GR JOURNALS

Journal of Information and Communications Technology: Algorithms, Systems and Applications

Research Article | *Open Access* | 🅭🅯🄏

Email Security Using Email Aliasing

Vijaykumar Bidve,[1] Kiran Kakade,[2] Rahul H. Bhole[3] and Mohd Shafi Pathan[4,*]

[1] *School of Computer Science and Information Technology, Symbiosis Skills and Professional University, Pune, Maharashtra, 412101, India*
[2] *Faculty of Management, Symbiosis Institute of Management Studies (SIMS), Symbiosis International (Deemed University), Pune, Maharashtra, 412115, India*
[3] *Department of Information Technology, School of Computing, MIT Art Design and Technology University, Pune, Maharashtra, 412201, India*
[4] *Department of Computer Science and Information Technology, MIT Art Design and Technology University, Pune, Maharashtra, 412201, India*
**Email:* shafi.pathan@mituniversity.edu.in (S. Pathan)

Abstract

E-mail has become a vital tool for communication in the digital era. But it's becoming more and harder to manage emails effectively while maintaining security due to the increase in online dangers and email traffic. One possible way to overcome these difficulties is via email aliasing, which involves setting up several email accounts that forward messages to a central mailbox. Generating many email names for a single mailbox, or email aliasing, has several advantages, such as increased security, better workflow, and effective communication. An in-depth discussion of email aliasing's features, advantages, potential security risks, and implementation methods is presented through this work. This article aims to provide helpful information to people and businesses looking to improve email management procedures by clarifying how email aliasing contributes to increased email security and efficiency.

Keywords: Email security; Spam prevention; Phishing mitigation; Alias management systems; Privacy protection.

Received: 20 May 2025; Revised: 18 June 2025; Accepted: 23 June 2025; Published Online: 24 June 2025.

1. Introduction

Email communication has become indispensable in personal and professional domains, serving as a cornerstone of digital interaction. However, the surge in email usage has been paralleled by escalating concerns over security vulnerabilities, privacy breaches, and the overwhelming influx of messages, necessitating innovative solutions for effective email management.[1,2] Email aliasing emerges as a pivotal strategy in this context, offering a robust mechanism to enhance security, streamline workflows, and safeguard user privacy.[3,4] By enabling the creation of multiple email aliases linked to a single mailbox, this approach facilitates the efficient management of diverse communication channels while mitigating risks associated with spam, phishing, and unauthorized access.[5] The evolution of email aliasing underscores its transformative potential in addressing modern email challenges. Initially conceived as a rudimentary tool for customizing email identities, aliasing has evolved into a sophisticated framework integrated with advanced email systems.[6] Contemporary implementations leverage cutting-edge technologies such as Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM), and Domain-based Message Authentication, Reporting, and Conformance (DMARC) to fortify authentication and minimize spoofing threats. Additionally, the incorporation of single sign-on (SSO) and identity management systems

DOI: https://doi.org/10.64189/ict.25306

exemplifies the versatility of email aliasing in corporate environments, enabling centralized control over access and communication protocols.[7,8] This research delves into the multifaceted dimensions of email aliasing, encompassing its conceptual underpinnings, technical implementations, and practical applications. It explores the diverse types of aliases—personal, role-based, generic, and disposable—and their utility in optimizing email workflows and ensuring privacy.[9] The study further examines the integration of aliasing with server-side configurations, client-side tools, and third-party services, highlighting their strengths and limitations. By addressing critical security considerations and proposing best practices for alias management, the research aims to equip users and organizations with actionable insights to harness the full potential of email aliasing.[10] Email aliasing is a testament to communication systems' adaptability in an era characterized by rapid technological advancements and growing cyber threats. Its capacity to enhance privacy, bolster security, and facilitate organized communication positions it as a vital tool for navigating the complexities of the digital age.[11] This paper seeks to contribute to the discourse on email management by elucidating the strategic advantages of aliasing and proposing innovative approaches for its effective implementation.

The evolution of email aliasing reflects the dynamic nature of email communication and its adaptation to address emerging privacy, efficiency, and security challenges. Initially, email systems provided users a static email address tied to their account credentials.[12] However, as email became an integral tool for personal and professional communication, users encountered challenges in managing increasing volumes of messages, distinguishing between different lines of communication, and safeguarding their privacy. These limitations prompted the development of alias-based systems, which allowed users to create additional email addresses, or aliases, that forwarded messages to a primary inbox.[13,14] Early implementations of email aliasing were rudimentary, requiring manual configuration via server-side settings or email client interfaces. Despite these initial complexities, the utility of aliases in streamlining communication and enhancing privacy led to their growing adoption.[15] As email services matured, providers integrated more sophisticated aliasing features into their platforms, making the process accessible even to users with limited technical expertise. Modern email systems offer intuitive interfaces and tools for alias creation, management, and customization, enabling users to adapt email communication to diverse organizational and individual needs. These advancements have been complemented by technological innovations that enhance the functionality and security of email aliasing. Protocols such as Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM), and Domain-based Message Authentication, Reporting, and Conformance (DMARC) have bolstered the authentication and verification of email aliases, mitigating the risks of spoofing and phishing attacks. Integrating email aliasing with identity management systems and single sign-on (SSO) solutions has expanded its utility, particularly in corporate environments.[16,17] Centralized management of aliases and authentication processes enables organizations to streamline user provisioning, enforce security protocols, and maintain control over access to digital resources. Additionally, the scalability of aliasing allows businesses to adapt to dynamic communication needs, such as managing temporary projects or facilitating customer interactions through role-based or disposable aliases.[18] The evolution of email aliasing underscores its critical role in modern email management. By addressing key challenges such as privacy protection, organizational efficiency, and security enhancement, email aliasing has transitioned from a niche feature to a fundamental component of digital communication. As advancements in email technologies continue, the potential applications and benefits of aliasing are poised to expand, reinforcing its significance in a rapidly evolving digital landscape.[19]

