## 1. INTRODUCTION

Email has long been a popular means for people and businesses to communicate information and move data. Additionally, these small businesses and start-ups may now more easily create their own cloud email systems that are far more scalable and less expensive than conventional alternatives thanks to the development and commercialization of cloud computing. This increases the usage of email even further. According to The Radicating Group, by 2020 there will be more than 4 billion email subscribers worldwide and more than 306 billion daily business and consumer emails sent and received.

## 2. LITERATURE SURVEY

**Gilchan Park et.al,** 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 deviate from training, while the accuracy of the original approach decreases with the number of deviations.

**Jonathan White et.al,** 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.

**Nafize Ishtiaque Hossain et.al,** 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 analysing 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 basedweb 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.

**Jiawei Zhao et.al,** network security has become an area of significant importance more thanever as highlighted by the eye-opening numbers of data breaches, attacks on critical infrastructure, and malware/ransomware/crypto jacker attacks that are reported almostevery day. Increasingly, we are relying on networked infrastructure and with the adventof 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.

## 3. EXISTING SYSTEM

**Concept**

Protecting user or customer data is a key requirement for providing authorizedservices. I have many users or customers that I can access using their email id. Unless security procedures are in place, unknown users with valid credentials may gain access.

**Technique**

Fs-PIBE Algorithm.

**Disadvantage**

It is not stable for network level sharing data.

## 4. PROPOSING SYSTEM

**Concept**

Authentication methods primarily protect access to resources. After receiving the registration details, the service provider who wishes to provide authentication services to the user or customer depends on their wishes.

**Technique**

DES algorithm.

**Advantage**

It has standard procedure to share data for communication.

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

e-ISSN : 2583-1062

www.ijprems.com
editor@ijprems.com

Vol. 03, Issue 04, April 2023, pp : 175-181

Impact Factor : 5.725

## 5. ARCHITECTURE DIAGRAM

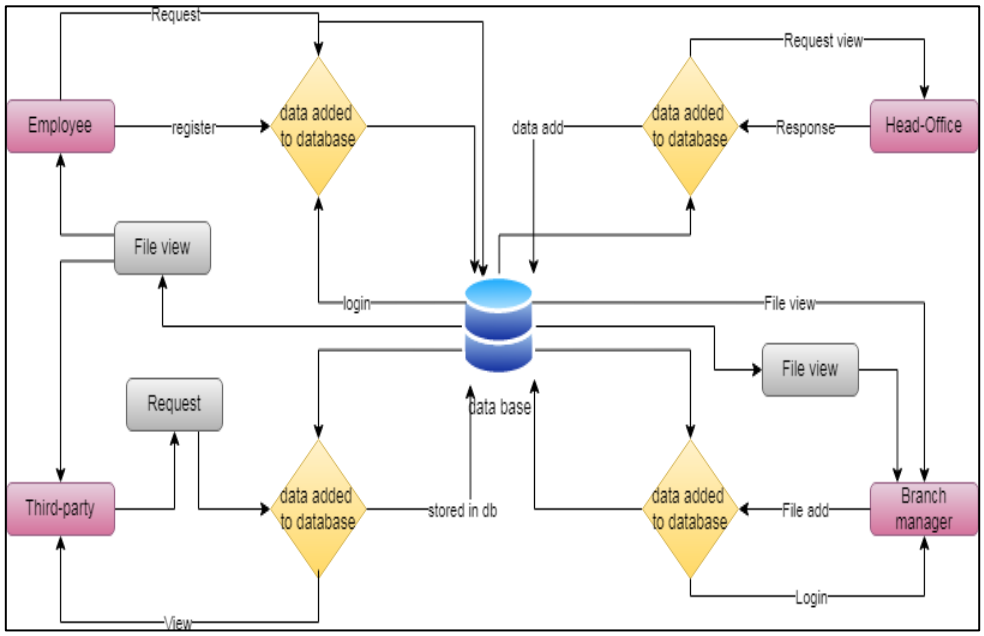


**Figure. 1 Architecture Diagram**

**List of Phases**

Register

This is the project's initial module. Important information in the login databaseis updated by the user.

Login

This module in our project represents a task carried out in a database management system (or a system comparable to it) against a database and handled in a reliable and cogent manner apart from other transactions. A transaction typically reflects anymodification to a database when a user transfers money to a supplier.

Employee File-View

Employees can examine the manager's updated files using this module. Adatabase is formed by file views.

Employee Request

Employees view data files in this module. Additionally, the head office is in charge of reviewing your file and confirming the reply.

Employee File-Download

Employees download completely analysed data files in categorised views inthis module. The database's files are the responsibility of the staff.

