The Seybold Report

ISSN 1533-9211

DOI 10.17605/OSF.IO/UX6NG

AN ANALYSIS OF AUTOMATED EMAIL ENCRYPTION USING NETWORK SECURITY

MYTHILI BOOPATHI

Associate Professor, Information Technology, Vellore Institute of Technology, Tamil Nadu, India.
Email: nmythili@vit.ac.in

N. SATHYAMOORTHY

Team leader, Cisco Systems, Bangalore, Karnataka, India. Email: nsathyamoorthy@gmail.cim

Abstract

Automated email encryption is a process of securing email communication by automatically encrypting the email messages sent between two parties. This technology provides an additional layer of protection to sensitive information, preventing unauthorized access to the message content. In this paper the author applied a methodology in which they stated that by using encryption algorithms, automated email encryption ensures that the email content is converted into a coded format that only the intended recipient can decipher, thereby keeping the message content confidential. The results show that the automated email encryption solutions can be integrated into email clients, allowing users to send and receive encrypted emails seamlessly without the need for manual intervention. The author concludes that this technology is particularly useful for businesses and organizations that deal with sensitive data, as it helps to maintain the privacy and integrity of their communications. Automated email encryption has the potential to enhance data security and privacy in communication, while reducing user burden.

Keywords: Automated Email Encryption, Email, Encryption, Network Security, Software.

1. INTRODUCTION

Network security is the process of avoiding unauthorised contact, modification, and obliteration of computer networks and the devices that are associated to them. It entails the use of several techniques, tools, and procedures to safeguard networks against a variety of cyberthreats, including ransomware, hacking, phishing, and virus assaults. Firewalls, which are hardware or software based technologies that control traffic between various network segments or between a network and the internet, are one of the most important elements of network security. Based on predefined security rules, firewalls examine incoming and outgoing traffic and stop unauthorised access to the network. To stop certain assaults, they might be set up to restrict particular ports or protocols [1]–[3].

The control of user identities and permissions is a key component of access control, which is another crucial component of network security. Only authorised users are given access to network resources and data thanks to access control systems. This may be done using a variety of authentication techniques, including smart cards, biometrics, and passwords. Another essential technique for network security is encryption. Data is transformed into a secret code via the process of encryption to prevent unauthorised access. By doing this, it is ensured that even if an attacker has access to the data, they would be unable to read or utilise it. Public key

The Seybold Report
ISSN 1533-9211
DOI 10.17605/OSF.IO/UX6NG

encryption and symmetric key encryption are only two examples of the many encryption techniques that are accessible.

1.1. Network Security

Network security also involves the use of imposition uncovering and preclusion systems (IDS/IPS), which display network traffic for potential security breaches. These systems are able to identify and stop suspicious behavior, such as efforts to take advantage of flaws or gain unauthorized access. Another important aspect of network security is network monitoring and logging. This involves the collection and analysis of network activity logs to identify and respond to security threats. Network administrators can use various tools to monitor network activity, such as network traffic analysis tools, log analysis tools, and intrusion detection systems [4]–[6]. In addition, network security also involves frequent security audits and assessments to find and fix any risks and vulnerabilities. These assessments can be performed internally or by third-party security experts. Overall, network security is an essential component of modern computing and is necessary to protect networks and their associated devices from a wide range of cyber threats. The implementation of various security measures, such as firewalls, access control, encryption, IDS/IPS, and network monitoring, can help safeguard networks and prevent security breaches. To protect the security of their networks and data, it is crucial for organizations to keep current with the newest security technology and best practices.

1.2. Email Security

Email security refers to the measures and tools used to safeguard email correspondence and the data it contains against theft, unauthorised access, interception, alteration, and destruction. Because email is a popular mode of communication and includes private information including financial data, personal information, and trade secrets, email security is crucial. Email security is achieved through a variety of methods and tools, including encryption, digital signatures, spam filters, antivirus software, and phishing defense. These methods try to safeguard email communications and their contents against numerous cyberthreats, including spam, malware, viruses, and phishing assaults. One of the essential methods for email security is encryption. To prevent unauthorised access, email messages are transformed into a secret code. Without the decryption key, even if an attacker manages to access the email, they will not be able to read or use it. Public key encryption and symmetric key encryption are only two examples of the many encryption techniques that are accessible. Digital signatures are another tool used in email security to validate the sender's authority and ensure the message's integrity. Digital signatures are special codes that are appended to the email message and may be used to verify the sender's identity and spot any message manipulation. Another crucial element of email security is spam filtering. They are designed to recognize and stop unwanted or unsolicited email communications, including spam and phishing emails. Spam filters utilise a variety of methods, including content screening, sender reputation analysis, and blacklisting, to detect and prevent spam [7]–[9]. To guard against viruses and malware that may be transmitted by email attachments, antivirus software is also utilised in email security. Incoming and outgoing