The integration of email aliasing into contemporary communication systems addresses the growing need for secure, efficient, and centralized email management. Email aliasing involves creating virtual identities or aliases that forward all correspondence to a single primary mailbox, enabling users to streamline communication while safeguarding privacy.[20] This approach enhances organizational efficiency by consolidating multiple communication channels into one inbox and strengthens security protocols. By isolating email interactions through distinct aliases, users mitigate risks associated with spam, phishing, and unauthorized access. Additionally, advanced email technologies, such as Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM), and Domain-based Message Authentication, Reporting, and Conformance (DMARC), further secure email aliasing by authenticating sender identities and reducing spoofing attempts.[21] The method of alias creation, whether through server-side configurations, client-side management, or third-party services, offers flexibility tailored to diverse user requirements. Furthermore, the use of disposable aliases for temporary purposes, such as online registrations, exemplifies the adaptability of email aliasing in preserving privacy. As demonstrated in practical implementations, email aliasing simplifies workflows and promotes privacy and resource optimization, making it a critical tool for modern communication in personal and professional contexts.[22]

The types of Email aliases are as mentioned subsequently. Personal Aliases: Personalized email addresses for private correspondence, such as firstname.lastname@example.com or nickname@example.com, are often created using these aliases. Role-based Aliases: These aliases, which include sales@example.com, support@example.com, and info@example.com, are intended to stand out for certain business positions or responsibilities. These aliases simplify departmental cooperation and communication channels. Generic Aliases: These catch-all or generic email addresses, such as contact@example.com or feedback@example.com, are used to receive messages about general questions, comments, or subscriptions but are not associated with any particular person. Disposable Aliases: Users may instantly generate disposable aliases, short-lived or one-time use addresses, to sign up for online services, engage in forums, or communicate with strangers. These aliases reduce spam and protect privacy.[23]

Email aliasing is implemented using various techniques as mentioned subsequently. Server-side Alias Configuration: Users may create and modify aliases using administrative controls or configuration files with this approach. Aliases are handled and configured at the email server level. Although server-side aliasing offers centralized administration and control over alias settings, its setup and upkeep may require technical know-how. Client-side Alias Management: A few email clients and programs have built-in tools to create and manage aliases from the user interface. Convenience and accessibility may be improved by users organizing aliases into groups or categories, creating aliases, and specifying forwarding rules. Third-party Alias Services: Several third-party email systems and services are experts at supplying aliasing features as a part of their service packages. To meet the requirements and preferences of specific users, these services may include additional capabilities like alias masking, alias rotation, and domain customization.[24]

2. Methodology

2.1 Literature review

Traditional email-based notifications have low delivery rates and are prone to distrust and spam filtering. Postal letters offer better remediation rates, but detailed descriptions of vulnerabilities can be mixed. Manual intervention and user engagement tools can help mitigate limitations, but higher operational costs are required.[25] A hybrid notification strategy, combining diverse communication methods, personalized messaging, and accessible remediation support, can improve response rates and security outcomes.[26] The document introduces a new method for enhancing the security of educational email services, particularly during the COVID-19 pandemic. The method uses a deep attention collaborative mechanism to detect and categorize spam emails, modeling spam as a social graph. It uses nonnegative matrix factorization and exponential random graph models to identify overlapping user communities and local dependencies. The method's superiority is demonstrated in sparse datasets typical of educational environments. Future research should explore complex network features and optimize computational efficiency with advanced hardware.[27] CyberDART is a federated system designed to combat email threats collaboratively. It uses a modular architecture with machine learning and advanced algorithms like PATCH for pseudonymous text analysis, enhancing detection and response to spam and phishing. The system uses real-time threat detection, secure data exchange, and adaptive learning to ensure scalability and adaptability to evolving cyber threats. It operates through hierarchical nodes, with local nodes performing initial analysis and central nodes aggregating data to detect invisible patterns. CyberDART achieves higher accuracy in identifying threats and maintains low false positives. It also emphasizes security and trust through configurable federation policies, allowing organizations with varying risk tolerances and operational needs to collaborate effectively. Based on the situational crime prevention framework, the document presents a sequential schema model for preventing and mitigating phishing emails. Key prevention strategies include limiting personal information availability, implementing robust email filtering systems, and conducting regular cybersecurity training. Email security is also discussed, focusing on techniques like digital signatures, encryption protocols, and hashing algorithms to protect sensitive information.[28] The document examines phishing email attacks and their mitigation measures within the situational crime prevention (SCP) approach. It highlights the persistent threat of phishing emails, which exploit human and environmental vulnerabilities to compromise sensitive information and disrupt operations. The paper highlights the increasing sophistication of phishing campaigns, particularly during global crises like the COVID-19 pandemic. A sequential schema model is introduced to address these attacks, integrating cybersecurity tools like email filters and multifactor authentication with situational crime prevention techniques. It emphasizes the importance of human-centric approaches, such as employee training and awareness campaigns, to promote vigilance and accountability. The model also explores emerging technologies like machine learning for phishing detection and response.[29] Phishing is a social engineering attack that exploits human vulnerabilities and technical weaknesses to deceive individuals into revealing sensitive information. The study categorizes phishing into phases, including planning, preparation, execution, and valuables acquisition. Attackers use psychological triggers like urgency, fear, and trust to exploit victims. The study identifies various attack vectors, including malware-based methods, DNS spoofing, and man-in-the-middle tactics. The research calls for a dual approach, combining technical solutions with user-centric strategies. It calls for robust security systems, regular user training, and interdisciplinary collaboration to address both technical and human factors in phishing.[30] Technology-centric systems use advanced methods like machine learning and neural networks to detect and prevent phishing attempts, targeting specific attack vectors like email and websites. However, these systems often have limitations in accuracy, especially against zero-day attacks. Human-centric approaches emphasize user awareness and behavioral modification, using training programs, gamification, and educational initiatives. The study also highlights gaps in addressing diverse literacy levels and evolving attack vectors. It calls for a holistic security culture, integrating organizational policies with individual education, and addressing the limitations of machine learning. The findings highlight the need for adaptable, multi-faceted solutions to combat phishing threats.[31] A study analyzing over 25 million emails from the Australian Spam Intelligence Database reveals that malware-laden spam is prevalent, with around 10% of URLs linked to malicious sites and 31.4% of attachments compromised. Trojans and ransomware are the dominant malware types in these attachments. The study also highlights the evolving techniques used by cybercriminals, such as URL shortening services and deceptive file naming. It also highlights significant temporal fluctuations in spam activity, suggesting targeted campaigns with specific malware payloads. The study criticizes the reactive nature of current detection methods and advocates for a multidimensional approach that integrates machine learning-based detection with proactive crime prevention strategies. It also stresses the need for collaboration between government agencies, private sectors, and academic institutions to enhance cybersecurity resilience.[32] Email is a critical target for cyber threats, with risks such as phishing, spoofing, spamming, malware distribution, and email bombing. Protocols like SMTP, POP, and IMAP rely on unencrypted communications, allowing eavesdropping and unauthorized access. Digital forensics has emerged as a vital discipline to mitigate these risks. While encryption mechanisms like S/MIME and PGP protect email content, they are inadequate against man-in-the-middle attacks and signature repudiation. Complementary strategies like digital signatures, hashing algorithms, and multi-factor authentication are essential for data authenticity.[33] Forensic tools like metadata analysis, keyword searches, and IP tracking are crucial for identifying and mitigating email-based threats. Advanced capabilities like offline analysis, email clustering, and visualization are needed. A collaborative approach combining technical innovation, organizational policies, and user education is needed to foster a secure and resilient email communication environment.[34]