Branch-Manager File-Upload

The user may use this module to upload a file containing the country'slongitude, amend the report with their feedback, and then store it in the database.

Branch Manager File View

Managers can upload files to the database with the aid of this module. Themanager should now check out the uploaded document. He then turns to the file.

Head-Office Request-View

This module aids in the control panel's presentation of user database queries. It ispublished on the page for headquarters.

Head-Office Response

The data files for this module are also visible in Head Office. Analysing files kept in the database is another duty of Head Office. The centre responds to the user's inquiryafter that.

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

www.ijprems.com
editor@ijprems.com

Vol. 03, Issue 04, April 2023, pp : 175-181

e-ISSN : 2583-1062

Impact Factor : 5.725

**Screen Shots**

**Figure. 2 Homepage**

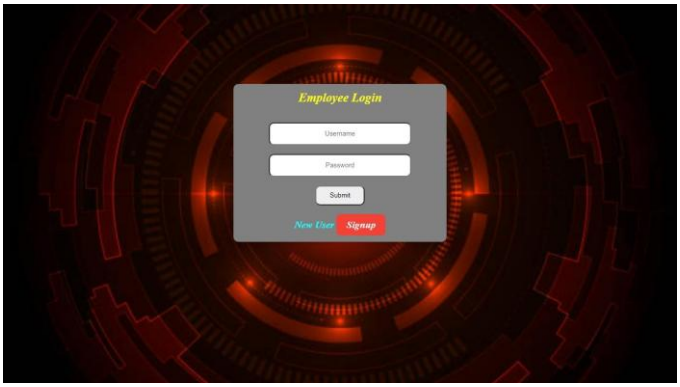


**Figure. 3 Homepage of Employee**

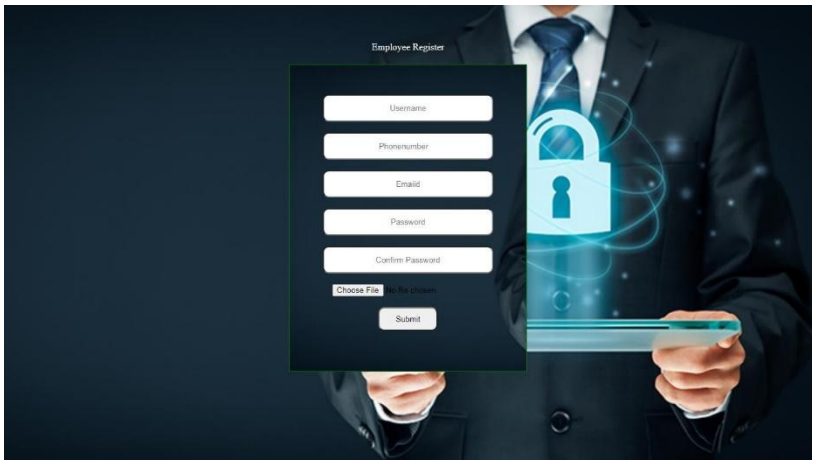


**Figure. 4 Employee Register Page**

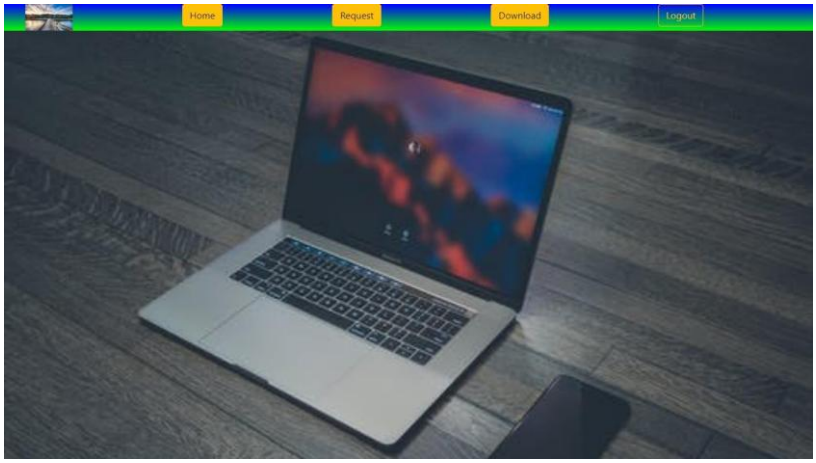


**Figure. 5 Employee Main Page**

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

www.ijprems.com
editor@ijprems.com

Vol. 03, Issue 04, April 2023, pp : 175-181

e-ISSN : 2583-1062

Impact Factor : 5.725


**Figure. 6 Employee Request Page**

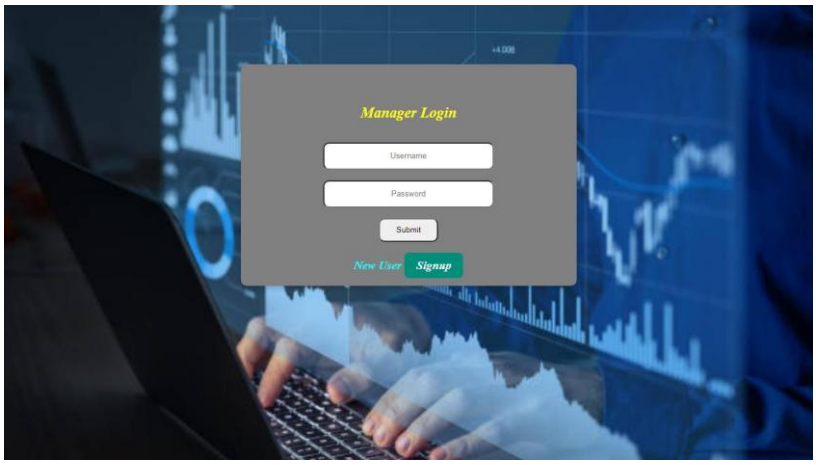


**Figure. 7 Manager Login Page**

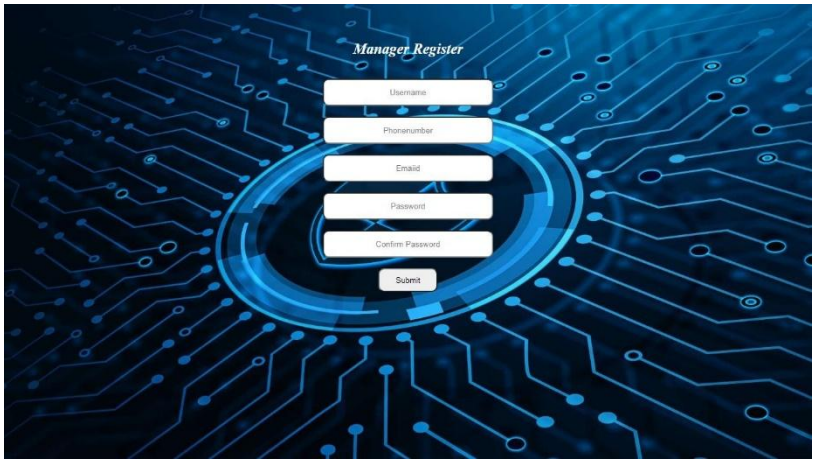


**Figure. 8 Manager Register Page**

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

www.ijprems.com
editor@ijprems.com

Vol. 03, Issue 04, April 2023, pp : 175-181

e-ISSN : 2583-1062

Impact Factor : 5.725

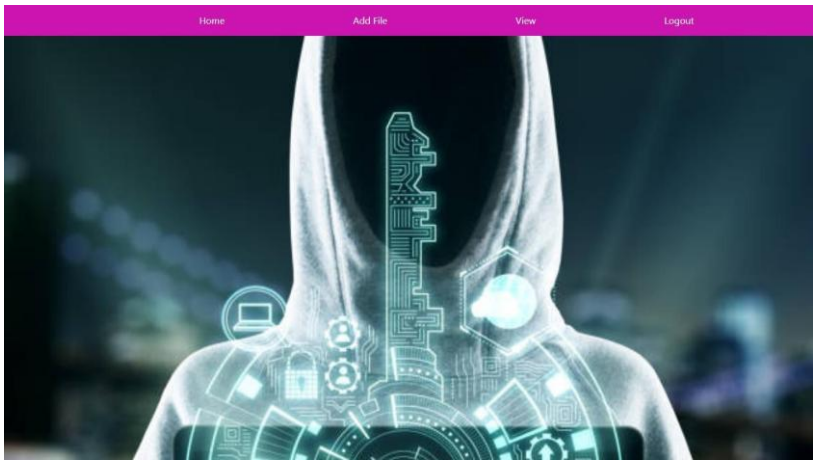


**Figure. 9 Head Office Homepage**

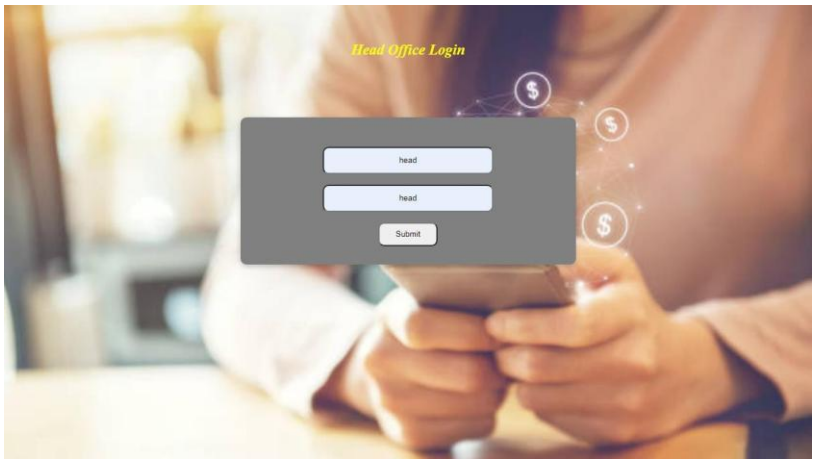


