Tuijin Jishu/Journal of Propulsion Technology
ISSN: 1001-4055
Vol. 45 No. 1 (2024)

A Bird's Eye View of Scientific Data Security Approach for Electronic Mail Data Transmission

Dr. Revathi R. , Sangeetha N.

Research Supervisior,Karpagam Academy of Higher Education,

Coimbatore-641021

Research Scholar,Karpagam Academy of Higher Education,

Coimbatore-641021

Abstract:- Today, security is a technical phrase that refers to securing one's daily life against theft and criminal activity. It is a more significant aspect of daily living for humans. The number of questionable actions both domestically and internationally has increased as a result of technology improvements. The electrical and electronic equipment can be used as a tool to carry out a targeted conduct, like phishing. Phishing involves obtaining private data from websites and emails. The article discusses the significance of unusual email traffic as well as people's motivations for plotting and carrying out assaults for their own gain as well as the growth of others. We primarily concentrated on security methods to stop email phishing and to address "secure framework for cache" using PishEM algorithm.

Keywords: Introduction, Related work, Statement of the problem, Classification of Phishing, Research objectives, Proposed work, An Algorithmic Approach, Performance Evaluation.

1. Introduction

The use of email is utilized by people all over the world to play tricks on friends, maintain conditional business relationships, send critical documents, remain in touch with family members, communicate joyous and saddening life events, and more. More and more people and companies use email as their main source of communication, a significant portion of which may contain confidential information, trade secrets. and personal data. Due to its significance, there have been a number of suspected attacks utilizing various techniques by professionals and others, either for their own purposes or for the benefit of others. All of these events happen exclusively with the intent of profiting off other people's labor, such as phishing [1].

2. Phishing On E-Mail

Phishing and spam emails are occasionally targeted together. The planned end action on the part of the targeted user is the primary distinction between a spam email and a phishing email attack. Phishing occurs when a phisher sends out an email and then tries to obtain the resources or information of the targeted user for their own gain or the gain of others. Sometimes the assault itself is a deception about how the user's data or resource will be used.

Typically, phishing emails that ask for details about financial accounts are hoping to utilize that information to withdraw money from the account in question. The resources required to run software on someone else's computer, such as broadband and disk space, are sought after by phishing emails that try to take advantage of software vulnerabilities on a user's PC.

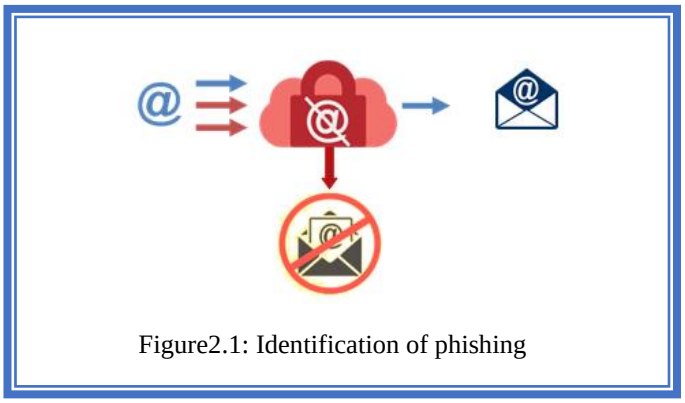

Figure2.1: Identification of phishing

The actor, commonly known as Phisher, aims to illegally obtain information of the target user by using deceptive tactics and fraudulent schemes for the purposes of making fraudulent withdrawals from the target's user account.

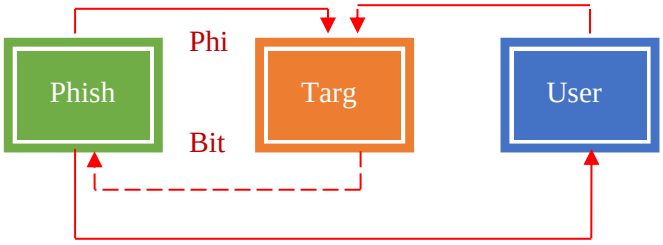

Figure 2.2: Phishing for account information

3. Statement of the Problem

Even while email is a popular form of communication, it is not the safest or most dependable. The main factors affecting the dependability of internet e-mail communication are virus-infected emails and eavesdropping on network links. [23].