The Seybold Report
ISSN 1533-9211
DOI 10.17605/OSF.IO/UX6NG

emails are checked by antivirus software for viruses and malware, and malicious emails may be quarantined or deleted. Protection against phishing is yet another crucial component of email security. Phishing is a sort of cyber-attack whereby false emails that look to be from reliable sources are sent in an effort to acquire sensitive or personal data. Protection against phishing involves a number of strategies, including educating staff members about phishing schemes and how to prevent them as well as putting in place systems to identify and stop phishing emails. In general, email security is crucial for defending against online attacks and guaranteeing the privacy, availability, and integrity of email communications and the data they contain. The usage of spam filters, antivirus software, phishing protection, digital signatures, and encryption may help preserve email communications and defend against different kinds of cyberattacks [10], [11].

1.3. Email Gateway:

An email gateway, also known as an email security gateway or email firewall, is a technology that is used to monitor and secure email traffic between different email systems. An email gateway sits between a company's email server and the Internet, filtering and analyzing incoming and outgoing email messages to protect against a wide range of security threats. An email gateway is typically a hardware or software-based appliance that is designed to provide advanced email security features, such as spam filtering, virus scanning, content filtering, and data loss prevention. It can also be used to enforce corporate email policies, such as archiving, encryption, and email retention. One of the main functions of an email gateway is spam filtering. It analyzes incoming email messages and blocks those that are identified as spam or phishing attempts. An email gateway uses various techniques to identify spam, such as content filtering, sender reputation analysis, and blacklisting. Another important function of an email gateway is virus scanning. It scans incoming and outgoing email messages for viruses and malware and blocks infected emails from reaching their destination. This helps to prevent the spread of viruses and malware through email [12]–[14].

Content filtering is another feature of an email gateway. It is used to block or quarantine email messages that contain inappropriate or sensitive content, such as adult material, hate speech, or confidential data. Content filtering is often used to enforce corporate email policies and compliance requirements, such as HIPAA and GDPR.Data loss prevention is another feature of an email gateway. It is used to prevent the loss or theft of sensitive data through email. Data loss prevention solutions may recognise and prevent the email transfer of sensitive data, including social security numbers, credit card numbers, and proprietary information. In summary, an email gateway is a technology that provides advanced email security features, such as spam filtering, virus scanning, content filtering, and data loss prevention. It helps to protect organizations from a wide range of security threats and ensures the confidentiality, integrity, and availability of email messages and their associated data [15]–[17]. In order to prevent the system from functioning improperly, the author of this paper thoroughly explains the fundamentals of email encryption and the system of clean and affected files. This allows the email gateway to identify virus-infected files, which need to be cleaned and removed from the system and provided the safe and secure networks of the emails. In this paper, the author

The Seybold Report
ISSN 1533-9211
DOI 10.17605/OSF.IO/UX6NG

applied a methodology in which an infrastructure of the Email Gate way is designed that consist of automated email Encryption that works on a simple model.

2. LITERATURE REVIEW

Al-Fedaghi et al. in their study embellish that in computer network security, operational security is studied together with the physical environment, internal procedures, resources, and information. In this paper, the author applied a methodology in which they stated that Current security framework development efforts concentrate on a security ontology that helps with the application of a common language, however such an approach does not help build a basis for a comprehensive security methodology. The results show characterize computer network operations, we propose a diagrammatic representation that focuses on setting boundaries and constructing a representation of a security system. The author conclude that the thinging machine model is the initial stage in creating a security strategy and plan [18].