**Figure. 10 Head Office Login Page**

## 6. CONCLUSIONS

In this article, in order to grasp the actual security of messaging structures in the cloud, we present another cryptographic sketch called a clear and proven evidence- based cryptographic plot. exploitable, this shard never needs the help of a PKI nor a source synchronization and messaging authority. More clearly, we first formalize DES'ssentence structure and prosperity trust, as we also expose the structure of the encrypted messaging structure in the cloud. Then we present a significant improvement of the DES plan to kick off the build. In particular, the proposed DES plot has a predictable ciphertext length, provable prosperity without subjective oracles, and the aid of more than one ciphertext signature. In addition, to overcome the inevitable problem of primary escrow in IBE and reduce the estimated cost of end customers, we became the recommended DES plan to guide the abandonment of prosperity and one-time more suitable, independent decoding. Finally,we implement the proposed DES and present various preparatory results to show its feasibility., which the segment never needed PKI support and synchronization between the service provider and the e-mail recipient. More explicitly, we first formalize the DES security trust and sentence design, considering what we propose in addition to a cloud- encrypted messaging architecture design. Next, we present a significant improvementto the DES blueprint for framework launch. In particular, the proposed DES provides features of constant ciphertext length, provable security without sporadic oracles, and the help of more than one cipher extension. In addition, to overcome the key margin certainty issue in the IBE and reduce end-customer computational costs, we extend the proposed DES plan to guide the security waiver and reconsider solve problems independently. Finally, we run the proposed DES and present various preparatory results to show its feasibility.