At this stage, it is important to point out important considerations and aspects of the situation for the insecurity in e-mail delivery pathway:

Email communications sent by a user may be vulnerable on four different systems: the sender's device, the recipient's device, the network, and the server. No matter how tech-savvy you are, anyone should be able to understand the first and last sentences. Email accounts are often always signed in, so any person using a computer or phone should be able to read any email message they want. Since saved communications from email providers are rarely encrypted, reading emails and attachments is as simple as using the application or going to the website.

An email message might travel through as it makes its way to the receiver, the ship contains thousands of routers and switches, each transmission providing an opportunity to the suspicious activities. There is no guarantee that each connection is equally secure. Email servers are rarely encrypted, because of the overhead costs of encryption. It emphasizes the importance and also highlights the value of protecting messages to plaintext, so hackers with admin passwords or access through security flaws can search Emails pass through vast expanses of personal data from sender to recipient, from storage to deletion. The inherent insecurity of email is undeniable throughout these processes.

On its way to a recipient, e-mail message may pass as emails travel through N number of router and switches, their path highlights the complex and interconnected nature of the digital infrastructure that enables communication., and each transmission presents a potential opportunity for shady behavior. No link can be guaranteed to be equally secure. Due to the high overhead costs of encryption as utility of preserving communications in plaintext, email servers are rarely encrypted, making it possible for hackers with admin passwords or access through security weaknesses to sift through enormous quantities of emails for personal information. Email is incredibly unsecure, from sending to receiving, saving to removing.

4. Research Objectives

The primary objective of the study, to arrive at and develop a framework, serves as the central focus of the research for secure data science using PhishEM guard algorithm for mail security awareness system [1],[3],[11].

- To explain the nature of SMTP email security and the reality that risks to data security are constantly growing.
- To conduct an examination of the SMTP routing protocols, clustering techniques, and security mechanisms currently in use.
- To create and implement a Hybrid Detection System model for communication networks utilizing Ant Colony Optimization (ACO) to find network anomalies and protect email network devices.
- To propose a cache discovery method employing ACO in order to build and create a Data Caching Scheme (DCS) that increases the data accessibility ratio and decreases query latency.
- To create an improved data science framework that increases security when retrieving data. To do this, immunity is incorporated into data packets, boosting data accessibility and decreasing query duration with the use of cross-layer design and clustering
- To discuss the creation of a framework to guarantee and protect data access via SMTP.

5. Proposed Work

We suggest implementing the research activity in order to generate fresh concepts, information, and awareness in the form of research methodologies. The study will create a framework for protecting data from attack. In order to isolate the attacker, these security procedures will include authenticating routing changes, setting up a firewall, spotting intrusion attempts, and responding with group rekeying techniques [1],[3].

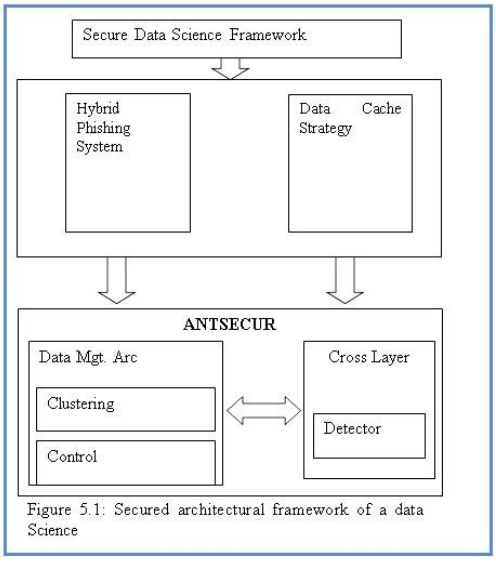

Figure 5.1: Secured architectural framework of a data Science

It enhances approaches to a challenge. The investigation is divided into two models in this section: theoretical and simulation. Theoretical model study incorporates several security concerns and answers. Run simulations using configuration in the simulation model in an effort to discover the processes that will enable us to enforce security in SMTP [3]. The Hybrid Phishing Deduction System looks for anomalies, and the Data Science Strategy uses a cache finding technique to find and retrieve the necessary data.

