Electronic Preprint for Journal of Information Processing Vol.27

Regular Paper

Helping Johnny to Search: Usable Encrypted Search on Webmail System

Tatsuya Midorikawa[1] Akihiro Tachikawa[1] Akira Kanaoka[1,a)]

Received: March 12, 2019, Accepted: September 11, 2019

Abstract: End-to-end encryption is becoming common in messaging applications. E-mail that is the one of most popular a messaging application has several standards and systems in its encryption. However, it is hard to say that e-mail encryption has spread enough. It has been pointed out that there are usability problems in message encryption. Even though various studies on message encryption and usability have been made, there is no study discussing utility function such as searching and sorting. In this paper, the search function is focused. We aim to investigate the usability problems on encrypted search. Therefore, a method that applies encrypted search transparently is proposed at first. The implementation of the proposed method is achieved using Google Chrome Extension for Gmail, and evaluation both performance and usability is conducted. We found that participants do not mind whether the search function is encrypted or not if both have almost identical UI and encrypted search operates at high speed.

Keywords: usable security, e-mail encryption, searchable encryption, encrypted search

1. Introduction

E-mail encryption has been a long-standing issue of usable security. After Whitten and Tygar have opened a new vista in usable security for e-mail encryption [1], there were many following studies which enhance the usability [2], [3], [4]. Finally, Ruoti et al. have achieved automatic e-mail encryption using Identity-based Encryption (IBE) without S/MIME and PGP [5]. Such automatic or transparent encryption has become common in various messaging tools, such as Whatsapp, Facebook Messenger, and LINE. As end users come to reach maturity, end-to-end encryption has come to be widely accepted.

In the e-mail application, there are various utility functions for messages other than sending and receiving. A typical function would be the search. Also, sort multiple data and sharing data with multiple users will be significant utility functions. It also has the function of detecting phishing sites and judging inappropriate advertisement as a security function. From the viewpoint of usability, it is desirable for users to be able to use these utility functions as before even if the e-mail itself is encrypted.

This paper focuses on search function from such utility functions for e-mail. In the current search system, the search index is prepared for messages in order to achieve a high-speed search. Even if e-mails are encrypted, information leaks will occur in its search index that includes partial e-mail contents information in plain text. As a countermeasure, there are encrypted search (or searchable encryption) techniques.

Encrypted search allows searching in an encrypted manner without leaking any information about e-mail contents, such as an encrypted index. Various studies have been actively studied in the encrypted search field. Encrypted search is one of the most promising techniques. However, it has never been discussed in the usability point of view. Therefore, we put the research questions as follows.

RQ1: Is it technically possible to simultaneously realize client-side encryption and secure search functions in e-mail services?

RQ2: If the above is possible, is the application or service usable?

In this paper, the first look at the usability of encrypted search is given. At first, a method that enables encrypted search transparently is proposed with the goal of achieving a transparently available environment, as Ruoti et al. have achieved e-mail encryption transparently. Our proposal achieves secure and usable webmail that can apply an encrypted search technique on the browser side and can closely cooperate with existing webmail services. Then, we make a prototype and evaluate the proposed method. The evaluation consists of two methods: Performance of encrypted search especially on encrypted query generation and encrypted search, and conducting user study using actual environment using the prototype browser extension. In the user study environment, a new encrypted index server using Symmetric Searchable Encryption (SSE) technique is built for server side. A Google Chrome extension for SSE that generates an encrypted query and communicate with the SSE server, is also prepared as for end-user side. It enables SSE without changing current Google Gmail service. The user interface of the end user side is almost identical in the Gmail service.

As a performance result, it shows acceptable levels of performance that takes about 1 msec for generating an encrypted query and about 180 msec for one searching with an index of 10,000 e-mails. The result of usability evaluation shows there are equiva-

[1] Toho University, Funabashi, Chiba 274–8510, Japan
[a)] akira.kanaoka@is.sci.toho-u.ac.jp

lent between regular Gmail and proposed method applied system.

On the other hand, some interesting reactions are given. For example, similar to the results of Ruoti et al. [5] and Fahl et al. [6], some users still expect that randomized string on the user interfaces as encrypted contents.

Our contribution is giving discussions on the usability point of view which is made for the first time in the field of encrypted search. Moreover, it shows that encrypted search can be applied without vitiating usability.

The structure of this paper is as follows. In Section 2, we will explain relevant research, and explain the encrypted search to existing webmail system in Section 3. In Section 4 we describe the evaluation methodology, and its results will be described in Section 5. In Section 6 we will discuss restrictions and future work in this research and this experiment. Finally, it is summarized in Section 7.

2. Background

2.1 Secure E-mail and Usability

Whitten and Tygar conducted a user study of e-mail encryption for the first time [1]. This paper is a representative paper mentioned for effective user interface focused on security. It pointed out that the cause of the failure in most of the computer security as a thing due to an error of the user. It also pointed out that the user interface is confusing and unwieldy for security, or does not exist.

They argued that there is a need for different usability from standard one, and user interfaces suitable for other software cannot resolve these problems.

Therefore, user study has been conducted for PGP 5.0, which is reputed and have a good user interface for security at the time. They revealed there are defects in the user interface from experimental result and usability for security defined in the paper.

