

# Intelligent Blacklist Security System for Protecting Spammer in Corporate Email Solution: A Case of Corporate Email Service Provider in Thailand

Rattanachai Wongwatkit\*, Montree Raktham\*, Thanadet Phawananthaphuti\*

\*Technology Land Co., Ltd., Bangkok, Thailand

contact@technologyland.co.th, montree.r@technologyland.co.th, thanadet.p@technologyland.co.th

**Abstract—** In the present, there're billions of information transactions around the world each day including email. Technology Land Co., Ltd. (TL) is the email service provider organization that provides the email domain name to the client's organization. However, there have been problems that occurred in the TL email service provider (TLESP) system which must be solved immediately to solve the existed problems and prevent further damage. Additionally, the improved TLESP system has used artificial intelligence (AI) as the core for email spamming, viruses, hackers, and unusual behaviour detection. Also, the advanced TL's email system incoming process and outgoing process security have been explained together with system results and user benefits after the improvement of the system in this study.

**Keywords—** Email Service Provider, Artificial Intelligent, Email Security, Email Spam Detection, Email Blacklisting, Corporate Email

## I. INTRODUCTION

In the past years, billions of information have been sent around the world each day including email. The email service provider has been playing an important role in modern society for providing the email address to the individuals or organizations for use in sending information or email through the internet, which might cause the leaking of confidential information if the email provides an insecure system to the clients [1]. Consequently, the leaking of confidential information may cause enormous damage to both the email service provider and clients. Therefore, the email service provider has a responsibility to offer a high-security system to the clients for preventing unexpected damage and bad consequence in the future.

Technology Land Co., Ltd. (TL) is the email service provider organization in Thailand that has limitations in the email system that has been provided to the organization as clients. The old system's problem includes the limitation in the behaviour analysis between actual user and robot, and country source to limit the email usage, the limitation in filtering system which filters only email content and virus without the protection of hacker trying to use email in different country and location, the limitation in user unusual behaviour checking that lead to the blacklist of email provider

server. As a result, the damage had been occurred to the clients in many ways, as the follows (1) The hacker deceived the client's business partner to transfer the money to a different account from a different country (2) The client email account had been used to send spam or marketing mail to a non-exist email account in great number results in email temporally not useable (3) Some of the email provider receivers like Hotmail has blocked the mail receiving from TL server because many users of TL server sent many spam mails to the receiver results in TL server blocking from the receiver server.

Based on the problems of the TL email system, TL email service provider must solve the problems and improve the system to prevent further severe damage for the clients. Accordingly, the approaches for solving problems have been provided in many ways including (1) Using the blacklist system which is the system that banned the unusual using behaviour account (2) Using the domain limit system which is the system for preventing from sending email to the domain that never contacts before over limits (3) Using the inappropriate content detection system to detect profanity language. Therefore, once the email service provider system security has been provided, the clients have received more secure email services in many ways. First, the hacker cannot use the email to subrogate as the client, as the ability to detect the strange location and behaviour of the email account in the system. Second, the safer email system that has been provided to clients can prevent unexpected issues between clients and receivers. Third, the system can prevent sending the spamming email of the client account to receivers if the account has been infected with a virus which might cause the loss of the client's credit toward the business's partner.

Additionally, this study will conduct the research that discusses and explain the approaches for solving the problems of TL email service provider in the following structure. The Introduction section provides the background and significance of the study. The Related Studies section explains the reviewing of related studies about the blacklist system, domain limit system, and inappropriate content detection system. Following the system development detail that will be explained in the Development section, then the results will be purposed in the Analysis and Results section. Finally, the

summary and discussion will be described in the Conclusion and Discussion section.

