www.ijbar.org
ISSN 2249-3352 (P) 2278-0505 (E)
Cosmos Impact Factor-5.86

EMAIL SECURITY AND AUTHENTICATION

[1] Mrs. E. Pavithra, [2] Prakash Reddy. M, [3] Kiran. M, [4] Sai Kiran. M, [5] Siddarth Reddy. P
[1] Assistant Professor, [2345]B.Tech Students
Department Of Computer Science & Engineering
Sri Indu College Of Engineering & Technology,Sheriguda, Ibrahimpatnam

ABSTRACT

At present generation e-mail plays a prominent role. It is most used application for communication. We don't know whether receiver has seen it or not. To know whether mail send or not we proposed a system for message receipt facility.

One fundamental issue in today On-line Social Networks (OSNs) is to give users the ability to control the messages posted on their own private space to avoid that unwanted content is displayed. Up to now OSNs provide little support to this requirement. To fill the gap, in this paper, we propose a system allowing OSN users to have a direct control on the messages posted on their walls. This is achieved through a flexible rule-based system, that allows users to customize the filtering criteria to be applied to their walls, and a Machine Learning based soft classifier automatically labelling messages in support of content-based filtering.

I. INTRODUCTION

At present generation e-mail plays a prominent role. It is most used application for communication through which we can send text messages, documents, images and files. In present e-mail system we have only the facility of file sent notification. We don't know whether receiver has seen it or not. To know whether mail send or not we proposed a system for message receipt facility. At present generation e-mail plays a prominent ole. It s most used application for communication through hich we can send text messages, documents , images and files. In present e-mail system we have only the facility of file sent notification. Server supports remote access which enables senders, receivers and administrator can get the updates and send the notifications.

The following chapter would be Chapter 2, Literature Reviews which will describe the studies on existing systems, technologies needed and methodologies. Next would be Chapter 3, Requirement Specification which discusses about the functional and non- functional requirements. Following by Chapter 4, Design phase of the application which discusses about the required uml diagrams. Chapter 5 would be implementation details of the application, containing the sample code. Continue with Chapter 6, will be System Testing Details. Chapter 7 will be the Results of the execution and the next chapter would be Chapter 8 Conclusion and Future Scope followed by the bibliography.

II. LITERATURE SURVEY

Title: Authentication by Email Reception

Authors: Don Libes

Abstract:

This paper describes the use of email addresses as an authentication mechanism for public access servers. Intended for untrusted and low-risk environments, this mechanism provides reasonable security at very low cost to both user and server administrator. In particular, the initial and subsequent registrations are totally automated, and problem detection/resolution is highly automated. Keywords: security, authentication, email reception, email address Introduction In this paper, I describe the use of email reception as an authentication mechanism for public access servers, such as email- and Web- based servers in untrusted and low-risk environments [DoD]. Even the simplest implementation provides security that is significantly better than trust and requires significant power to crack. Despite its security limitations, this type of authentication should be attractive for a large percentage of servers that are now currently trust based. In particular, the system administration cost...

Title: A uniform approach for multilevel email security using image authentication, compression, OTP & cryptography

Authors: Apeksha Nemavarkar; Rajesh Kumar

Chakrawarti

Abstract:
Online email chronicles are an under-ensured yet greatly delicate data asset. Email documents can store year of individual and business email in a simple to-get to structure, one that is much less demanding to trade off than messages being transmitted on the wire. Most email files, be that as it may, are secured by reusable passwords that are frequently frail and can be effortlessly bargained. To secure such files, we propose novel multilevel email security building design. The proposed structural planning deals with three levels of security which are picture confirmation through example matching, pressure & cryptography in light of characteristic. At the starting levels our methodology is by all accounts at more elevated amount that the current ones. It is extraordinary that moderate mediums that course messages in the middle of sender and beneficiaries can be a genuine risk to security as these halfway can be effortlessly catch and messed with email messages numerous programming based arrangements has been proposed to tackle these issue, for example, it were created however these arrangements were sufficiently bad to give security and different assaults can meant to it and they can misuse the vulnerabilities of these administration 2 [2]. It is vital to forestall such phishing assaults. One of the approaches to keep the watchword burglary is to abstain from utilizing passwords and to confirm a client without a content secret key. This work proposes a safe confirmation administration construction modelling ISA-CC (Image Sequence Authentication Compression & Cryptography) that is picture based and wipes out the requirement for content passwords.