The ANTSECUR Framework is used to integrate Hybrid PDS and cache management [3][4]. The Cross Layer and the Cache Management architecture (Data Mgt. Arc) make up this framework. To deal with node failure and misbehavior, the data packets include the control packets, Cross Layer protocol, and detector set.

6. An Algorithmic Approach

The Ant Colony Optimization (ACO) Algorithm has been demonstrated to give an optimum solution in autonomous knowledge gathering challenges for awareness, resilient routing, screening, and tracking, among other issues [19],[21],[22]. Swarm intelligence encompasses a variety of techniques. An optimization algorithm class known as ACO is based on how an ant colony functions. ACO techniques are used to solve issues when goals need to be found.

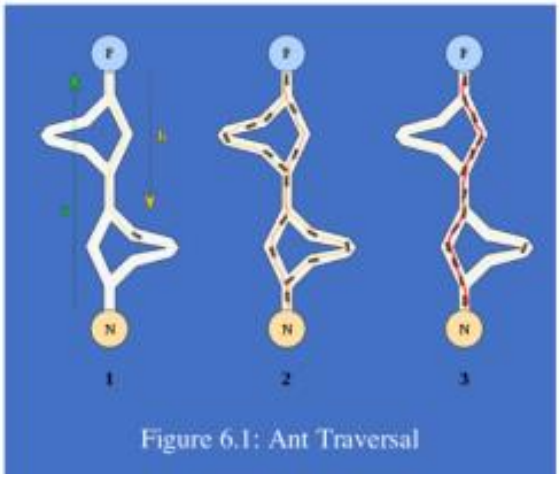

Figure 6.1: Ant Traversal

While scouting their surroundings, real ants leave behind pheromone trails that guide one another to resources. Like real ants, the computer-generated 'ants' record their positions and the effectiveness of their discoveries so that more 'ants' can come up with better solutions in later simulation trials. The ants always use the same route, they increase the density of the pheromones, making it a more potent source of food. The more dense the pheromone trails are, the more likely it is that a food source is there. The pheromone trails are sparsely distributed along the less-traveled ant pathways and do not strongly suggest a food source. This idea of ACO can be compared to email networks, where the network's devices communicate data between the other devices in packets. In order to route the information along the shortest path, the ACO algorithm incorporates this kind of information exchange.

The following is the algorithm of ACO.

```
start procedure     ACO_MetaHeuristic
do while(if not termination)
                antGeneration_and_Activity()
                   phishActions()
     phishUpdate()
end do
end procedure
```

The creation of ants, their movement, and activities associated with them are all covered by the ant Generation_and_Activity function. The phishActions() function is used to perform centralized activities that cannot be performed by a single ant, such as calling a localized optimized procedure or updating global data to

determine whether to bias the search process from a non-local perspective. To avoid the unlimited accumulation of trace values across connections, phishUpdate() is used to remove trace values over time. [19],21],[22].

7. Performance Evalution

An NS-2 simulation environment was used to assess the proposed ANTSECUR framework [29]. A variety of simulation situations have been run. The end-to-end delay and proportion of packets delivered are used to assess the effectiveness of the suggested framework works Each host in the simulation navigates the simulated space using a mobility model with random waypoints. The transportation pattern of email data in SMTP is simulated using the random waypoint model. A 1500*1000m simulation was run for 150 and 200 nodes. In Table 6.2, the simulation parameters are listed.

Parameter	**Value**
TransmissionRange(M)	300
Bandwidt(Mbps)	3
NodeSpeed(M/s)	0-10
RoutingProtocol	AntPhishNet
PauseTime(S)	100
Data size(KB)	300
AverageTTL(S)	100-3000
Zipf-likeParameter( )	0.5-1.0
Number of Data items	1000
No.of nodes	150,200
RequestInterval(S)	10
SimulationTime	2000 .