## II. RELATED STUDIES

There has been widespread use of blacklist system to help with the spam email address blocking security, the spam email refers to a list of IP addresses that send spam email in a large proportion of mail by spambots or standalone email agents [2]. Also, there are many methods for conducting the blacklisting system, for example, manual IP entry that is reported by clients, the scanning of IP addresses to find a software that sends the email without authenticating the senders, etc. The blacklist system has been applied in various approaches, the clustering of network interaction datasets to find the malicious IP [3], the origin-based spam mail filtering techniques to categorized the spam email [4]. Also, the domain limit system has been using to limit the traffic from sending emails in an amount that the email service provider defined to prevent from spamming a huge amount of email. However, the clients still able to receive mail from other domains after reaching the maximum amount of mail sending quota [5]. For scanning and filtering the mail that has been sent to the user, the content filtering system must be applied for finding viruses, or spam content or appropriate content embedded in the mail [6]. Recently, there has been used of artificial intelligence or Machine Learning (ML) as the advanced and recommended tool for spam filtering widely around the world and by many techniques to provide effective email spam, content, and virus filtering system[7], [8].

## III. DEVELOPMENT

### A. Analysis

The TL's original email service providing server system (TLESP) has several drawbacks which caused damage to the clients. However, those defects have been analysed from the TL's teams and found the insights in both of the problems to the system and the problems to the clients, these problems also were a factor that could cause the risk for further damage to occur in the future. The problem analysis of the system pointed out that, there were three major problems in the system that have to be solved. First, the original TLESP system blocked the client from sending email when the amount of email limit has been met, without checking the mail's source country and sending from robot or user attending to send it [9]. Second, there were virus and content filtering system in the original TLESP system, but there was a flaw in hacking protection of the email and use of the hacked email in other countries. Third, there was a chance for the server to get blacklisted from other domains easily, the reason was from the unusual email using behaviour of the user but the original system cannot find out.

Particularly, from the flaws of the original TLESP system which has occurred, several damages resulted in negative ways to the clients or business as the following. First case, the hacker can hack the client email account, then tricked client's business partner to transfer the money to another bank account from other country domains. Second, the client email account

has been used to send spam mail or marketing mail to non-exist account in a large amount resulted in temporally unusable of email. Third, the TLESP server usually has been blocked by other email provider server especially Hotmail, the main reason was because many TL's clients have sent a lot of spam mail to the destination server. Therefore, these problems and damage cases must have been solved immediately to protect the client benefits for using TL email service provider [10].

For protecting the client's benefits and account security, TL organization has improved the security process in both incoming process and outgoing process of the system for solving the existed problems and improve server security system. Moreover, the new TL improved system version has been providing a very secure system and better account protection benefits to the clients. First, the TL's system provides more advanced security system protection to the clients by the system will be able to detect the uncommon using behaviour of the email account in different countries and this function can prevent from the damage that may occur from the hacker in other countries domain [9]. Second, TL new system offers the advanced protection system that can prevent from hackers to the clients which this function has been provided by a few or none organization(s) that value this point in the present time. Third, as the new TLESP system provides more security email system which can protect the client account from both of the hacker and spammer, the chance of TL's server IP will be blocked as a blacklist server IP will be prevent and protect to avoid the mistake between incoming and outgoing system [11].

Additionally, for improving the server system security, TLESP has provided a unique security system in both incoming and outgoing processes [12]. Incoming process, the process that TL server would receive mail from other domain or email service provider (ESP) that has been sent from users then TLESP system would check whether it is a spam mail or not and proceed with security checking that check the sent mail in many points as follows, fake sender name, fake domain, imitate domain, and reply to other domain. The incoming process proceeds the security checking system with artificial intelligence (AI) that uses big data and incoming log as a factor to assess the incoming mail. There is also an application of AI in the outgoing process which is the process that checking mail when a client account would send mail to other domains. The AI in the outgoing process will check the outgoing mail in many points as the follows, sender location IP checking, send mail in the same time with many devices checking, historic behaviour comparing, destination email has been contacted in the past checking, the amount of mail has been sent in a minute.