Yang et al. in their study discloses that Phishing continues to be one of the most dangerous assaults on contemporary network security, despite advancements in ant phishing tactics over time. In this paper, the author applied a methodology in which they stated that phishing preys on individuals, one of a network system's weakest points. The aim of this study is to identify potential phishing victims. In this study, we propose the multidimensional phishing resistance prediction model (MPSPM) to implement the estimation of user vulnerability to phishing. The results show that phishing emails and valid emails, two different sorts of emails. By recruiting volunteers, we were able to enlist 1105 people in our study. These emails were sent to volunteers, and we used a questionnaire to gather information on their demographics, personalities, knowledge backgrounds, security behaviors, and thought processes. The author concludes that two groups using multidimensional characteristics utilizing seven supervised learning techniques: susceptible and no susceptible [19]. Xu et al. in their study embellish that the upgrading of standard email system design using blockchain technology within the current network environment is the main topic of this study. The system's security and stability can be enhanced more effectively thanks to the upgraded system design. The email content is obtained and stored on the blockchain network, according to the methods used by the author in this study to demonstrate regulatory tracing between the supplier of email services and the higher-level organization. The next suggestion is for a blockchain-based enhanced email system, or BUES. The results show the problems of the present conventional email system are solved. Firstly, the threat model of the typical email system is studied, and remedies are offered for different threats. The architecture established by the blockchain network, email servers, and users, according to the author [20].

Lee et al. in their study embellish that the COVID-19 pandemic has increased the damage caused by malicious software, including spear-phishing attacks on businesses or research institutions and attacks using ransomware on information technology and operational computer systems based on commercial networks and social infrastructures. In this paper, the author applied a methodology in which they stated that recently, various studies have been undertaken to avoid additional phishing emails in the workplace since malware assaults utilise emails as

ISSN 1533-9211

DOI 10.17605/OSF.IO/UX6NG

the major way of infiltration. The findings of the most current research reveal that sophisticated blocking systems as a whole such as spam email filtering programs and highly sophisticated persistent threat systems as a whole may have certain limits in their ability to prevent email spoofing. Therefore, experts believe that in the event of damage from malicious software, swift service restoration through resilience is more important than a complex security plan of action. The writer claims that In keeping with this development, we undertook a survey of 100 information security professionals in order to identify the key factors that may effectively stop malware attacks through email [21]. In this paper, the author discussed about the security ontology that aids in the application of a common language, such an approach does not contribute to the creation of a foundation for an all-encompassing security methodology. The findings characterise computer network processes, and we suggest a diagrammatic representation that focuses on creating a representation of a security system and defining limits. The author comes to the conclusion that developing a thinging machine model is the first step in coming up with a security strategy and plan.

3. METHODOLOGY

3.1. Design

In this paper, the author applied a methodology in which an infrastructure of the Email Gate way is designed that consist of automated email Encryption that works on a simple model. There are lots of mails when a virus-infected email message is detected by an email gateway, it needs to be cleaned up or removed from the system to prevent it from infecting other systems or causing harm. Email gateways use various techniques to clean up virus-infected files, such as quarantine, disinfection, and deletion. Figure 1 discloses the Email Gateway that consist of affected files and cleaned files.

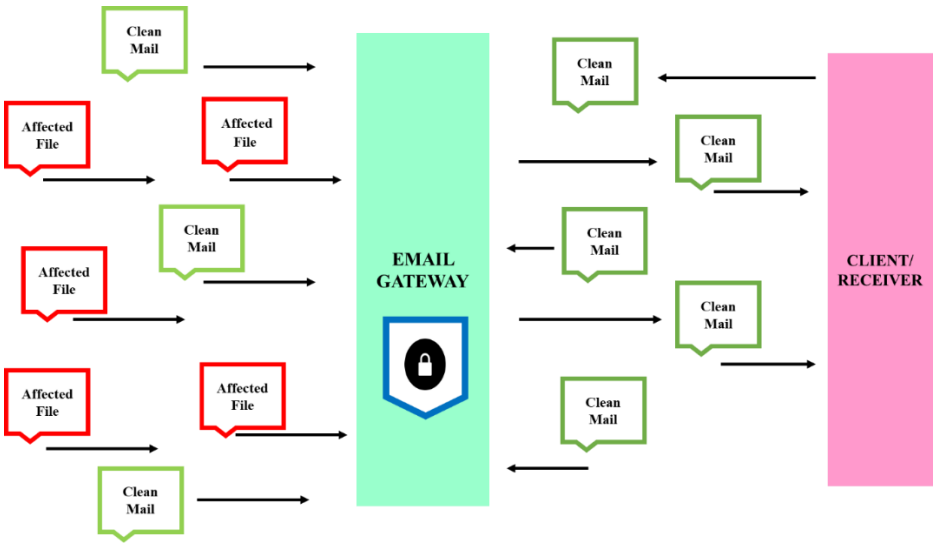

Figure 1: Discloses the Email Gateway that consist of affected files and cleaned files.