Table 6.1. ns-2 Simulation Parameters

Two scenarios dependent on the quantity of client nodes have been taken into consideration in order to assess the performance of the proposed ANTSECUR framework. The average delay from end to end and packet delivery ratio were calculated from five Tcl simulations that were conducted in 150 and 200 nodes. Generally speaking, a bad node can increase latency, drop packets, and lower network throughput. The data packet contains AISp, which has been integrated to lessen this influence. This shields the network from nodes that behave strangely.

The mean value is calculated and shown in Table 6.3 for the packet delivery ratio with the end-to-end delay of ANTSECUR framework. It shows good performance than AODV+COCA because it contains cross layer control CLC. This CLC controls path distraction brought on by node failure, thereby lowering end-to-end latency. The packet delivery ratio increases as latency decreases. But there is no control for managing Path distraction in case of AODV+COCA. The delivery ratio was 95.58% in the ANTSEC framework where it was 90.92% in case of AODV+COCA. When transmitting packets,

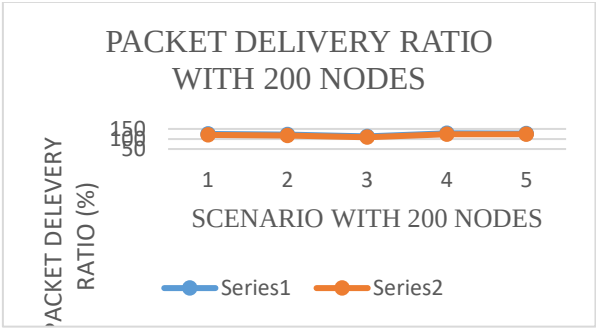

Figure 7.1 PDR(Packet Delivery Ration)With reference to 200 nodes

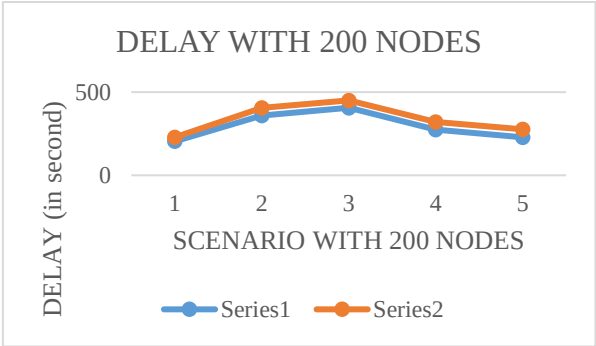

Figure 7.2 Delay of Packets with 200 Nodes

The packet delivery ratio of the network with 200 nodes and 150 nodes is depicted in the Figure 7.1 and Figure 7.3 respectively. The packets delay of the network with 200 nodes and 150 nodes is depicted in Figure 7.2 and Figure 7.4 respectively.

The statistical paired t-test has been proposed to evaluate the significant difference betweenthe ANTSEC framework is 7.70% more efficient at improving the packet delivery ratio and 22.91% more efficient at reducing delay than AODV+COCA.

Table 6.5 indicates that the ANTSECUR framework performs well in the Tcl simulation runs. In the ANTSEC framework, the delivery ratio was 92.26%, whereas for AODV+COCA, it was 88.79%. If there is a delay, AODV+COCA takes about 252.17 ms to transmit the packet, whereas ANTSEC transmits it in 220.85 ms. Compared to AODV+COCA, the suggested framework transmits packets with a 12.42% delay reduction and a 3.9% packet delivery ratio improvement efficiency.