### B. System Design

Since there was an improvement in the TLESP system from an original system to the improved version system, the security system design has been redesigned in a more secure way for both incoming and outgoing processes. The receiving security or incoming mail of the user from other ESP domains to TS server's client email would be controlled by the TL

server incoming process, it is a necessary process to prevent the clients from receiving spam mail in a huge amount, or fake email from the undesired person as these problems can cause damage in various ways to the clients.

Figure 1 illustrates the overall concept of the TLESP incoming process. The objectives of the incoming process security can be explained as the following. First, the incoming process security can prevent a fake account or fake sender name, for example, “John Dong” has sent a mail to the client with “info@example.com” email in the first time, but in the second time “John Dong” has sent mail by “john@gmail.com” that means the second time there is a high chance that the clients have been a target from the spammer, this is the fake sender detection system of TLESP. Second, the fake domain is another problem that can result in user subrogate, the incoming security can protect the client from a fake domain account with fake domain detection, for example, the client has usually contacted the business partner named “John Dong” and John Dong’s email domain was “info@exmple.com” but the second time there was email sending from John Dong with email “info@example.org”, the second time user was the fake user and TL server would block this account as a blacklist IP. Third, besides the 2 tricks that the spam account has tried to attack the TL server, there was another method of spam account. The domain imitate was another method for spamming email server, for example, the real user named “John Dong” has an email named “info@example.com” but the spammer account tried to imitate the real one named “info@exampla.com” which can be considered as looking alike as the real one, the TL incoming process security can also detect this kind of spam in the server. Forth, the TLESP system would check whether the incoming mail has the right format, not empty or anonymous, and not spammer account before receiving that mail. The incoming security process use AI as the core for analysing the incoming mail.

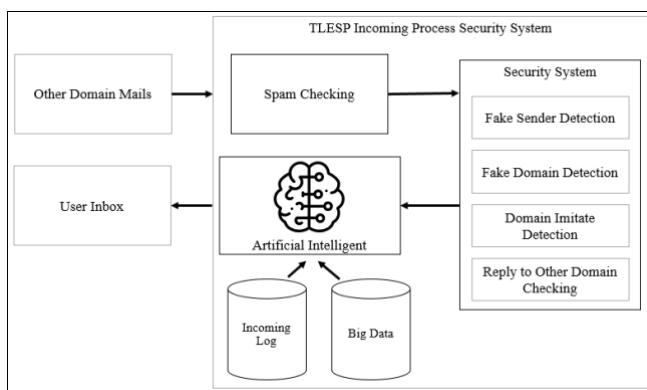


Figure 1. Incoming process diagram of TLESP system

In fact, the original system of TLESP has main problems in outgoing process about the clients’ email account were hacked and used in sending large amount of spam or pretending to be client and subrogate to be client then fraud the business partner. Also, it caused the blacklisting of TLESP from other

domains, these were an urgent and important problems that must be fixed. The TL organization has improved the outgoing process security to be more secure and provided protection system for preventing from outgoing process problems. Figure 2 displays the overall process of the outgoing process security of the email provider server. With the smart analysis from AI that can examine the unusual behaviour from sender before the mail will be sent out to other domain servers, for example, sender location IP checking to prevent from hacker assessing client’s account from different country. Additionally, the AI can provide a real-time protection to the server system for blocking the spammer or hacker email account from trying to attack the server and client account. Besides, the TLESP system also provide security system functions apart from sender IP checking as the follows, the detection of sending mail from many devices in the same time, behavioural historical data analysis which compare the client behaviour since the past before sending the mail, checking the destination account whether it is the first time contact or not, and checking the amount of the mail that will be sent if the amount is more than the limit or more than unusual amount.