The Seybold Report
ISSN 1533-9211
DOI 10.17605/OSF.IO/UX6NG

3.2. Sample and Instruments:

There are different methods in which Email gateway works like quarantine, disinfection and Deletion.

Quarantine: The email gateway can move the infected email message to a quarantine area, where it is isolated from the rest of the system. This prevents the virus from spreading to other systems or causing further harm. The quarantine area can be a separate folder or location on the email gateway, where the infected file is held until it can be safely deleted.

Disinfection: Some email gateways have the ability to disinfect infected files, which means that the virus is removed from the file without deleting the entire file. This can be done by removing the virus code from the infected file or by repairing the file to remove the virus.

Deletion: In some cases, the infected email message may need to be deleted from the email gateway. This is done to prevent the virus from spreading to other systems or causing harm. Once the infected file is deleted, it cannot be recovered.

3.3. Data Collection:

After cleaning up a virus-infected file, the email gateway can send a notification to the sender and/or recipient of the infected email message. This notification informs them that the email message was infected and has been removed or cleaned up. It can also provide instructions on how to prevent further infections and protect their systems. It's important to note that different email gateways may use different methods for cleaning up virus-infected files. The method used will depend on the type of virus, the severity of the infection, and the email gateway's capabilities. Regardless of the method used, the goal is to prevent the virus from causing harm and protect the email system and its users from further infections.

3.4. Data Analysis:

All the data is collected and analysis the first step in the Automated Email Encryption is the sender plain text that is analyzed further. Later on the text goes to the ciphered data set and after that the Encryption takes places. This process carry on till the private key takes places and the Decryption come in action after that the cleaned data goes to the recipient. Figure 2 discloses the Flow between the Sender and the Recipient.

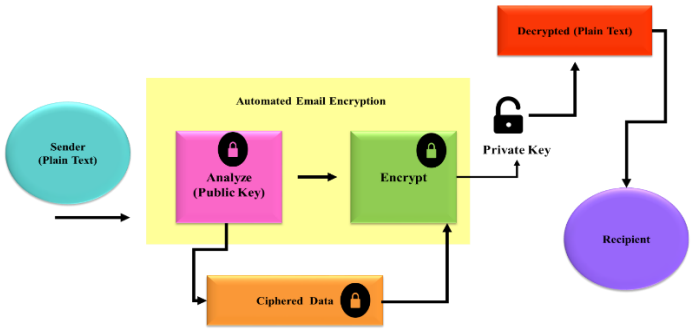

Figure 2: Discloses the Flow between the Sender and the Recipient

The Seybold Report
ISSN 1533-9211
DOI 10.17605/OSF.IO/UX6NG

4. RESULTS AND DISCUSSION

Automated email encryption is a process of automatically encrypting email messages to protect the confidentiality of the message content and attachments. The encryption process involves converting the email message and attachments into a code that is unreadable without a decryption key. The recipient must have the decryption key to unlock and read the encrypted message. Automated email encryption can be implemented using various technologies, such as email encryption software, email gateways, and email clients. The process of automated email encryption typically involves the following steps:

4.1.1. Encryption Setup: Before automated email encryption can be implemented, the encryption system must be set up. This typically involves configuring the encryption software or gateway and generating the necessary encryption keys.

4.1.2. Message Composition: When the sender creates an email message, the email encryption software or gateway automatically detects the message and scans it for sensitive or confidential content. If the message contains sensitive content, the encryption system will automatically encrypt the message and its attachments.

4.1.3. Key Exchange: The encryption system will automatically exchange encryption keys with the intended recipient to allow them to decrypt the message. This key exchange can be done through a secure channel or using public key encryption.

4.1.4. Delivery: The encrypted message is delivered to the addressee's inbox. The inheritor can then decrypt the message using their decryption key.

4.1.5. Decryption: When the recipient opens the encrypted message, the email encryption software or client automatically detects the encryption and prompts the recipient to enter their decryption key. Once the correct decryption key is entered, the encrypted message is decrypted and displayed in its original form.

Automated email encryption provides a secure and convenient way to protect sensitive or confidential email communications. It ensures that only authorized recipients can read the message and protects against unauthorized access or interception. Automated email encryption can be particularly useful for businesses or organizations that handle sensitive information or need to comply with data privacy regulations.