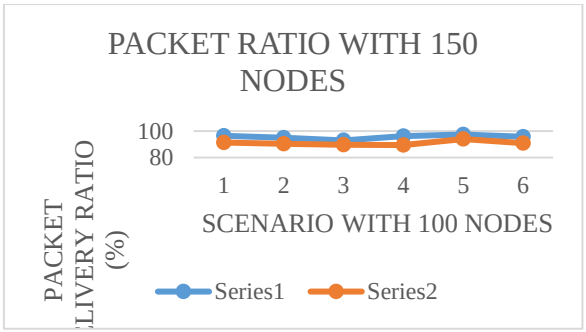

Figure 7.3 PDR(Packet Delivery Ration)With reference to 150 nodes

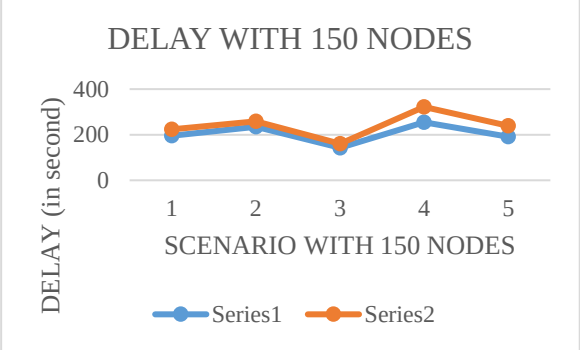

Figure 7.4 Delay of Packets with 150 Nodes

proposed model and existing model with respect to Packet Delivery Ratio (PDR) and Packet Delay. Hence, the proposed model has found significant effect on existing model with respect to Packet Delivery Ration(PDR) and Delay in both the scenarios with 150 nodes and 200 nodes.

The ANTSECUR framework always outperforms AODV+COCA as it embeds ACO and PhishEM; both factors make the proposed framework more efficient with higher PDR (Packet Delivery Ratio). As the framework uses SMTP and the misbehaving nodes are identified by the email data which are embedded into the Data Packets (DP) the end-to-end delay is lowered. From the above results, it is proved that the proposed ANTSECUR framework works well in large network size including malicious nodes.

Conclusion

Due to its widespread use, email will inevitably be used for illegal purposes like phishing. By passing the Information Technology Act and granting exclusive rights to the police and other authorities to combat such crimes, governments all over the world have made significant strides in the prevention of phishing E-Mail.

National laws have been passed in an effort to combat E-crime, but in the long term, their benefits may not be as great as hoped. To combat the impending threat of email-related crimes and create a cyberspace free of crime, an effort is still needed to create an international law on internet usage. The best treatment, they say, is prevention. Cyber laws apply criminal penalties to try to stop

References

[1] Dr. K. Thangadurai, Gopu.G, “A secure data cache framework to deduct phishing E-Mail using ACO technique” IJRAR January 2019, E-ISSN 2348-1269, P-ISSN 2349-5138.

[2] Annu K Simon, Dr, S Subasree, “Design and Development of Enhanced Optimization Techniques based on Ant Colony Systems”, IJIRST - International Journal for Innovative Research in Science & Technology Volume3, Issue 04, ISSN (online): 2349-6010, September 2016.

[3] Dr. K. Thangadurai, Gopu.G, “A study on Ethical Phishing on E-mail networks and its impacts in India”, Indian Journal of Science and Technology, Vol 9(45), DOI: 10.17485fijst/2016/69i45/90847, December 2016.

[4] Karthika Renuka D, Visalakshi P, Girish R “A Hybrid ACO Based Feature Selection Method for Email Spam Classification”, WSEAS transactions on computers, E-ISSN: 2224-2871, Volume14, 2015.

[5] Ankur Dumka, Ravi Tomar, J.C.Patni, Abhineet Anand, “Taxonomy of E-Mail Security Protocol”, International Journal of Innovative Research in Computer and Communication Engineering, Vol-2, no.-4, April2014.

[6] P.Rohini, K.Ramya, “Phishing Email Filtering Techniques A Survey”, Volume 2, Issue 1, February 2011, Volume 17 number1, Nov 2014.

[7] Gori Mohamed .J, M. Mohammed Mohideen, Mrs. Shahira Banu.N “E-Mail Phishing – An open threat to everyone” International Journal of Scientific and Research Publications, Volume 4, Issue 2, February 2014,

ISSN 2250-3153.