Title: A Secure Email System Based on Fingerprint Authentication Scheme

Authors: Zhe Wu; Jie Tian; Liang Li; Cai-ping Jiang; Xin Yang

Abstract:
Most of secure email systems adopt PKI and IBE encryption schemes to meet security demands in communications via emails, however, both PKI and IBE encryption schemes have their own shortcomings and flaws and consequently bring security problems to email systems. This paper proposes a new secure email system based on a fingerprint authentication scheme which combines fingerprint authentication technology with IBE scheme. The system perfectly solves the existing problems encountered in email security protection implementations.

Title: Secure Emails in XML Format Using Web Services

Authors: Lijun Liao; Jorg Schwenk

Abstract:
Cryptographically signed email has been widely used to provide the end-to-end authentication, integrity and non-repudiation. PGP mail and S/MIME have the significant drawback that the headers are unauthentic. DKIM protects specified headers, however, only between the sending server and the receiver. These lead to possible impersonation attacks and profiling of the email communication, and encourage spam and phishing activities. Furthermore, none of the currently available security mechanisms supports signature generation over partial email content by distinct signers, which might be useful in commercial scenarios. In order to handle these problems we suggest a new approach which can be considered as an advanced email security mechanism based on the popular XML technology. Our approach supersedes currently available email security standards in the sense of the higher flexibility and security, and can be transported via Web Services easily.

Title: Implementation of image based authentication to ensure the security of mail server

Authors: Abdul Rahim M; Anandhavalli D

Abstract:
Electronic communication is an emerging technique where we send information from sender to receiver in the form of E- Mail. To send and receive an Email, each user should have an ID. That ID must be locked with the unique password. The password is in the form of text. It may be alphabetical, numbers, alphanumerical and etc. Email servers provide the constraints to set the

www.ijbar.org
ISSN 2249-3352 (P) 2278-0505 (E)
Cosmos Impact Factor-5.86

passwords, for the users. Even most 3 of the servers secured, Black hat hackers hack the account and access the informations. A graphical password is an authentication system, that works by having the user select from images, in a specific order, presented in a graphical user interface(GUI). The most common computer authentication method is to use alphanumerical usernames and passwords. This method has been shown to have significant drawbacks. For example, user tends to pick a passwords that can be easily guessed. On the other hand, if a password is hard to guess, then it is often hard to remember.

III. SYSTEM ANALYSIS

EXISTING SYSTEM

In present e-mail system we have only the facility of file sent notification. But we don't know whether receiver has seen it or not. Because of this some important mails may get ignored by the receiver after seeing it also.

Disadvantages

- We have only the facility of file sent notification.
- The sender doesn't know whether user received the email or not.
- No acknowledgement

1.2. PROPOSED SYSTEM

Our proposal system for message receipt facility when it is seen by the recipient, so that sender is aware of the fact that his message has been read. This also displays the time and date when the receiver opens the mail.

Advantages

- Sender is aware of the fact that his message has been read.

This also displays the time and date when the receiver opens the mail

IV. IMPLEMENTATION

MODULES

- SENDER
- RECEIVER
- ADMIN

MODULE DESCRIPTION

SENDER

When it comes to email security and authentication in the sender module, it's all about ensuring that the emails you receive are actually from the sender they claim to be from. This helps in preventing email spoofing and phishing attacks.

The sender module typically involves implementing authentication protocols like SPF (Sender Policy Framework), DKIM (DomainKeys Identified Mail), and DMARC (Domain-based Message Authentication, Reporting, and Conformance). These protocols work together to verify the authenticity of the sender's domain and email address.

SPF allows the recipient's email server to check if the incoming email is sent from an authorized server for the sender's domain. DKIM adds a digital signature to the email to verify that it was not altered in transit and that it originated from the stated domain. DMARC complements SPF and DKIM by providing policies for how to handle emails that fail authentication checks.

By implementing these authentication mechanisms in the sender module, organizations can enhance email security, reduce the risk of email fraud, and protect both the sender's and recipient's email accounts from being compromised.