2.2 Gap analysis of literature review

Email security and management strategies have improved, but gaps remain in addressing cyber threats and user-centric challenges. Traditional methods like email-based systems have low delivery rates and are susceptible to spam filters. Current technical solutions, like machine learning-based detection systems, have limitations in accuracy against zero-day threats. Human-centric approaches fail to address varying literacy levels and the rapid adaptation of attackers to new technologies. Emerging methodologies like deep attention collaborative mechanisms and federated systems like CyberDart promise to enhance threat detection and response, but computational efficiency, scalability, and user accessibility remain critical challenges. Hybrid strategies combining diverse communication methods, personalized messaging, and enhanced remediation support are underexplored. Interdisciplinary research is needed to merge technical solutions with behavioural interventions. Future studies should prioritize scalability and usability of these solutions to foster a resilient email ecosystem.

2.3 Methodology

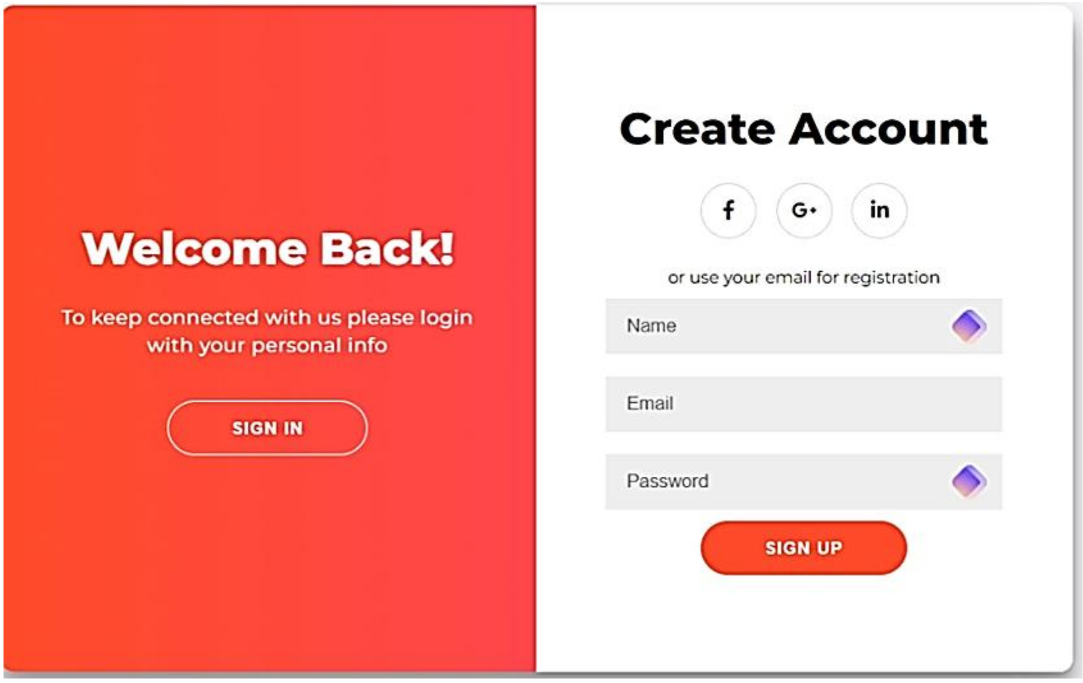
In this work a Python-based approach is employed to automate the generation and management of email aliases, ensuring efficiency in deployment and execution. The process commenced with user input for the primary email address and the desired number of aliases. The script then systematically generated these aliases, which serve as unique identifiers for account creation and communication on various platforms. This automation facilitates privacy by enabling users to segregate their interactions and maintain organized email management. To validate functionality, the script incorporated a mechanism to utilize the generated aliases for account signups across specified services. Emails directed to these aliases were automatically forwarded to the user's primary inbox, consolidating communications while preserving ease of access. This forwarding mechanism was verified using the Simple Mail Transfer Protocol (SMTP), ensuring robust delivery and receipt of messages. Thorough testing was conducted to confirm the reliability of alias creation, forwarding, and SMTP configurations. The process guarantees that emails forwarded from aliases are consistently received, ensuring seamless communication. By automating these tasks, the method significantly enhances email management, privacy, and operational efficiency. This approach offers a scalable and secure solution for handling multiple accounts, streamlining workflows, and mitigating risks associated with email-based interactions. The technical aspects of the implementation of this work as explained below.