[8] SANS the monthly security awareness newsletter for computer users, "Email Phishing Attacks", February 2013.

[9] Phishing attack against MSN/Hotmail users - a new year, but old tricks still persist by Graham Cluley, Monday, January 14, 2013.

[10] N. Vijayalakshmi, E.Sivajothi, Dr.P.Vivekanandan, "Efficiency and Limitation of Secure Protocol in Email Services", International Journal of Engineering Sciences and Research Technology, pp-539-544, Nov-2012.

[11] Umamaheswari S, Radhamani G, "Clustering Schemes for Mobile Ad Hoc Networks: A Review", IEEE sponsored Second International Conference on Computer Communication and Informatics (ICCCI 2012), 2012.

[12] Sunny gill, Gaurav Rupnar, Vaibhav Ramteke, Prof. Dipit Patil, Vijay M.Wadhai. "Email Security Protocol", International Journal of Computer Trends and Technology – March to April Issue 2011.

[13] Shamal Firake, Pravin Soni, Dr. B.B. Mesharam, "Phishing E-mail Analysis", International Journal of Computer Trends and Technology, Volume 2, Issue 1, February 2011.

[14] Hung-Min Sun, Bin-Tsan Hsieh, Hsin-Jia Hwang, "Secure E-mail Protocols Providing Perfect Forward Secrecy", Volume 2, Issue 1, February 2011.

[15] Mrs. K.Shanmugavadivu, Dr M. Madheswaran, "Caching Technique for Improving Data Retrieval Performance in Mobile Ad Hoc Networks", (IJCSIT) Vol. 1 (4),2010,249-255

[16] Nada M.A.Al Salami, M.A., "Ant Colony Optimization Algorithm", UbiCC Journal, Vol.4, No.3, pp.823-826, 2009.

[17] Stuart McClure, Joel Scambray, George Kurtz, "Hacking Exposed 6 Network Security Secrets & Solutions" 10th Anniversary Edition, 2009, the McGraw-Hill.

[18] Chu Yan, Zhang JianPei, Zhao Chunhui, "Data Cache Strategy Based on Colony Algorithm in Mobile Computing Environment", IEEE International Conference on Internet Computing in Science and Engineering, pp.235-238, 2008.

[19] Dorigo, M., Mauro Birattari, Thomas Stiizle, "Ant Colony Optimization", IEEE Computational Intelligence magazine, November 2006.

[20] M. Altinet, Q. Luo, S. Krishnamurthy, C. Mohan, H. Pirahesh, B. G. Lindsay, H. Woo, L. Brown, "DBCache: Database Caching for Web Application Servers", 612, SIGMOD 2002.

[21] Cordon, O., F. Herrera and T. Stützle, special issue on "Ant Colony Optimization", Vol. IX, No.2-3, Mathware and Soft Computing, November, 2002.

[22] James Kennedy, Russel C.Eberhart, Yuhui Shi, "Swarm Intelligence", Morgan Kauffman Publishers, 2001.

[23] Ankit Fadia, "E-mail Hacking", Vikas Publishing House Pvt. Ltd.

[24] Rajendra Maurya "HACKING MADE EASY", SCORPIO NET SECURITY SERVICES Publication, 2nd Edition.

[25] Agrawal, D. P. and Qing-An Zeng, "Introduction to Wireless and Mobile Systems", 2005, Brooks/Cole.

[26] Andrew S. Tanenbaum, David J. Wetherall, "Computer Networks, Pearson", 2011.

[27] CISCO Security White Paper "Email Attacks: This Time its Personal", June 2011.

[28] Behrouz A, Forouzan, "Data Communications and Networking", New Delhi: Tata McGraw-Hill, 2011.

[29] Artail, H., Haidar Safa, Khaleel Mershad, Zahy Abou-Atme, Nabeel Sulieman, "COACS: A Cooperative and Adaptive Caching System for MANETs".[30] Network Simulator 2, http://www.isi.edu/nsnam/ns