Although this paper studied the usability of PGP 5.0, it also brought the pioneering concepts for the field of usable security. The impact of this paper is significant, such as definitions for usability of security, properties associated with security, and user study procedure. After this paper, many successor studies were published. Also in addition to the encryption field, this paper also is the cause of usability research in the wide range of the security and privacy field, called as usable security and privacy.

Garfinkel et al. conducted a questionnaire analysis for PEM, PGP and S/MIME on 470 people who sell goods on Amazon.com [2]. As a result, it was claimed that the majority of participants could use digitally signed e-mail. Further, Garfinkel et al. conducted a user experiment on e-mail encryption in a similar approach as Whitten and Tygar, intended for S/MIME [3]. They have pointed out that things showed in the paper of Whitten and Tyger can be applied to a wide range.

Sheng et al. compared with PGP9 against PGP5 [4]. In the study, several tasks were given to participants: key pair generation, acquisition and verification of public key, encryption and decryption of e-mail, sign and verify of a digital signature, and store and backup of key pair.

In 2013, an entirely different approach for usable e-mail encryption had been proposed by Ruoti et al. They proposed a secure webmail Pwm (Private WebMail) using an overlay for tightly integrated with existing Webmail service like Gmail [5]. It achieves transparent encryption which does not require users to manage keys and operate encryption and decryption. In other words, encryption/decryption and key management are performed automatically. It shows the effect of prevention of incorrectly sending an e-mail in plain text and the trust of Pwm.

As pointed out also in that paper, the most notable point is another experiment to use customized Pwm (Message Protector, MP) that requires several actions for encryption and decryption. As a result of another experiment, these extra steps, such as cutting and pasting ciphertext, was accepted to participants. Furthermore, it obtains higher trust than original Pwm.

These results suggested that there is a need to rethink the design of such transparent e-mail encryption system. Ruoti et al. have achieved a lot of improvement result after the paper [7], [8].

After Snowden leaks, since the use of end-to-end message encryption has spread and such transparent encryption has come to be accepted to end users, we can see the maturity of end users about end-to-end message encryption. The result of Bai et al. supports them [9]. In order to perform transparent encryption, the facilitation of key management is essential. Therefore, many users have recognized the security problem of Key-Registration Encryption System employed at many major systems like Facebook Messenger, Whatsapp, and LINE, but have accepted the system.

It can be said that the foundation of transparent encryption has been sufficiently grown up.

Unger et al. discuss in deeper about secure messaging [10].

2.2 Search Index

In this section, we show a general view of current data contents of typical search index. To achieve search function in softwares and services, search index is usually used for efficient search. If these indexes are not protected, information of data contents can be leaked regardless of data contents encryption.

In Mozilla Thunderbird, message indexing and search system “Gloda (Global database)” which is implemented using SQLite, is used. In the technical documents of Gloda, there is no description about index data encryption and protection [11]. In Microsoft Outlook, Windows search system is used. In the technical documents of Windows search system, it described that the protection of index is based on access control list and light obfuscation [12].

In Apache Lucene which is an typical open source full-text search engine, the contents of index files is described in detail in the official technical documents [13]. We can see that partial plaintext information about messages is easily obtained from the index files.

Even though these systems achieve high-performance search system, it is hard to say that they have strong protection mechanism for search index.

2.3 Encrypted Search

Encrypted Search or searchable encryption is divided into two categories: Searchable Symmetric Encryption (SSE) and Public Key Encryption with Keyword Search (PEKS).

In SSE, practical scheme of searchable encryption has been proposed by Song et al. for the first time [14]. After a lot of following studies [15], [16], [17], [18], [19], [20], [21], [22], it has become a practical technique. Thus, it has come to support a variety of functions: multi-keyword SSE [23], arbitrary boolean function [21], ranked search [24], k-NN scheme [25], fuzzy search [26], [27], and wild-card [28], [29]. A survey of Poh et al. [30] is helpful to overview SSE.

Compared to SSE which is a single reader and single writer model, PEKS gives several models like Multiwriter and Multireader. PEKS is first proposed by Boneh et al. [31], then have a variety of models have been proposed. Since SSE is used in implementation in this paper, a detailed description of PEKS is omitted. A survey of Bösch et al. [32] is helpful to overview PEKS.

3. Encrypted Search to Existing Webmail Systems

In this section, the basic approach to applying encrypted search to existing webmail systems and our proposal are described. Firstly, the basic approach is described on Section 3.1, then our proposal follows.

3.1 Basic Approach

There are two approaches to applying an encrypted search to a webmail system. First one is a method for improving the system itself. The other one is a method for add-on functionality without changing the existing system. Since add-on function is applicable without the need to improve an existing system substantially, it is applicable to webmail systems used already in many scenes. This approach has excellent practicality. Pwm which perform transparent e-mail encryption has adopted this approach. In our paper, a method for applying encrypted search to existing webmail system by adopting this approach.

Encryption of the e-mail itself is performed independently of the proposed system. Therefore, the proposed method does not matter whether the e-mail encryption algorithm or method is used.

3.2 Proposed Method to Add Encrypted Search Function into Existing Webmail Service

In webmail systems, webmail users access to webmail server from browser, then send, receive, view, and search e-mails (**Fig. 1**).