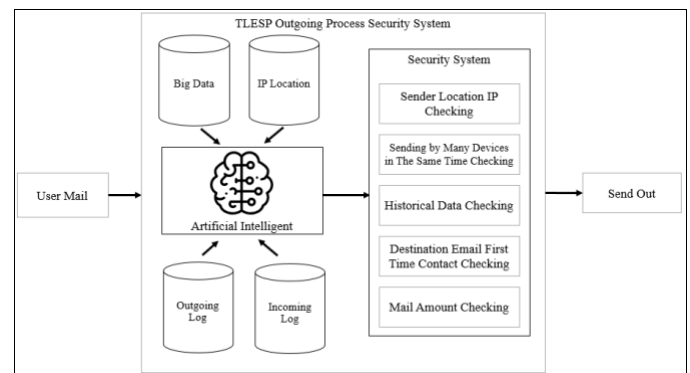


Figure 2. Outgoing process diagram of TLESP

## IV. ANALYSIS AND RESULTS

### A. System Results

From the improvement of the TLESP system in the security protection which can prevent spammer of both TL’s clients and other domain users, also avoiding the blacklisting of TL by other email provider domains. The TL organization discovered that using the new TLESP system for 3 months long and found that the new TLESP system can protect and prevent spam users in many ways, the TL outgoing security can provide a better system for preventing spam users. There are about over 100,000 active users in the TLESP system. The system has blocked about 862 user accounts, which over 344,800 spam mails are considered as spam mails and they would be sent out to other domains which could be spam mail or hacker mail. Originally, the email limit system of old TLESP usually limits the email sending amount for 400 mails/user daily, and with this limit system the enormous amount of spam would be sent and it may result in negative

effects for the clients without the real-time protection of the TLESP system.

### B. Client Benefits

As the new system has been released to the clients' organization, the client can receive a safe email system to use within the organization and reassure from the virus, spam mail, and blacklisting server in the TLESP. The client's organization of TL has been asked to give satisfaction scores (out of ten) in the security system both before and after the improvement of the TLESP. As shown in Table 1, the satisfaction scores before system improvement ( $M = 5.22$ ,  $SD = 1.52$ ) were lower than the clients' satisfaction scores after system improvement ( $M = 7.86$ ,  $SD = 1.24$ ). Also, Figure 3 shows the clients' satisfaction in the comparison between before and after system improvement.

TABLE 1. SATISFACTION SCORE COMPARISON TABLE

| Group  | N  | Mean | SD   |
|--------|----|------|------|
| Before | 44 | 5.22 | 1.52 |
| After  | 44 | 7.86 | 1.24 |

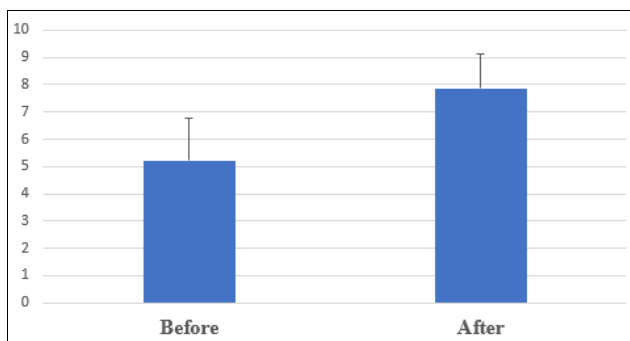


Figure 3. Clients' satisfaction scores before and after system improvement comparison

## V. CONCLUSION AND RESULTS

### A. Summary

In summarization, this study provides the methodology and ideas for the email service provider to use artificial intelligence for checking the incoming and outgoing process of the email provider server. Including giving the ideas about solving the email spammer, hacker, virus, and blacklisting in the email provider context, which these mention problems are some of the factors that can cause more or less damage to the email service provider around the world. Based on the questionnaire and system results, this study shows that there had been an increase in clients' satisfaction toward the improved version of the email system, and the method uses in this study can provide a more secure email provider system.

### B. Discussion

The results of this study indicate that the application of artificial intelligence can provide a high-security system to the email service provider system. Also, the high-security system can make the clients have more confidence and satisfaction toward the email provider system.