4.2. Public and Private Key

Public and private keys are a fundamental part of automated email encryption. They are used in asymmetric encryption, which employs two distinct keys for encryption and decoding. Each user has two keys in asymmetric encryption: a public key and a private key. The private key is used to decode data, whereas the public key is used to encrypt data. Only the recipient's private key may decode an email message that is encrypted by the sender using the recipient's public key. This means that only the recipient can read the message, even if it is intercepted during transmission. The public key, which is used to encrypt communications, is a key that is publicly accessible. It is often distributed, and anybody may use it to encrypt and send a message to the

The Seybold Report
ISSN 1533-9211
DOI 10.17605/OSF.IO/UX6NG

key's owner. For message decryption, a private key is a confidential key. It should never be disclosed to anybody and is kept private by the key's holder. A sender must first get the recipient's public key in order to transmit an encrypted message to them. The message is subsequently encrypted and sent to the recipient using the recipient's public key by the sender. Only the receiver with their private key may decipher the encrypted communication. A high degree of security is offered by automatic email encryption using public and private keys. Without the private key, a third party will not be able to decrypt the communication, even if they manage to intercept it. This makes automatic email encryption an efficient approach to safeguard private or sensitive email correspondence.

Automated email encryption using network security is a method of automatically encrypting email messages using network security protocols. This ensures that the email is secure and cannot be intercepted or read by unauthorized parties. The process of email encryption involves transforming the email message into an unreadable format using encryption algorithms, and then decrypting it at the recipient's end using a decryption key. This process ensures that even if an unauthorized party intercepts the email message, they will not be able to read it because they do not have the decryption key. Automated email encryption using network security involves implementing encryption at the network level, which means that all email messages sent and received within the network are automatically encrypted. This can be done using various encryption protocols such as transport layer security (TLS) or secure/multipurpose internet mail extensions (S/MIME). Implementing automated email encryption using network security is essential for protecting sensitive information, such as personal identifiable information (PII), financial data, and confidential business information. This is especially important for organizations that handle sensitive data and want to ensure that their communications are secure and protected from unauthorized access.

5. CONCLUSION

In conclusion, automated encryption systems have become an essential tool for securing sensitive information in the digital age. These systems use complex algorithms to clamber data, production it indecipherable without the suitable decryption-key. The implementation of automated encryption has been critical in safeguarding personal, financial, and proprietary information across industries, including finance, healthcare, and government. One of the significant benefits of automated encryption systems is their ability to confirm the concealment, integrity, and availability of data, confirming that only sanctioned festivities can access it. This system reduces the risk of data breaches, cyber-attacks, and unauthorized contact. It can also provide a sense of security for individuals and businesses, knowing that their sensitive information is adequately protected. However, it is crucial to recognize that encryption systems are not foolproof and may have vulnerabilities that can be exploited by attackers. As such, it is essential to implement best practices such as establishing proper key management, regularly updating encryption algorithms, and staying up-to-date with the latest threats and vulnerabilities. Additionally, it is essential to implement multiple layers of security to protect data fully, including access controls, firewalls, and intrusion detection systems.

The Seybold Report
ISSN 1533-9211
DOI 10.17605/OSF.IO/UX6NG

References

1) P. Bhattacharya, S. B. Patel, R. Gupta, S. Tanwar, and J. J. P. C. Rodrigues, "SaTYa: Trusted Bi-LSTM-Based Fake News Classification Scheme for Smart Community," *IEEE Trans. Comput. Soc. Syst.*, vol. 9, no. 6, pp. 1758–1767, Dec. 2022, doi: 10.1109/TCSS.2021.3131945.

2) P. O. Baafi, "Tools For Cyber Forensics," *Adv. Multidiscip. Sci. Res. J. Publ.*, vol. 1, no. 1, pp. 285–290, Jul. 2022, doi: 10.22624/AIMS/CRP-BK3-P46.

3) A. Ostapuk, O. Pluhova, R. Lazuta, and A. Minochkin, "Version of architecture and functioning of the network security management subsystem.," *Commun. Informatiz. cybersecurity Syst. Technol.*, vol. 2, no. 2, Nov. 2022, doi: 10.58254/viti.2.2022.05.36.

4) N. Doukas *et al.*, "Survivability Using Artificial Intelligence Assisted Cyber Risk Warning," in *Advances in Information Security*, 2022, pp. 285–308. doi: 10.1007/978-3-030-97087-1_12.

5) C. C, P. K. Pareek, V. H. Costa de Albuquerque, A. Khanna, and D. Gupta, "Improved Domain Generation Algorithm To Detect Cyber-Attack With Deep Learning Techniques," in *2022 IEEE 2nd Mysore Sub Section International Conference (MysuruCon)*, Oct. 2022, pp. 1–8. doi: 10.1109/MysuruCon55714.2022.9972526.