If we want to apply encrypted search here, it is difficult to use the APIs and data of existing webmail server directly. Encrypted search dedicated server is prepared to solve this problem. The encrypted search server holds the search index. Encrypted e-mails are stored in the current webmail server. Each e-mail is assigned with a unique ID, and the ID is included in title, header, or body in plain text, even e-mail contents itself are encrypted. In the encrypted index, the keyword with each of mail content is stored. Each keyword has bound to e-mails which have the keyword. Webmail user side firstly creates an encrypted search query, then send the query to the encrypted search server. Encrypted search server searches using a received encrypted search query, then returns obtained IDs to the webmail user. The webmail user side

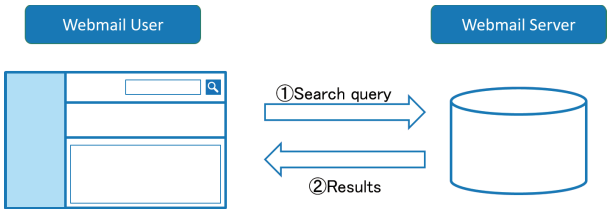

Fig. 1 Normal webmail system model.

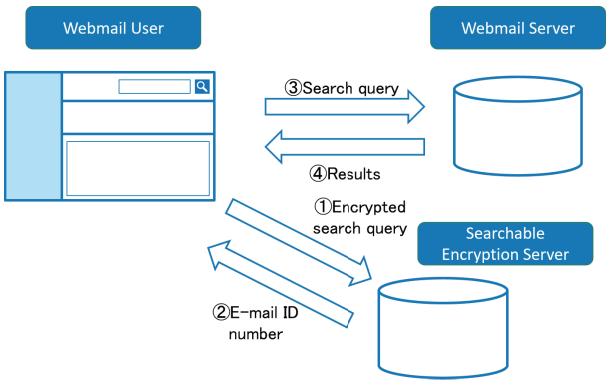

Fig. 2 Proposed model.

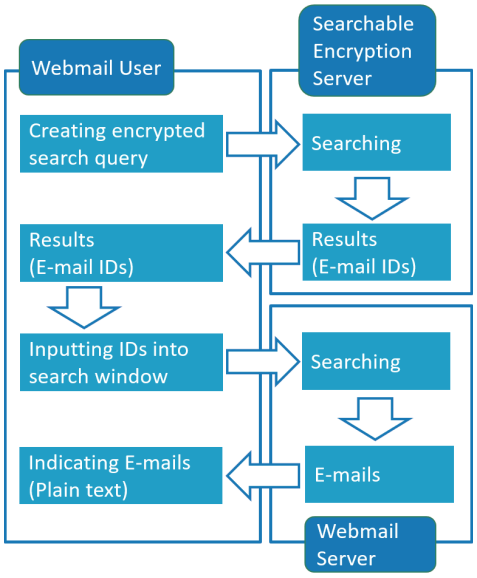

Fig. 3 Flow of proposed model.

which includes user and applications, browser extentions) then makes a query of OR search using received e-mail IDs, and send the query to webmail server. As a search result from the webmail server, e-mails which include IDs on the titles are returned to webmail user. The webmail user side decrypts (if it is encrypted) and displays them. In this way, an e-mail system which enables an encrypted search can be achieved. The relationship diagram for each entity is shown in **Fig. 2**, and the flow of search is also shown in **Fig. 3**.

This model is based on the assumption that e-mail contents are encrypted, but in order to achieve the utility function, the proposed method aims to implement a search using an encryption index. While e-mail encryption is expected from the start, the model itself is independent of whether e-mail encryption is in place.

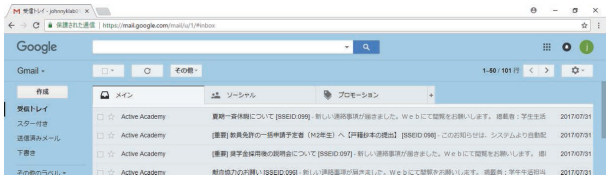

Fig. 4 User interface on standard Gmail.

Fig. 5 User interface on improved Gmail (Gmail+SSE).

3.3 Developed System for Evaluation

For use in the evaluation, a prototype system of the proposed system is developed.

Google Chrome which can easily add functionality using Chrome Extension is selected for the client side. Moreover, Gmail which is one of the most popular e-mail services and enables OR search is selected for existing email service.

3.3.1 Encrypted Search Method

Curtmola's SSE1 [17] is implemented in the system. For server side, *Search* function, and web server function are developed using Java language. For client side, *Trapdoor* function is developed using JavaScript.

3.3.2 Google Chrome Extension

A prototype chrome extension is developed to enable encrypted search on the client side. It hooks user input on the Gmail search window. When a user pushes the search button, it obtains the value on the Gmail search windows. Then it calculates the encrypted search query, then send the encrypted query to the SSE server. After receiving results (E-mail IDs) from the SSE server, it generates a query for Gmail using E-mail IDs, and send the OR query to Gmail Server. Finally, after receiving a result from the Gmail server, it decrypts all e-mails on the results then show to a user.

User interface of original Gmail and the proposed system which is Gmail adapted with developed extension, are almost identical (**Figs. 4**, **5**). Magnifying glass icon was omitted from Gmail+SSE, and a simple lock icon was shown next to the URL bar.