2.3.1 Implementation details

Aliases are generated using Python’s random module to create unique strings like e.g. abc123@mail.com. Aliases follows a predefined structure based on the user's input i.e. user+tag@domain.com, leveraging Gmail and Outlook's aliasing format. Some aliases incorporated timestamps to prevent duplication i.e. user_20250128@mail.com. Simple Mail Transfer Protocol (SMTP) handshake verification is used to check status of alias received messages. Test email messages are sent to each alias, and receipt confirmation is logged. Email servers’ response codes are analyzed to determine alias functionality. Aliases are linked to primary inboxes to confirm that messages are successfully redirected. Sender Policy Framework (SPF) is used to prevent spoofing by verifying that emails are sent from authorized mail servers. Domain Keys Identified Mail (DKIM) used to ensures message integrity by adding digital signatures to outgoing emails. Domain-based Message Authentication, Reporting & Conformance (DMARC) is used to enforces policies based on SPF/DKIM results and prevents unauthorized domain use. Transport Layer Security (TLS) is used for encryption of emails in transit between mail servers and Secure Sockets Layer (SSL) is used email clients to encrypt communication channels. Gmail and Outlook allow alias management via native settings. Webmail Interfaces provides an intuitive way to switch between aliases while composing emails. In short, aliases are tested, validated and secured using above mentioned techniques.

2.3.2 Flow of working environment

1. Open Website
2. Register Account
3. Login
4. Input Email Address for Primary Address
5. Enter the Number of Alisas to generate
6. Generate Aliasis
7. Copy the Aliasis to Use
8. The Aliasis in use are saved
9. Click history to show previous Aliasis
10. Logout



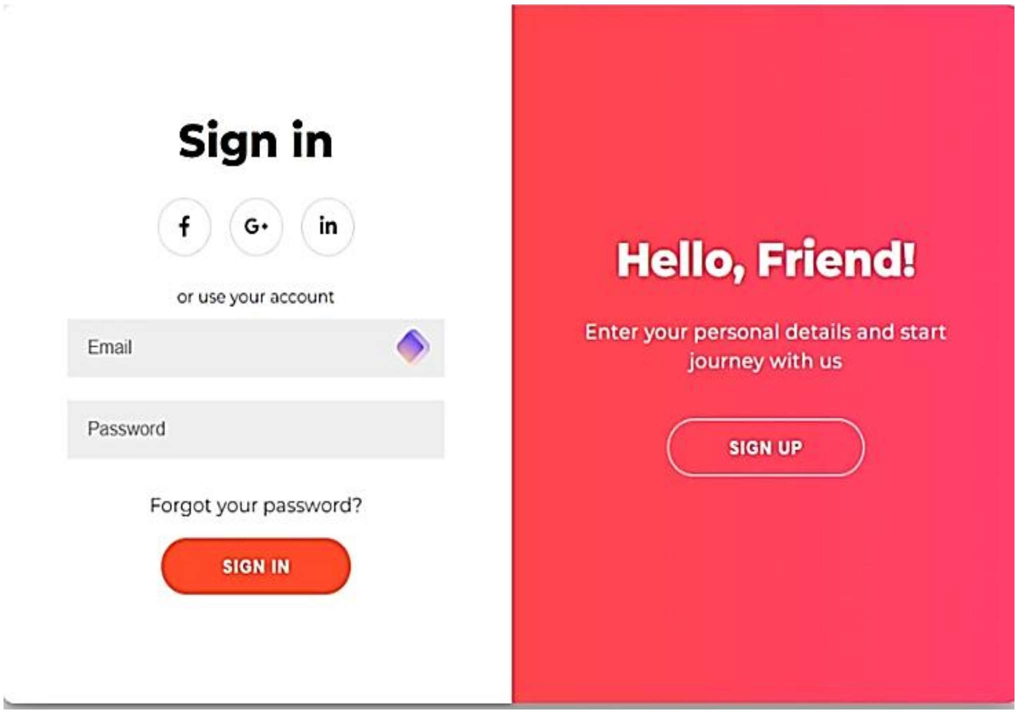
Welcome Back!

To keep connected with us please login with your personal info

Create Account

or use your email for registration

Fig. 1: Register account.



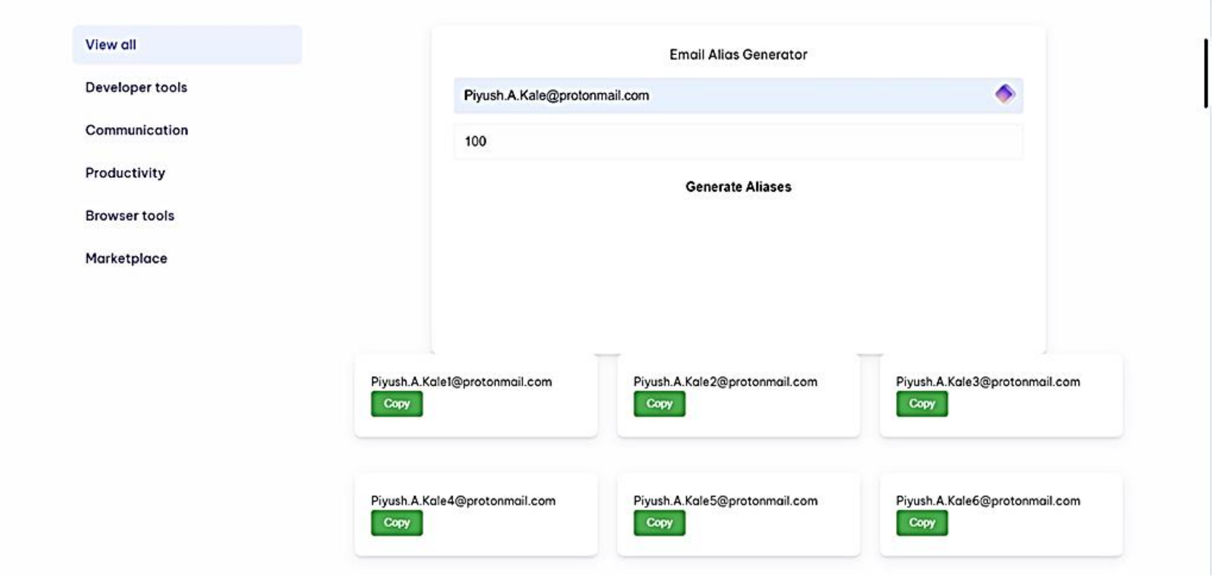
Sign in

or use your account

Hello, Friend!