### C. Recommendation and Guideline

The recommendation in this study for future researchers, the proposed system about artificial intelligent security could be applied in various contexts besides email service providers, for example, e-commerce security systems, online course security systems, financial database security systems, etc. Moreover, it can proceed with the complex data and take an action immediately without delay and hesitation for preventing the occurring damage over time to the organization and clients [7].

### D. Limitations and Future Study

As the reason that this study is a study from a business organization, the information in some parts is confidential and cannot be revealed to the public community. However, the complex of artificial intelligence has consumed quite some time to be developed, but the damage that has been occurred over time. The organization must solve the problems against time to prevent further damage in both the TL organization and clients' organization.

## REFERENCES

- [1] T. Herath, R. Chen, J. Wang, K. Banjara, J. Wilbur, and H. R. Rao, "Security services as coping mechanisms: An investigation into user intention to adopt an email authentication service," *Inf. Syst. J.*, vol. 24, no. 1, pp. 61–84, 2014.
- [2] M. Jakobsson, "Understanding social engineering based scams," *Underst. Soc. Eng. Based Scams*, pp. 1–130, 2016.
- [3] B. Coskun, "(Un)wisdom of crowds: Accurately spotting malicious ip clusters using not-so-accurate IP blacklists," *IEEE Trans. Inf. Forensics Secur.*, vol. 12, no. 6, pp. 1406–1417, 2017.
- [4] N. Agrawal, "Detection and Spam Mail Filtering Approach," in *2016 Third International Conference on Digital Information Processing*, 2016, pp. 99–104.
- [5] Z. Wang, M. Qin, M. Chen, and C. Jia, *Hiding fast flux botnet in plain email sight*, vol. 239. Springer International Publishing, 2018.
- [6] G. Mujtaba, L. Shuib, R. G. Raj, N. Majeed, and M. A. Al-Garadi, "Email Classification Research Trends: Review and Open Issues," *IEEE Access*, vol. 5, no. c, pp. 9044–9064, 2017.
- [7] E. G. Dada, J. S. Bassi, H. Chiroma, S. M. Abdulhamid, A. O. Adetunmbi, and O. E. Ajibuwa, "Machine learning for email spam filtering: review, approaches and open research problems," *Heliyon*, vol. 5, no. 6, 2019.
- [8] T. Gangavarapu, C. D. Jaidhar, and B. Chanduka, *Applicability of machine learning in spam and phishing email filtering: review and approaches*, vol. 53, no. 7. Springer Netherlands, 2020.
- [9] J. Golbeck and J. Hendler, "Reputation Network Analysis for Email Filtering," *Proc. 1st Conf. Email Anti-Spam*, no. July 2004, 2004.
- [10] G. Kim, B. Shin, and H. G. Lee, "A study of factors that affect user intentions toward email service switching," *Inf. Manag.*, vol. 43, no. 7, pp. 884–893, 2006.
- [11] H. Lee, A. Girish, R. van Rijswijk-Deij, T. Kwon, and T. Chung, "A longitudinal and comprehensive study of the DANE ecosystem in email," *Proc. 29th USENIX Secur. Symp.*, no. 3, pp. 613–630, 2020.
- [12] Y. Cohen, D. Gordon, and D. Hendler, "Early detection of spamming accounts in large-scale service provider networks," *Knowledge-Based Syst.*, vol. 142, pp. 241–255, 2018.



**Rattanachai Wongwatkit** is a founder and programmer of the Technology Land Co., Ltd. in Bangkok, Thailand. He is an expert which has over ten years' experience in email security and large-scale email system design that can support a huge number of users. He is guaranteed and certificated by an institution in Netherland.



**Montree Raktham** is currently a programmer of the Technology Land organization in Bangkok, Thailand. He has expertise in Big Data and Artificial Intelligence for email security safety processing.



**Thanadet Phawananthaphuti** is an expert in email system design that can handle a large number of users with node balance technology, and Mail Server installing for safety using. Currently, he is a system engineer at the Technology Land Co., Ltd.