4. Evaluation Methodology

This section gives an overview of our experimentation for evaluating our proposed system. In the experimentation, performance evaluation and user study are conducted.

4.1 Hypothesis

Following the result by Ogata et al. [20] which shows good performance of SSE, we hypothesize the followings:

(1) Generating encrypted query (*Trapdoor*) on a browser and searching (*Search*) on SSE server is acceptable and unaware of additional action

(2) There is no difference in user awareness between original Gmail and the proposed encrypted search system without e-mail contents encryption

To test the hypothesis, we conduct performance evaluation and user study.

4.2 System used for the Evaluation

The evaluation system is applied the system described in Section 3.3.

There are several evaluation objects to evaluate the proposed system. For example, it is conceivable to compare a system that encrypts e-mail contents without search function, such as Pwm 2.0, with a system that further incorporates our proposed method into Pwm 2.0. In this case, the usability evaluation results of the Pwm 2.0 itself and the usability evaluation of our proposed system are likely to be mixed. And the evaluation is difficult to separate. Therefore, in order to evaluate the usability of our proposed system, we thought it would be appropriate to compare it with the original Gmail, which is most familiar to the participants of the experiment. In the evaluation system, the e-mail contents in Gmail is not encrypted, but only the search information was encrypted.

The evaluation system also requires a independent SSE server for the Gmail service and the Google Chrome extensions on the client. It was set up in our organization. Access information to the SSE server was pre-configured in Chrome Extensions.

4.3 Performance Evaluation

The purpose of the performance evaluation is giving information to discuss usability between original Gmail and the proposed system (Gmail+SSE) whether the performance effect to the usability. Performance evaluation is conducted independently from the following user study.

We prepare an environment for performance evaluation as follows. For the client side, a Windows 10 PC which Intel Core i5-6200U (2.30 GHz), 8 GB RAM, Google Chrome 63 (63.0.3239.84), is used. Also, a Linux (Ubuntu 16.04) machine which Intel Core i3-3220 (3.3 GHz), 6 GB RAM, OpenJDK 1.8.0_151, is used for the server side.

In Curmola's SSE, since the size of the index is changed mainly by the number of documents (E-mails), three types of e-mail nums (100, 10000, 10000) are prepared. E-mails are randomly chosen from Enron Email Dataset [33]. Searching is performed 100 times. *Trapdoor* function execution time and *Search* function execution time are measured. 128-bit AES is chosen for a symmetric encryption scheme within Curtmola's SSE.

4.4 User Study

4.4.1 Study Setup

The study ran from July 18, 2017, to December 18, 2017, and included 13 participants that were randomly assigned to test either standard Gmail or the proposed system (Gmail+SSE) that applied encrypted search. In the study, we did not encrypt e-mail contents itself to avoid performance and usability difference by e-mail encryption and decryption and focus on encrypted search evaluation only.

The recruitment was carried out on the university's webmail

and campus bulletin board.

Participants took about 30 minutes to complete the study and were compensated 500-yen worth of book cards for their efforts.

As far as seeing the papers doing user studies, remuneration in the United States paper was around $10 per hour [5]. After that, it changed from 15 to 20 dollars after raising the minimum wage to 15 dollars [7], [8], [9]. The minimum wage per hour in that country seems to be a base of remuneration amount. Therefore, the minimum wage in Chiba prefecture was 842 yen at the time of the user study [34] and the experimental time was 30 minutes, we decided that 500 yen close to half of the hourly wages of the minimum wage was reasonable as a reward.

Studies were conducted in a room dedicated to this study. When participants first entered the room, they were given out a study manual and received a description to the study. All tasks were written on paper, and answers were written on the paper. Also, in order to analyze the behavior of the participant more deeply, we recorded a video of the experiment.

This experiment was approved by the Internal Review Board (IRB) of our university.

4.4.2 Demography

We have 13 participants in total. Ten are male, and three are female. All participants are a bachelor or master course student of the faculty of science. **Table 1** shows demography of participants.

4.4.3 Scenario and Task Design

During the study, participants were given a role becoming a student of a university, and one scenario to complete searching for e-mails received in the past. We prepared e-mail data for the user study as natural as possible and designed realistic tasks. Participants were provided e-mail account during the study and conducted tasks using this e-mail account.

4.4.3.1 Role Playing

Participants were a student of a university and forwarded all e-mails from the university's Webmail system to Gmail. Usage of e-mail is all done with Gmail.

4.4.3.2 Task

The task for participants is searching for e-mails containing specific keywords from e-mails received in the past, and writing the result on the answer sheet. There are five keywords to find out, and all the keywords are described on the answer sheet.

4.4.4 Study Questionnaire

After finishing tasks, semi-structured interview is conducted. Questionnaire of System Usability Scale (SUS) is used to the interview, and addition to the SUS questionnaire, the following questions were asked.

- Do you have experience with Gmail?
- How often do you use Gmail?
- Have you ever considered message sensitivity on messaging tools, such as Facebook messenger or LINE?
- Do you know Facebook messenger and LINE are already encrypted all messages by default?
- Where do you think the information leaked when your information is leaked?
- Did you feel the stress during tasks?
- Did you recognize that the e-mail contents are encrypted?