RECEIVER

1. SPF, DKIM, and DMARC Verification: The receiver module checks incoming emails against SPF, DKIM, and DMARC records to verify the authenticity of the sender. If an email fails these checks, it may be flagged as potentially fraudulent or suspicious.
2. Email Filtering: The receiver module uses filters to scan incoming emails for malicious content, attachments, or links. This helps in detecting and preventing phishing attempts, malware, and other email-based threats
3. Anti-Spam Measures: The receiver module employs anti-spam techniques to identify and filter out unsolicited or unwanted emails. This helps in reducing inbox clutter and minimizing the risk of falling victim to spam campaigns.
4. Encryption: Secure email protocols like TLS (Transport Layer Security) can be used in the receiver module to encrypt email communications between the sender and

www.ijbar.org
ISSN 2249-3352 (P) 2278-0505 (E)
Cosmos Impact Factor-5.86

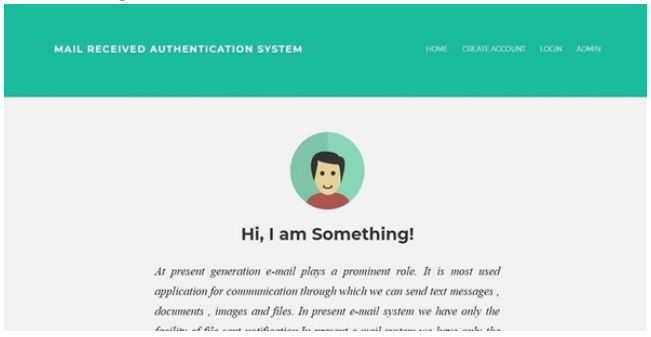
recipient, ensuring that sensitive information remains confidential.

ADMIN

1. Configuration of SPF, DKIM, and DMARC: The admin module involves setting up and managing SPF, DKIM, and DMARC records for the organization's email domains. This includes defining policies, monitoring authentication results, and adjusting settings as needed to enhance email security.
2. Monitoring and Reporting: Admins in the email security realm monitor authentication results, analyze email traffic patterns, and generate reports to identify any anomalies or potential security threats. This proactive approach helps in maintaining a secure email environment.
3. Security Policy Enforcement: Admins enforce security policies related to email authentication, encryption, anti-phishing measures, and spam filtering. They ensure that all security protocols are correctly implemented and adhered to across the organization.
4. Training and Awareness: Admins may also be responsible for conducting security awareness training for users to educate them about email security best practices, how to identify phishing attempts, and the importance of following security protocols.