Enter your personal details and start journey with us

Fig. 2: Login into account.



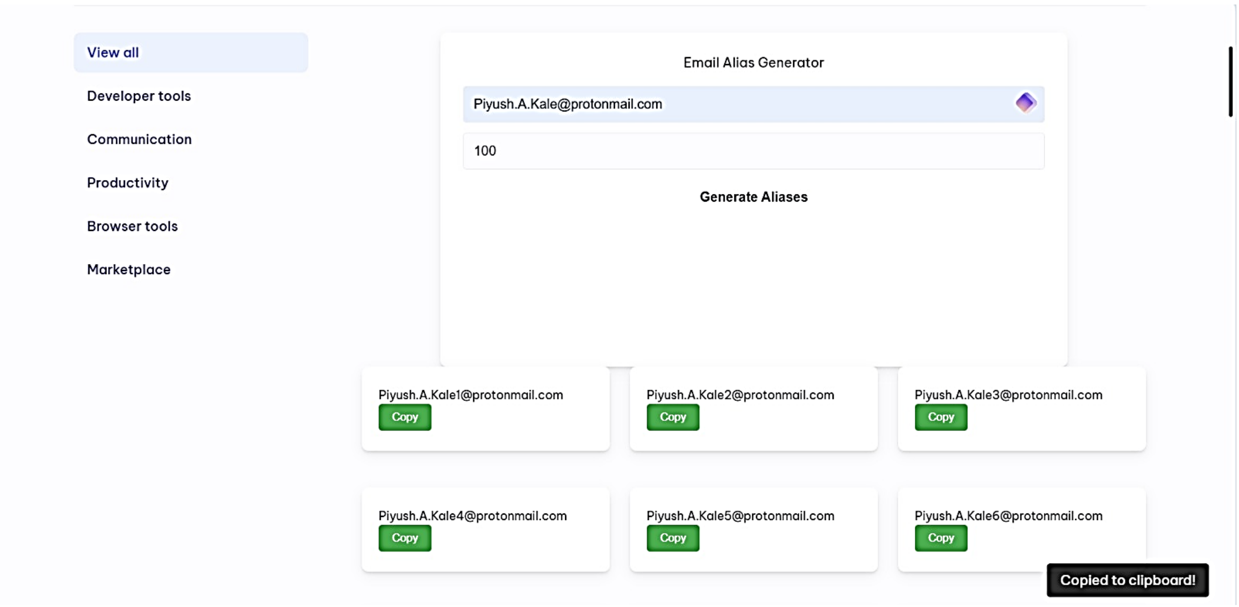
Email Alias Generator

Piyush.A.Kale@protonmail.com

100

Piyush.A.Kale1@protonmail.com
Piyush.A.Kale2@protonmail.com
Piyush.A.Kale3@protonmail.com
Piyush.A.Kale4@protonmail.com
Piyush.A.Kale5@protonmail.com
Piyush.A.Kale6@protonmail.com

Fig. 3: Creating of email aliases.



Email Alias Generator

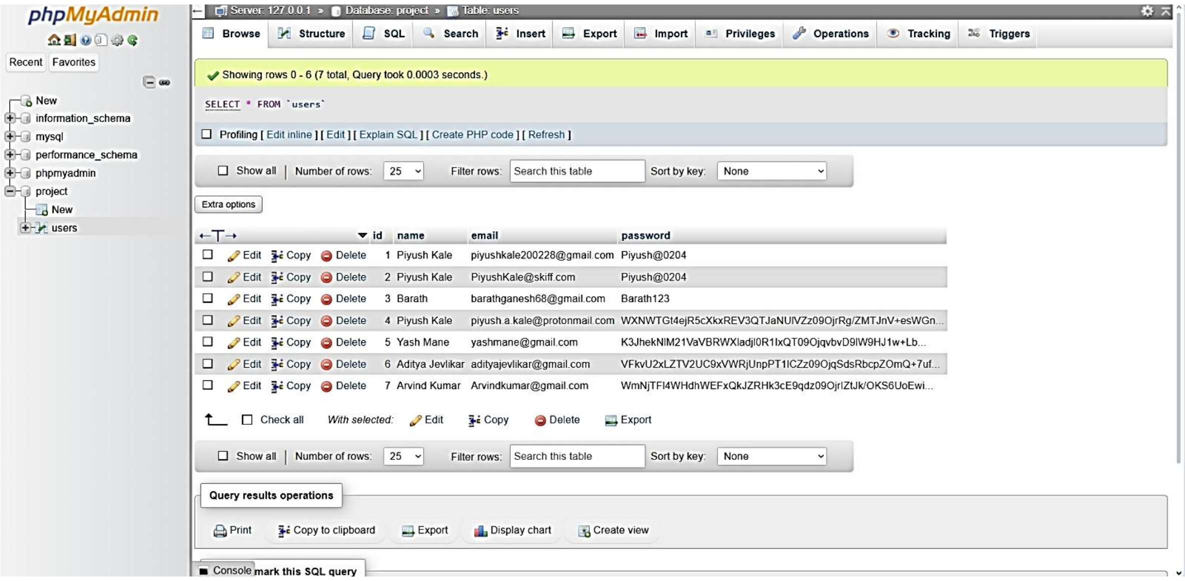
Piyush.A.Kale@protonmail.com

100

Piyush.A.Kale1@protonmail.com
Piyush.A.Kale2@protonmail.com
Piyush.A.Kale3@protonmail.com
Piyush.A.Kale4@protonmail.com
Piyush.A.Kale5@protonmail.com
Piyush.A.Kale6@protonmail.com

Copied to clipboard!