Table 1 Participants.

	Gender	Grade	Department
p1	Female	4th, Bachelor	Biomolecular Science
p2	Female	4th, Bachelor	Biomolecular Science
p3	Male	4th, Bachelor	Information Science
p4	Female	4th, Bachelor	Biomolecular Science
p5	Male	2nd, Bachelor	Information Science
p6	Male	2nd, Bachelor	Information Science
p7	Male	2nd, Bachelor	Information Science
p8	Male	1st, Master	Information Science
p9	Male	1st, Master	Information Science
p10	Male	2nd, Master	Information Science
p11	Male	2nd, Master	Information Science
p12	Male	4th, Bachelor	Information Science
p13	Male	2nd, Master	Information Science

- Did you recognize that the search keywords are encrypted?

4.4.5 Usability Analysis

To analyze the usability of the proposed method, we conducted qualitative analysis using Grounded Theory Approach (GTA) from interview results and behavior during the study and prior orientation. GTA is common method to evaluate usability qualitatively in usable security and privacy field [35], [36], [37], [38], [39], [40], [41], [42], [43], [44], [45], [46], [47]

5. Evaluation Results

From performance evaluation and Usability evaluation, we found the result shows there is equivalent between regular original Gmail and a proposed system (Gmail+SSE).

Next, we discuss these findings in detail based on performance result and categories derived from GTA.

5.1 Performance

Performance evaluation is conducted independently from a user study. The purpose of the performance evaluation is giving information to discuss usability between Gmail and Gmail+SSE whether the performance affects usability.

Index size of each types is shown in **Table 2**, and performance result of each function and types is shown in **Table 3**.

Even index size is more extensive, the performance of *Trapdoor* and *Search* seems acceptable level for end users. Each value is about less than 100 msec, and it means that end users might feel an instantaneous response. Its value is from "Response-Time Limits" by Jakob Nielsen [*1].

This result supports the first hypothesis.

5.2 Categories Derived from GTA

GTA was conducted based on the questionnaire answer and behavior during the study. The total number of codes are 52 including duplication. Then 8 categories were classified.

A list of obtained categories is shown in **Table 4**.

5.2.1 Gmail Experience

All participants answered that they had experience of using Gmail. Many participants were not from the website but the app. Besides, many participants use it for service registration of shopping sites and receiving direct mails. It can not be said that they are used daily and familiar with the usage.

[*1] https://www.nngroup.com/articles/website-response-times/

Table 2 Average E-mail Size and Index Size of Curtmola's SSE.

# of e-mails	Avg. E-mail size (KB)	Size (MB)
100	1.18	6.3
1,000	1.87	88.1
10,000	2.01	941.7

Table 3 Performance of *Trapdoor* and *Search*.

# of e-mails	*Trapdoor* (ms)	*Search* (ms)
100	1.30	65.93
1,000	1.76	66.61
10,000	1.57	179.66

Table 4 Categories obtained as a result of GTA.

Gmail Experience
Mention about Information Leakage
Knowledge of End-to-end Encryption
Search
Preception of Search Keyword Encryption
Usability of the Proposed System
Stress
Others

p2: "I hardly use Gmail from the site. I usually use from the application of my iPhone."
p3: "I do not use it much recently. I made only an account."
p7: "I use it for shopping and registration of sites. I'm using from the app."
p10: "I used for site registration and job hunting."
p13: "See in the app about three times a week. The mail of Yahoo is being forwarded."

5.2.2 Mention about Information Leakage

The responses of all participants to information leakage were mentioned in terms different from the purpose of the study. When many participants heard about information leakage of e-mail, they thought the leaked information was not an e-mail text but an e-mail address. Although there was an answer that seemed to contain the e-mail text as well, only one participant who assumed a leak due to the service company being attacked or wiretapping were considered.

p1: "When I look at the news, I think that a company providing e-mail service or an individual is infected with a virus and leaked on the Internet."
p2: "Website. For example, when searching on the net, you get a virus and from there."
p8: "Password is leaked. It is stolen when sending and receiving messages."
p10: "System vulnerability. A password is weak."

In addition, regarding the information leakage route, their opinions tend to that it was not the problem of the system, but the information was leaked by infection with a site such as a phishing site or a virus. As seen in p1's answer, the influence of the media is considered to be large.

From these results, it is considered that the necessity of content encryption or the threat what we assumed as a threat model is not conscious.

5.2.3 Knowledge of End-to-end Encryption

Most of the participants answered that they did not care if the text or message of the mail, LINE or Facebook messenger was encrypted. Also, most participants did not know that LINE and Facebook messengers had their messages encrypted by default.

Only one participants know the LINE encrypts messages [*2].

p2: "Encryption...Yes. I know that. When I opened configuration of LINE to store specific messages, I saw an item named "Encryption". So I realize they have some mechanism of encryption somewhere in LINE app".
p6: "I do not know in detail. I thought it was encrypted. Maybe it's not good that the message is not encrypted. I think that encryption is done, but I have not actually investigated it."
p10: "I know. I think that it is strange that it is not encrypted."

p2 knew that there was a system called encryption, but did not know detailed information such as which information was encrypted. Also, it can be seen from the answers of p6 and p10 that performing encryption is obvious or that it is a problem if it is not encrypted.