6) H. Johnson, K. Volk, R. Serafin, C. Grajeda, and I. Baggili, "Alt-tech social forensics: Forensic analysis of alternative social networking applications," *Forensic Sci. Int. Digit. Investig.*, vol. 42, p. 301406, Jul. 2022, doi: 10.1016/j.fsidi.2022.301406.

7) P. Soppelsa, "Theorizing Infrastructure and Affect," in *Urban Infrastructure*, University of Pittsburgh Press, 2022, pp. 207–222. doi: 10.2307/j.ctv30pnvb9.19.

8) Y. Pachipala, E. Nandhitha, K. Haritha, B. V. N. S. Chandrika, and V. C. Jadala, "Face Recognition Application using Offloading Computation over Google Cloud," in *2022 6th International Conference on Computing Methodologies and Communication (ICCMC)*, Mar. 2022, pp. 1395–1400. doi: 10.1109/ICCMC53470.2022.9753980.

9) B. C. Desai, "Meta-stasis of the Internet," in *International Database Engineered Applications Symposium*, Aug. 2022, pp. 43–54. doi: 10.1145/3548785.3548805.

10) A. Joshi and V. Anand, "Design of Novel Key Generation Technique Based RSA Algorithm for Efficient Data Encryption and Decryption," *ECS Trans.*, vol. 107, no. 1, pp. 2585–2592, Apr. 2022, doi: 10.1149/10701.2585ecst.

11) M. E. Hussain and R. Hussain, "Cloud Security as a Service Using Data Loss Prevention: Challenges and Solution," in *Lecture Notes in Networks and Systems*, 2022, pp. 98–106. doi: 10.1007/978-3-030-94507-7_10.

12) N. Gupta, "Quantum and Blockchain for Computing Paradigms Vision and Advancements," 2022, pp. 158–177. doi: 10.4018/978-1-6684-5072-7.ch008.

13) M. Shah, S. Gala, P. Doshi, V. Venkataramanan, and R. Shah, "Security Management in Optical Fiber," in *2022 International Conference on Innovative Computing, Intelligent Communication and Smart Electrical Systems (ICSES)*, Jul. 2022, pp. 1–4. doi: 10.1109/ICSES55317.2022.9914255.

14) M. Shah, S. Gala, P. Doshi, V. Venkataramanan, and R. Shah, "Security Management in Optical Fiber," 2022. doi: 10.1109/ICSES55317.2022.9914255.

15) K. Koo, D. Moon, J.-H. Huh, S.-H. Jung, and H. Lee, "Attack Graph Generation with Machine Learning for Network Security," *Electronics*, vol. 11, no. 9, p. 1332, Apr. 2022, doi: 10.3390/electronics11091332.

16) X. Wu, D. Wei, B. P. Vasgi, A. K. Oleiwi, S. L. Bangare, and E. Asenso, "Research on Network Security Situational Awareness Based on Crawler Algorithm," *Secur. Commun. Networks*, vol. 2022, pp. 1–9, Jul.

The Seybold Report
ISSN 1533-9211
DOI 10.17605/OSF.IO/UX6NG

2022, doi: 10.1155/2022/3639174.

17) R. Afzal and R. Kumar Murugesan, "Rule-Based Anomaly Detection Model with Stateful Correlation Enhancing Mobile Network Security," *Intell. Autom. Soft Comput.*, vol. 31, no. 3, pp. 1825–1841, 2022, doi: 10.32604/iasc.2022.020598.

18) S. Al-Fedaghi and H. Alnasser, "Modeling network security: Case study of email system," *Int. J. Adv. Comput. Sci. Appl.*, 2020, doi: 10.14569/ijacsa.2020.0110312.

19) R. Yang, K. Zheng, B. Wu, D. Li, Z. Wang, and X. Wang, "Predicting User Susceptibility to Phishing Based on Multidimensional Features," *Comput. Intell. Neurosci.*, 2022, doi: 10.1155/2022/7058972.

20) D. Xu, F. Wu, L. Zhu, R. Li, J. Gao, and Y. She, "BUES: A blockchain-based upgraded email system," *China Commun.*, 2022, doi: 10.23919/JCC.2022.00.029.

21) C. Lee and K. Lee, "Impact Analysis of Resilience Against Malicious Code Attacks via Emails," *Comput. Mater. Contin.*, 2022, doi: 10.32604/cmc.2022.025310.