## 7. 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.infosecuritymagazine.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. Donnerhacke, H. Finney, D. Shaw, and R. Thayer, "OpenPGP Message Format," https://tools.ietf.org/html/ rfc4880, November 2007, RFC 4880 (Proposed Standard).

[6] B. Ramsdell and S. Turner, "Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.2 Message Specification," https: //tools.ietf.org/html/rfc5751, January 2010, RFC 5751 (Proposed Standard).

[7] R. Abu-Salma, M. A. Sasse, J. Bonneau, A. Danilova, A. Naiakshina, and M. Smith, "Obstacles to the adoption of secure communication tools," in 2017 IEEE Symposium on Security and Privacy. IEEE, 2017, pp. 137–153.

[8] S. Ruoti, J. Andersen, D. Zappala, and K. Seamons. (2015) Why johnny still, still can't encrypt: Evaluating the usability of a modern pgp client. [Online]. Available: https://arxiv.org/pdf/ 1510.08555.pdf

[9] S. Sheng, L. Broderick, C. A. Koranda, and J. J. Hyland, "Why johnny still can't encrypt: evaluating the usability of email encryption software," in Symposium On Usable Privacy and Security, 2006, pp. 3–4.

[10] Shamir A, "Identity-based cryptosystems and signature schemes," in Advances inCryptology–CRYPTO 1984. Springer, 1984, pp. 47– 53.

[11] Roof point, "Proofpoint Email Protection," https://www. proofpoint.com/us/products/email-protection, 2005, accessed April 18, 2019.

[12] Data Motion, "Data Motion SecureMail," https://www.proofpoint. com/us/products/email-protection, 2013, accessed April 18, 2019.

[13] N. Unger, S. Dechand, J. Bonneau, S. Fahl, H. Perl, I. Goldberg, and M. Smith,"SoK: secure messaging," in 2015 IEEE Symposium on Security and Privacy. IEEE, 2015,pp. 232–249.

[14] H.-M. Sun, B.-T. Hsieh, and H.-J. Hwang, "Secure e-mail protocols providingperfect forward secrecy," IEEE Communications Letters, vol. 9, no. 1, pp. 58–60, 2005.

[15] J. O. Kwon, I. R. Jeong, and D. H. Lee, "A forward-secure e-mail protocol withoutcertificated public keys," Information Sciences, vol. 179, no. 24, pp. 4227–4231, 2009.