Fig. 4: Copying email aliases to use.



Server: 127.0.0.1 » Database: project » Table: users

✓ Showing rows 0 - 6 (7 total, Query took 0.0003 seconds.)

```
SELECT * FROM `users`
```

□ Show all | Number of rows: 25 Filter rows: Search this table Sort by key: None

	id	name	email	password
□ Edit Copy Delete	1	Piyush Kale	piyushkale200228@gmail.com	Piyush@0204
□ Edit Copy Delete	2	Piyush Kale	PiyushKale@skiff.com	Piyush@0204
□ Edit Copy Delete	3	Barath	barathganesh68@gmail.com	Barath123
□ Edit Copy Delete	4	Piyush Kale	piyush.a.kale@protonmail.com	WXNWTGt4ejR5cXkxREV3QTJaNUlVZz09OjrRg/ZMTJnV+esWGn...
□ Edit Copy Delete	5	Yash Mane	yashmane@gmail.com	K3JhekNIM21VaVBRWXladjl0R1IxQT09OjqvbvD9lW9HJ1w+Lb...
□ Edit Copy Delete	6	Aditya Jevlikar	adityajevlikar@gmail.com	VFkvU2xLZTV2UC9xVWRjUnpPT1lCZz09OjqSdsRbcpZOmQ+7uf...
□ Edit Copy Delete	7	Arvind Kumar	Arvindkumar@gmail.com	WmNjTFl4WHdhWEFxQkJZRHk3cE9qdz09OjrlZtJk/OKS6UoEwi...

□ Show all | Number of rows: 25 Filter rows: Search this table Sort by key: None

Fig. 5: Password encryption.

3. Results and discussion

Email aliasing offers numerous practical applications, enhancing privacy, workflow efficiency, brand management, and security. Users can use aliases for distinct interactions to protect their primary email addresses from spam, phishing, and unsolicited communications, ensuring robust privacy. Workflow optimization is achieved through alias-based filtering and labeling, enabling users to prioritize tasks and streamline inbox management, thereby boosting productivity. For organizations, branded aliases strengthen brand identity, build stakeholder trust, and maintain consistent communication. Furthermore, alias-based authentication and access restrictions reinforce security standards, mitigate unauthorized access, and facilitate compliance and auditing. The technological implementation of email aliasing is underpinned by established email protocols, server configurations, and client applications. SMTP facilitates message routing from sender to recipient, while IMAP and POP3 allow recipients to retrieve messages addressed to aliases. Server-side configurations enable administrators to create aliases and establish forwarding rules, ensuring seamless message delivery to designated mailboxes. These configurations are managed using administrative controls, allowing the mapping of aliases to specific recipients and applying forwarding criteria, such as domain or message content. On the client side, users manage aliases through email client interfaces, where they can create aliases, specify forwarding addresses, and customize settings like reply-to headers. Advanced organizational features in email clients allow users to group aliases into folders or categories, simplifying access and enhancing usability. By integrating practical applications with robust technical execution, email aliasing is a scalable and efficient solution for improving privacy, security, and operational workflows across personal and organizational contexts. This dual approach underscores its potential to address growing email traffic and evolving cyber threats.

Email aliasing has emerged as a robust solution to enhance security, streamline communication, and provide flexibility for individuals and organizations. Authentication and security protocols are fundamental to safeguarding email conversations when using aliases. Techniques like SPF, DKIM, and DMARC authenticate senders and prevent phishing or spoofing attempts. SSL and TLS encryption further secure email content, while access controls ensure only authorized individuals can manage aliases, preventing misuse. Integrating identity management systems and single sign-on solutions centralizes alias administration, enabling businesses to enforce consistent security measures across platforms. One of the key benefits of email aliasing lies in its ability to enhance privacy and security. By compartmentalizing email interactions, users shield their primary email accounts from spam, phishing, and identity theft. Aliases can be easily updated or revoked if compromised, minimizing risks of unauthorized access. Additionally, alias-based filtering and labeling simplify workflow management, enabling users to prioritize and organize communications effectively. Users reduce inbox clutter by creating project- or contact-specific aliases and ensure timely responses to critical messages. Customization is another advantage, as aliases can reflect professional identities, preferences, or branding requirements. Personalized aliases foster professionalism, strengthen brand awareness, and support consistent communication with clients or stakeholders. Furthermore, email aliasing offers scalability and flexibility, allowing users to create temporary aliases for specific purposes, such as registrations or event RSVPs, and deactivate them when no longer needed. Despite these benefits, email aliasing poses security challenges, including the risk of phishing and spoofing attacks. Malicious actors may exploit aliases to deceive users. Organizations must implement robust authentication protocols to mitigate these risks and educate users on recognizing suspicious communications. By balancing security considerations with operational efficiency, email aliasing provides a practical, cost-effective approach to managing digital communications while safeguarding privacy and reinforcing organizational identity.

Effective management of email aliases is essential to prevent misuse, unauthorized access, or malicious exploitation. Implementing stringent access controls and permissions for creating, updating, and deleting aliases ensures robust administration. Regular audits and reviews of alias settings are vital for detecting irregularities or unauthorized changes that may indicate policy violations or security breaches. Such proactive measures reinforce the integrity of alias management systems. Data protection and privacy compliance are critical for email aliasing, particularly when handling sensitive information. Organizations must adhere to legal frameworks like GDPR and HIPAA, enforcing data retention policies and utilizing encryption protocols such as TLS to secure data in transit. These measures safeguard sensitive information and ensure compliance with privacy regulations, fostering trust among stakeholders. Strong authentication mechanisms are indispensable for preventing unauthorized access to email aliases. Solutions like multi-factor authentication (MFA) and single sign-on (SSO) add layers of security, reducing the likelihood of account compromise. By requiring multiple verification factors or centralized identity credentials, organizations can mitigate risks associated with credential theft and unauthorized account access. Educating users about email security plays a pivotal role in addressing vulnerabilities related to email aliasing. Comprehensive training programs should emphasize best practices, such as recognizing phishing techniques, verifying sender identities, and maintaining secure communication habits. Empowering users with knowledge foster a culture of vigilance and accountability, reducing the likelihood of successful phishing attempts. Continuous monitoring of email traffic, alias

Table 1: Existing email aliases.