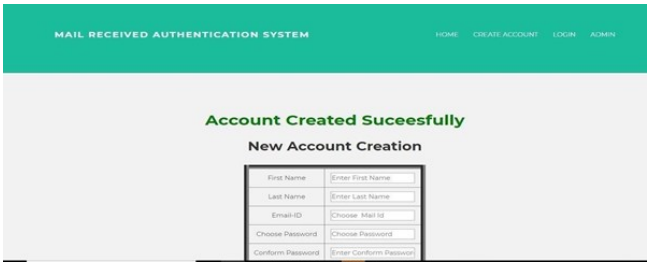
V. SCREENSHOTS

Home Page

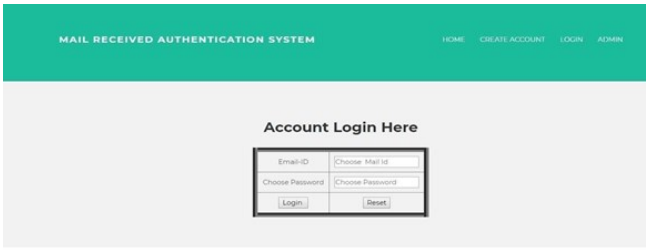


Registration Page

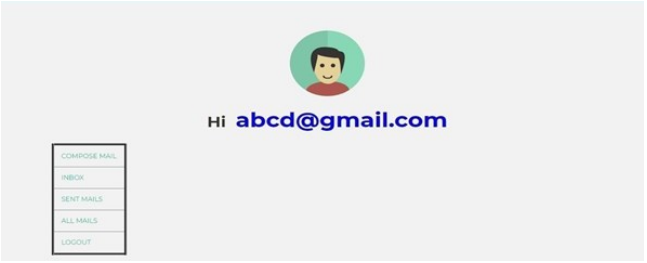
Registration Successful Page



Login Page

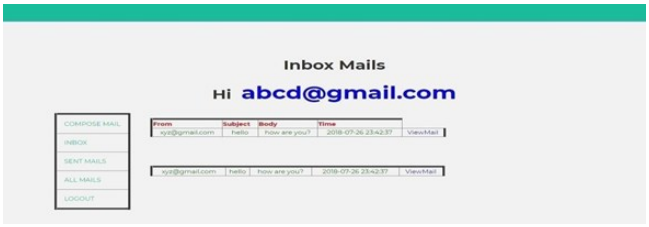


Index Page



Compose Mail Page

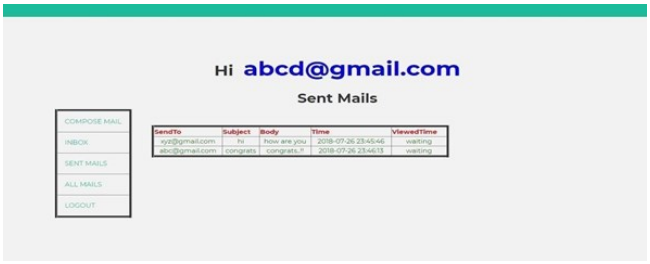
Inbox Mails



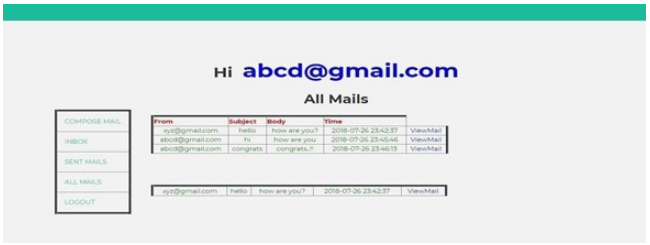
Checking Mails

www.ijbar.org
ISSN 2249-3352 (P) 2278-0505 (E)
Cosmos Impact Factor-5.86

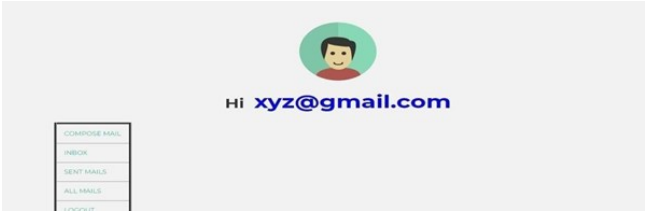
Sent Mails



All Mails

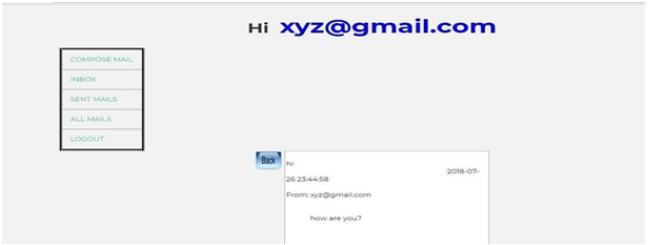


Receiver Home Page



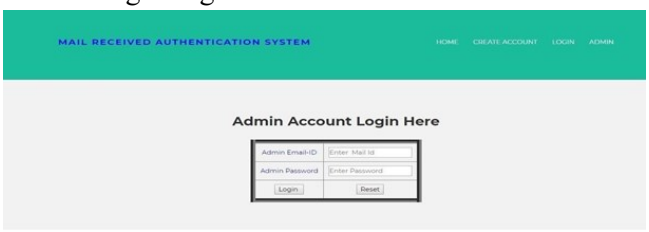
Checking Mails

Viewing Mails

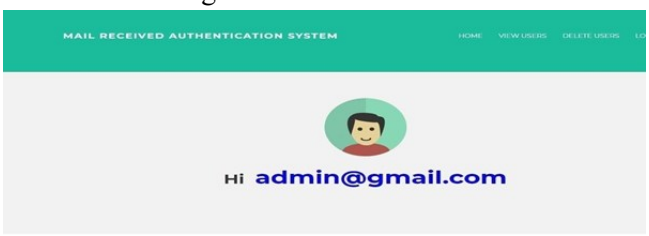


Acknowledgement

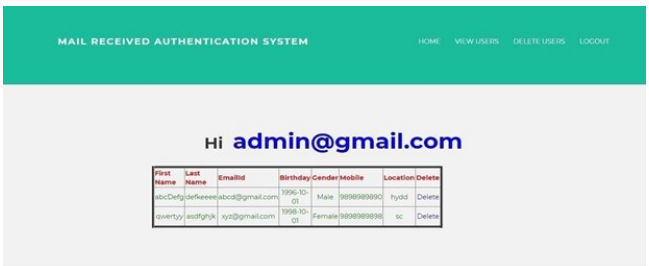
Admin Login Page



Admin Home Page



Delete Users Page



VI. CONCLUSION

CONCLUSION

The receiver and admin modules play crucial roles in ensuring the integrity, authenticity, and confidentiality of email communications.In the receiver module, the emphasis is on verifying incoming emails, filtering out malicious content, and implementing anti-spam measures to protect the recipient from potential threats.

On the other hand, the admin module focuses on

configuring and managing security protocols like SPF, DKIM, and DMARC, monitoring authentication results, enforcing security policies, and conducting training to enhance overall email security within the organization.

By effectively implementing measures in both modules, organizations can establish a robust email security framework that safeguards against phishing attacks, malware, spam, and other email-related risks.

FUTURE SCOPE

- Enhanced AI and Machine Learning: The integration of advanced AI and machine learning algorithms can help in better detecting and mitigating email-based threats like spear-phishing attacks and zero-day exploits.
- Zero Trust Security Model: The adoption of a Zero Trust security model for email systems can provide an added layer of protection by assuming that every access attempt is potentially risky. This approach verifies each user and device before granting access, reducing the risk of unauthorized access and data breaches.