From these answers, there were those who knew that they were encrypted and those who did not know it, but they did not recognize the detailed contents such as where is specifically encrypted.

5.2.4 Search

Several participants mentioned the search function.

p10: "If you just search, you don't need support. But I do not know the contents."
p11: "You may not get what you want when you miss to use search keywords."
p13: "PC beginners and others have a difference in searchability. Whether OR or AND search."

From these facts, the use of ordinary search functions such as single keyword search can be used without the support. However, in order to perform an advanced search such as OR search and AND search, it is necessary to support technicians. Moreover, although this system only supports single keyword search and multiple keyword searches cannot be performed, the demand for more advanced search functions such as multiple keyword searches can be considered from these facts.

5.2.5 Perception of Search Keyword Encryption

Most participants did not perceive encryption of search keyword regardless of Gmail or Gmail+SSE.

Although a few participants felt strange, it was originated from original index data.

p2: "I was told it was encrypted because I received an explanation, but I did not feel it at all at the stage of use."
p7: "Does it mean that the search keyword was not caught? It was displayed that there were 50 problems. I felt if that was the case."
p10: "I recognized it because it was explained, but I didn't care."
p13: "I recognized it because I received the explanation, but I did not feel it."

There were participants who felt something strange because

[*2] LINE is popular messaging tool in Japan.

e-mails without search keywords were displayed in the search results. However, this problem is an Apache Lucene problem used to create an index for e-mails, not an essential problem of searchable encryption.

What we have to think about here is whether or not it was due to the explanation that the feeling of incongruity was applied to the new function. Temporarily, if it is what was explained, it will be solved by applying transparently. This issue is mentioned in the paper [5] published in 2013. In this paper, it is stated that the user is confused when encryption of e-mail is fully transparent. However, it is fully conceivable that the usability of searchable encryption can be improved by making it transparent from the key management model mentioned in the paper [9].

5.2.6 Usability of the Proposed System

When we asked about the usability, all participants answered that they were easy to use and did not change as usual. However, there were the following opinions.

p1: "If you have to install software etc. in order to use it, just a little .... I don't know much about PC. If I can easily install."

p12: "People who are not familiar with the computer may not know how to use it. I think it's fine if you are a university student."

From the opinion of p1, not only the ease of use of the service but also the ease of installation can be considered to affect the ease of use. In addition, it is possible that differences in knowledge about personal computers affect the ease of use from the opinion of p12.

5.2.7 Stress

Many participants answered that they did not feel stress whether the encrypted search is applied or not.

p3: "There is only one case. When I search for a specific keyword, it also shows in the result that the search keyword is not included."

p13: "There was stress on keywords. For example, search the graduation ceremony by "graduation.""

Reasons for the stress of these participants are stress against the content of the index or task created when applying the searchable encryption. It was not stressed for applying searchable encryption.

5.2.8 Others

The following answers were obtained as other opinions.

p5: "I heard that it was encrypted, so I thought it was a common mess that I didn't understand, but I could read it properly."

p6: "I use Gmail only for registration. I do not send personal information at all. I will only send safe information."

One participant mentioned the user interface of messaging encryption. While the participant p5 only thought that a randomized string would be displayed when the message was encrypted, other participants did not mention that. The look & feel that displays such random strings as an encrypted text is also shown in the Ruoti et al. study [5] and the Fahl et al. study [6]. Transparent end-to-end encryption is considered to be generalized since only one participant mentions this.

Table 5 System usability scale results.

Participant	Service	SUS Score
p1	Gmail+SSE	80
p2	Gmail	95
p3	Gmail+SSE	67.5
p4	Gmail	85
p5	Gmail+SSE	87.5
p6	Gmail	100
p7	Gmail+SSE	72.5
p8	Gmail	72.5
p9	Gmail+SSE	80.0
p10	Gmail+SSE	62.5
p11	Gmail	87.5
p12	Gmail+SSE	75.0
p13	Gmail	82.5

Table 6 System usability scale scores.

Service	Mean	SD
Gmail	87.1	8.83
Gmail+SSE	75.0	7.79
Overall	80.6	10.20

From the opinion of p6, we can see there is a recognition that messaging tools exchange more sensitive information such as personal information than e-mail.

5.3 System Usability Scale Results

Interviews were conducted using SUS questions. Therefore, the score of SUS can be calculated. However, since the number of participants is 13, which is not suitable for quantitative evaluation, the SUS score is presented here as a supplementary discussion and is not adopted as a conclusion of the usability results itself.

We evaluated the proposed system (Gmail+SSE) that applied an encrypted search using the System Usability Scale (SUS). Original Gmail had a SUS score of 87.1, and the Gmail+SSE had a SUS score of 75.0. Details of the SUS scores obtained from our study can be found in **Table 5**.

6. Discussion

6.1 Number of Participants

In this study, there were as few as 13 participants, which was insufficient for quantitative analysis.

According to Nielsen et al., It is analyzed that 85% of usability problems can be found by conducting a subject experiment with five people [48]. Since the experiment conducted in this study is related to security and is an experiment using a web browser as a platform, it is not necessarily consistent with the demonstration results of Nielsen et al. There were six participants in the Gmail system and seven in the Gmail + SSE system. Both have more than five users, so if one of them has usability problems, it can be expected to find them through interviews. Therefore, the number of subjects is not small.