Email Alias	Description	Limitations
Gmail	A popular email service provider offering aliasing functionality.	Limited alias creation options compared to some other providers.
Aqua Mail	Another email service provider with aliasing capabilities.	Requires a separate application for managing aliases.
Yahoo Mail	Offers email aliasing functionality for users.	Limited integration with third-party services.
Outlook	Microsoft's email service provider, which allows users to create aliases.	May require a Microsoft account for full functionality.
ProtonMail	A secure email service provider offering aliasing features.	Limited to users of ProtonMail's platform.
Zoho Mail	Provides email aliasing features for users and businesses.	Some advanced features may require a premium subscription.
iCloud Mail	Apple's email service with aliasing capabilities for iCloud users.	Limited integration with non-Apple services and applications.

activity, and security logs enables organizations to detect and address threats promptly. Incident response protocols should be established to investigate breaches, minimize risks, and mitigate potential damage. Rapid identification and resolution of security issues not only protect sensitive information but also enhance operational resilience and prevent future compromises. The existing techniques of Email aliasing are discussed in Table 1.

4. Conclusion

Email aliasing has emerged as an indispensable tool in modern communication, addressing the dual challenges of privacy and efficiency in a digital era characterized by increasing security threats and communication complexity. This research highlights the evolution of email aliasing from rudimentary alias-based systems to sophisticated, user-centric solutions that integrate advanced security protocols and scalable management frameworks. By enabling the creation of virtual identities linked to a primary mailbox, email aliasing empowers users to compartmentalize communication, enhance privacy, and streamline workflows. Implementing email aliasing offers significant benefits for individuals and organizations alike, including improved security, enhanced productivity, and optimized communication channels. From safeguarding sensitive information through alias-based encryption to mitigating phishing risks with authentication protocols such as SPF, DKIM, and DMARC, email aliasing demonstrates its potential as a robust security measure. Moreover, its versatility in accommodating personal, role-based, generic, and disposable aliases underscores its adaptability across diverse use cases. Effective deployment of email aliasing requires a comprehensive approach encompassing meticulous planning, user education, and integration of advanced technologies. Organizations must prioritize secure authentication, rigorous access controls, and compliance with privacy regulations to mitigate risks and ensure the integrity of alias-based systems. Additionally, leveraging automated tools and third-party services can enhance the efficiency of alias management while reducing administrative overhead. As digital communication evolves, email aliasing remains a critical enabler of secure and efficient interactions. By embracing its principles and addressing its challenges, individuals and organizations can harness its full potential to foster collaboration, protect identities, and maintain resilience in an increasingly interconnected world. Future research and innovation in this domain will further refine its capabilities, ensuring its continued relevance in the dynamic landscape of email communication.

Conflict of Interest

There is no conflict of interest.

Supporting Information

Not applicable

Use of artificial intelligence (AI)-assisted technology for manuscript preparation

The authors confirm that there was no use of artificial intelligence (AI)-assisted technology for assisting in the writing or editing of the manuscript and no images were manipulated using AI.

References

[1] M. Yin, X. Li, J. Luo, X. Li, Y. Tan, Automatically extracting name alias of user from email, *International Journal of Engineering and Manufacturing*, 2011, **1**, 14-24, doi: 10.5815/IJEM.2011.06.03.

[2] S. Shukla, M. Misra, G. Varshney, Email bombing attack detection and mitigation using machine learning, *International Journal of Information Security*, 2024, **23**, 2939–2949, doi: 10.1007/s10207-024-00871-7.

[3] A. Venckauskas, J. Toldinas, N. Morkevicius, F. Sanfilippo, An email cyber threat intelligence method using domain ontology and machine learning, *Electronics*, 2024, **13**, 2716, doi: 10.3390/electronics13142716.

[4] F. Wang, J. Tian, J. Ling, Z. Chen, Z. Xu, A multi-stage

resilience analysis framework of critical infrastructure systems based on component importance measures, *Reliability Engineering System Safety*, 2025, **256**, 110720, doi: 10.1016/j.ress.2024.110720.

[5] C. Curt, J.-M. Tacnet, Resilience of critical infrastructures: review and analysis of current approaches: resilience of critical infrastructures, *Risk Analysis*, 2018, **38**, 2018, doi: 10.1111/risa.13166.

[6] D. Piedrahita, J. Bermejo, F. Machio, A secure email solution based on blockchain, Blockchain and Applications, Lecture Notes in Networks and Systems, Springer, 2022, **320**, doi: 10.1007/978-3-030-86162-9_36.

[7] J. N. Al-Karaki, A. Gawanmeh, C. Fachkha, Blockchain for email security: a perspective on existing and potential solutions for phishing attacks, IEEE Fifth International Conference on Blockchain Computing and Applications (BCCA), Kuwait, 2023, doi: 10.1109/BCCA58897.2023.10338865.

[8] R. Gupta, A. Raghuwanshi, Comparative study of email spam filtration using machine leaning algorithms, *International Journal of Science and Research*, 2023, doi: 10.21275/sr23827122535.

[9] A. K.Sharma, S. Sahni, A comparative study of classification algorithms for spam email data analysis, *International Journal on Computer Science and Engineering*, 2011, **3**, 1890-1895.

[10] V. K. Devendran, H. Shahriar, V. Clincy, A comparative study of email forensic tools, *Journal of Information Security*, 2025, **6**, 111-117, doi: 10.4236/jis.2015.62012.

[11] S. M. Abdulhamid, M. Shuaib, O. Osho, Comparative analysis of classification algorithms for email spam detection, *International Journal of Computer Network and Information Security*, 2028, **1**, 60-67, doi: 10.5815/ijcnis.2018.01.07.