- End-to-End Encryption: Future email security measures may focus on implementing end-to-end encryption to protect the confidentiality of email content throughout its entire journey, from sender to recipient. This ensures that only the intended recipient can decrypt and read the message.
- Biometric Authentication: Biometric authentication methods, such as fingerprint or facial recognition, may be integrated into email security systems to enhance user verification and prevent unauthorized access to email accounts.
- Blockchain Technology: The use of blockchain technology in email security can provide a tamper-proof and decentralized system for verifying the authenticity of emails and ensuring secure communication between parties.

REFERENCES

1. Komanduri, S., Mazurek, M. L., Shay, R and Kelley, P. G., "Guess Again (and Again and Again): Measuring Password Strength by Simulating Password-Cracking Algorithms" Security and Privacy (SP), IEEE Symposium, 2012.
2. Arunprakash, M., Gokul, T. R, "Network Security-Overcome Password Hacking Through Graphical Password Authentication", National Conference on Innovations in Emerging Technology 2011.
3. Palmer, e. e., "Ethical Hacking, " IBM Systems Journal VoI. 40, Issue. 3
4. Smith, B., Yurcik, W and Doss, D., "Ethical Hacking: The security Justification Redux", Technology and Society, (1ST AS'02), International Symposium 2012.
5. Surabhi Anand, Priya Jain, Nitin and Ravi Rastogi., "Security, Analysis and Implementation of 3-Level Security System using Image Based Authentication", 4tl' International Conference on Modeling and Simulation", 2012.
6. Zuo, Y and Panda, B., "Network viruses: their working principles and marriages with hacking programs", Infonnation Assurance Workshop, IEEE Systems, Man and Cybernetics Society, 2013.
7. Putri Ratna., Anak Agung Dewi., Purnamasari., Prima., Shaugi., Ahmad., Salman and Muhammad., "Analysis and comparison of MD5 and SHA-I algorithm implementation in Simple-O authentication based security system", QiR (Quality in Research) International Conference on 2013
8. Sai Sathish, Srinivasa Rao K., Aditya Gupta, Hacking Secrets, 2012, pp. 8 -26.
9. Ankit Fadia, Email Hacking: Even You can Hack, Vikas Publishers, 2012, pp. 77-89.
10. William Stallings, Cryptography and Network Security, Pearson Prentice Hall, 2009, pp. 317-346.