6.2 Performance of Search System

For the question "Do you feel stress in searching mail?", the answer p3 "Emails without search keywords was also displayed in search results" is interesting for future studies. The fact that e-mail without search keyword was displayed is a matter of Lucene used when creating indexes and is not an essential problem of

searchable ciphers. However, it is a problem to be improved in the future.

6.3 Key Management

Also, the problem of key management is a big problem in the future. In Ruoti et al.'s Pwm, the private key is issued by the server and the key is received. In 2016, the paper published by Bai was discussed this problem [9]. This paper conducted comparison studies on usability of key exchange model which manages keys among users and key registration model which registers keys to a server. An interesting result of this study is that the participants understand the potential risk of the key registration model, recognize that the key exchange model is safer, but answer that the key registration model is sufficient for the daily purpose. From this, key registration model service can be considered for implementing services for our proposal.

6.4 Application for Existing Webmail Services

The chrome extension created in the paper applies searchable encryption to Gmail and does not support other webmail systems. However, it is desirable to be able to apply searchable encryption not only to Gmail but also to other webmail systems considering practical use. The following comments were also obtained from semi-structured interviews.

> *p1: If you have to install software etc. in order to use it, just a little... I don't know much about PC. If I can easily install.*

From these things, it is considered necessary to automatically locate the search window and search button of the existing Webmail system and apply searchable encryption. Also, it is possible to consider semi-automation to apply searchable encryption by selecting search window or search button.

6.5 User Interface Differences

There were subtle differences in the user interface between the experimental system and the original Gmail (Fig. 4, Fig. 5). It should have been exactly identical, based on research questions or hypotheses for hypothesizes.

This difference in UI may cause bias in usability evaluation results. However, based on the results of the interview, none of the participants mentioned this UI difference, nor did they comment on it. Therefore, the effect of UI differences could not be said to be significant.

6.6 SSE Types

SSEs are classified into static ones that do not support deletion and insertion, and dynamic ones that support deletion and insertion. The SSE1 used in our evaluation system is classified as static. Static systems are not ideal for e-mail applications because they do not support deletions or insertions. Therefore, it is desirable that evaluation by dynamic SSE is carried out in future. There are various types of dynamic SSE, and it is conceivable that the performance is heavy depending on the level of security, etc., but there are also lightweight ones. For example, SimpleSSE in Ogata's proposal is a lightweight but dynamic SSE. Depending on the level of security required, the usability issue may not be significant if such a lightweight device is used.

6.7 Future Outlook

The following two problems exist as problems in applying searchable encryption to an existing Webmail system in practice. "When creating an index, the data must be in plain text." "When, who creates the index?" In order to solve this problem, two methods can be considered: "a method that can create an index in an encrypted state" or "a generation of index information each time it is encrypted." In order to realize these, technologies such as linkage with ID-based encryption and PEKS (Public Key Encryption with Keyword Search) can be considered, and it is necessary to study in the future.

7. Conclusion

In this paper, the usability of encrypted search is discussed for the first time. Firstly, a system that is integrated with an existing webmail service using an overlay technique and enables encrypted search transparently is proposed. Then, a prototype system is developed using Curtmola's SSE, like Google Chrome extension for generating an encrypted query and a server-side application for searching. Finally, performance evaluation and usability evaluation are conducted.

Our study indicates a high usability of searchable encryption.

In the system, it shows acceptable levels of performance that takes about 1 msec for generating an encrypted query and about 180 msec for one searching with an index of 10,000 e-mails. The result of usability evaluation shows there are equivalent between regular Gmail and proposed method applied system. For usability evaluation, semi-structured interview with System Usability Score (SUS) questionnaire is conducted with 13 participants, and Grounded Theory Approach (GTA) is used for qualitative evaluation of the usability. The result of usability evaluation shows there are equivalent between regular Gmail and proposed method applied system.

Our contribution is giving discussions on the usability point of view which is made for the first time in the field of encrypted search. Moreover, it shows that encrypted search can be applied without vitiating usability.

References

[1] Whitten, A. and Tyger, J.D.: Why Johnny Encrypt: A Usability Evaluation of PGP 5.0, *8th USENIX Security Symposium* (1999).

[2] Garfinkel, S.L. and Miller, R.C.: Johnnny 2: A User Test of Key Continuity Management with S/MIME and Outlook Express, *Symposium On Usable Privacy and Security* (*SOUPS*) (2005).

[3] Garfinkel, S.L., Margrave, D., Schiller, J.I., Nordlander, E. and Miller, R.C.: How to Make Secure Email Easier To Use, *SIGCHI Conference on Human Factors in Computing* (*CHI'05*) (2005).

[4] Sheng, S., Broderick, L. and Koranda, C.A.: Why Johnny Still Can't Encrypt: Evaluating the Usability of Email Encryption Software, *Symposium On Usable Privacy and Security* (*SOUPS*) (2006).

[5] Ruoti, S., Kim, N., Burgon, B., van der Horst, T. and Seamons, K.: Confused Johnny: When Automatic Encryption Leads to Confusion and Mistakes, *Symposium On Usable Privacy and Security* (*SOUPS*) (2013).