[12] T. Muralidharan, N, Nissim, Improving malicious email detection through novel designated deep-learning architectures utilizing entire email, *Neural Networks*, 2023, 157, 257-279, doi: 10.1016/j.neunet.2022.09.002.

[13] D. K. Yadav, A.Raj, Rajlakshmi, N.Kumar, R. Kumari, Enhancing email security: a real-time machine learning-based spam detection system, *Internet Technology Letters*, 2024, e618, doi: 10.1002/itl2.618.

[14] E. G. Dada, J. S. Bassi, H. Chiroma, S. M. Abdulhamid, A. O. Adetunmbi, O. E. Ajibuwa, Machine learning for email spam filtering: review, approaches and open research problems, *Heliyon*, 2019, **5**, e01802, doi: 10.1016/j.heliyon.2019.e01802.

[15] R. Fatima, M. M. Sadiq Fareed, S. Ullah, G. Ahmad, S. Mahmood, An optimized approach for detection and classification of spam email's using ensemble methods, *Wireless Personal Communications*, 2024, **139**, 347–373, doi: 10.1007/s11277-024-11628-9.

[16] S. K. Birthriya, P. Ahlawat, A. K. Jain, An efficient spam and phishing email filtering approach using deep learning and bio-inspired particle swarm optimization, International *Journal of Computing and Digital Systems*, 2024, **15**, doi: 10.12785/ijcds/150144.

[17] N. Elisa, L. Yang, F. Chao, N. Naik, "TOSSAPON BOONGOEN secure and privacy-preserving e-government framework using blockchain and artificial immunity, *IEEE Access*, 2023, **11**, 8773-8789, doi: 10.1109/ACCESS.2023.3239814.

[18] C. Lambrinoudakis, S. Gritzalis, F. Dridi, G. Pernul, Security requirements for e-government services: a methodological approach for developing a common PKI-based security policy, *Computer Communications*, 2003, **26**, 1873-1883, doi:10.1016/S0140-3664(03)00082-3.

[19] F. A. Rawdhan, M. K. Ibrahim, enhancement of email security services, *International Journal of Scientific & Engineering Research*, 2017, **8**, 2090-2095.

[20] S. Choudhary, R. Ghusinga, E-mail security: issues and solutions, *International Journal of Computer Information Systems*, 2013, **7**, 42-63.

[21] S. K. Devineni, AI in data privacy and security, *International Journal of Artificial Intelligence and Machine Learning*, 2024, 3, 35-39, doi: 10.17605/OSF.IO/WCN8A.

[22] P. Mwiinga, Privacy-preserving technologies: balancing security and user privacy in the digital age, *International Journal of Scientific and Research Publications*, 2023, doi: 10.5281/zenodo.10406538.

[23] A. Reuter, K. Boudaoud, M. Winckler, A. Abdelmaksoud, W. Lemrazzeq, Secure Email - a usability study, *Cryptography and Security*, 2021, doi: 10.48550/arXiv.2110.06019.

[24] E. Nunes, Email security, *Trends in Data Protection and Encryption Technologies*, 2023, doi: 10.1007/978-3-031-33386-6_36.

[25] M. Maass, M-P. Clement, M. Hollick, Snail mail beats email any day: on effective operator security notifications in the internet, In Proceedings of the 16th International Conference on Availability, Reliability and Security (ARES '21). Association for Computing Machinery, New York, USA, 2021, **11**, 1–13, 2021, doi: 10.1145/3465481.3465743.

[26] Y. Chen, Y. Yang, An advanced deep attention collaborative mechanism for secure educational email services, *Computational Intelligence and Neuroscience*, 2022, 3150626, doi: 10.1155/2022/3150626.

[27] S. Stryczek, M. Gwiazdowicz, J. Gozdecki, K. Kosek-Szott, N. Rapacz, J. Rzasa, CyberDART: a corporate federation system for mitigating email threats, *IEEE Access*, 2024, **12**, 189344-189358, doi: 10.1109/ACCESS.2024.3516657.

[28] Y. E. Suzuki, S. A. S. Monroy, Prevention and mitigation measures against phishing emails: a sequential schema model, *Security Journal*, 2022, **35**, 1162–1182, doi: 10.1057/s41284-021-00318-x.

[29] E. Altulaihan, A. Alismail, M. M. Hafizur Rahman, A. A. Ibrahim, Email security issues, tools, and techniques used in investigation, *Sustainability*, 2023, **15**, 1-28, 2023, doi: 10.3390/su151310612.

[30] Z. Alkhalil, C. Hewage, L. Nawaf, Imtiaz A. Khan, Phishing attacks: a recent comprehensive study and a new anatomy, *Frontiers in Computer Science*, 2021, **3**, doi: 10.3389/fcomp.2021.563060.

[31] B. Naqvi, K. Perova, A. Farooq, I. Makhdoom, S. Oyedeji, J. Porras, Mitigation strategies against the phishing attacks: A systematic literature review, *Computer & Security*, 2023, **132**, doi: 10.1016/j.cose.2023.103387.

[32] R. Broadhurst, H. Trivedi, Malware in spam email: risks and trends in the Australian Spam Intelligence Database, *Trends & Issues in Crime and Criminal Justice*, 2020, **603**, 2020, doi: 10.52922/ti04657.

[33] R. G. Broadhurst, H. Trivedi, Malware in spam email: trends in the 2016 australian spam intelligence data, *SSRN Electronic Journal*, 2019, doi: 10.2139/ssrn.3413442.

[34] F. Janez-Martino, R. Alaiz, V. Gonz lez-Castr, E. Fidalgo, E. Alegre, A review of spam email detection: analysis of spammer strategies and the dataset shift problem, *Artificial Intelligence Review*, 2022, **56**, doi: 10.1007/s10462-022-10195-4.

Publisher Note: The views, statements, and data in all publications solely belong to the authors and contributors. GR Scholastic is not responsible for any injury resulting from the ideas, methods, or products mentioned. GR Scholastic remains neutral regarding jurisdictional claims in published maps and institutional affiliations.