[6] Fahl, S., Harbach, M., Muders, T., Smith, M. and Sander, U.: Helping Johnny 2.0 to Encrypt His Facebook Conversations, *Symposium On Usable Privacy and Security* (*SOUP*) (2012).

[7] Ruoti, S., Andersen, J., Hendershot, T., Zappala, D. and Seamons, K.: Private Webmail 2.0: Simple and Easy-to-Use Secure Email, *Proc. 29th Annual Symposium on User Interface Software and Technology*

(*UIST '16*) (2016).
[8] Ruoti, S., Andersen, J., Heidbrink, S., O'Neill, M., Vaziripour, E., Wu, J., Zappala, D. and Seamons, K.: We're on the Same Page: A Usability Study of Secure Email Using Pairs of Novice Users, *Proc. 2016 CHI Conference on Human Factors in Computing Systems* (*CHI '16*) (2016).
[9] Bai, W., Namara, M., Qian, Y., Kelley, P.G., Mazurek, M.L. and Kim, D.: An Inconvenient Trust: User Attitudes toward Security and Usability Tradeoffs for Key-Directory Encryption Systems, *Proc. 9th Symposium on Usable Privacy and Security*, ACM (2016).
[10] Unger, N., Dechand, S., Bonneau, J., Fahl, S., Perl, H., Goldberg, I. and Smith, M.: SoK: Secure messaging, *IEEE Symposium on Security and Privacy* (*SP*), IEEE (2015).
[11] Mozilla: Gloda, available from ⟨https://developer.mozilla.org/en-US/docs/Mozilla/Thunderbird/gloda⟩.
[12] Microsoft: Windows Indexing Features - TechNet, available from ⟨https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-7/dd744700(v=ws.10)⟩.
[13] Apache: Apache Lucene - Index File Formats, available from ⟨https://lucene.apache.org/core/3_5_0/fileformats.html⟩.
[14] Song, D.X., Wagner, D. and Perrig, A.: Practical Techniques for Searches on Encrypted Data, *Proc. IEEE Symposium on Security and Privacy* (*S&P '00*), IEEE Computer Society (2000).
[15] Goh, E.-J.: Secure Indexes, IACR Cryptology ePrint Archive, Report 2003/216 (2003).
[16] Chang, Y.-C. and Mitzenmacher, M.: Privacy Preserving Keyword Searches on Remote Encrypted Data, *Proc. International Conference on Applied Cryptography and Network Security* (*ACNS '05*) (LNCS), Ioannidis, J., Keromytis, A.D. and Yung, M. (Eds.), Vol.3531, Springer, pp.442–455 (2005).
[17] Curtmola, R., Garay, J.A., Kamara, S. and Ostrovsky, R.: Searchable Symmetric Encryption: Improved Definitions and Efficient Constructions, *Proc. ACM Symposium on Information, Computer and Commucations Security* (*CCS '06*), Juels, A., Wright, R.N. and De Capitani di Vimercati, S. (Eds.), pp.79–88, ACM (2006).
[18] Chase, M. and Kamara, S.: Structured Encryption and Controlled Disclosure, *Proc. Internaional Conference on the Theory and Applications of Cryptology and Information Security* (*ASIACRYPT '10*) (LNCS), Abe, M. (Ed.), Vol.6477, pp.577–594, Springer (2010).
[19] Kamara, S., Papamanthou, C. and Roeder, T.: Dynamic searchable symmetric encryption, *Proc. ACM Symposium on Information, Computer and Commucations Security* (*CCS '12*), Yu, T., Danezis, G. and Gligor, V.D. (Eds.), pp.965–976, ACM (2012).
[20] Ogata, W., Koiwa, K., Kanaoka, A. and Matsuo, S.: Toward Practical Searchable Symmetric Encryption, *Proc. International Workshop on Security* (*IWSEC '13*) (LNCS), Sakiyama, K. and Terada, M. (Eds.), Vol.8231, pp.151–167, Springer (2013).
[21] Cash, D., Jarecki, S., Jutla, C.S., Krawczyk, H., Rosu, M.-C. and Steiner, M.: Highly-Scalable Searchable Symmetric Encryption with Support for Boolean Queries, *Proc. International Cryptology Conference* (*CRYPTO '13*) (LNCS), Canetti, R. and Garay, J.A. (Eds.), Vol.8042, pp.353–373, Springer (2013).
[22] Cash, D., Jaeger, J., Jarecki, S., Jutla, C.S., Krawczyk, H., Rosu, M.-C. and Steiner, M.: Dynamic Searchable Encryption in Very Large Databases: Data Structures and Implementation, *Proc. Network and Distributed Systems Symposium* (*NDSS '14*), Vol.2014, Internet Society (2014).
[23] Ballard, L., Kamara, S. and Monrose, F.: Achieving Efficient Conjunctive Keyword Searches over Encrypted Data, *Proc. ICICS 2005*, LNCS Vol.3783, pp.414–426 (2005).
[24] Cao, N., Wang, C., Li, M., Ren, K. and Lou, W.: Privacy-Preserving Multi-Keyword Ranked Search over Encrypted Cloud Data, *IEEE Trans. Parallel and Distributed Systems*, Vol.25, pp.222–233 (2014).
[25] Wong, W.K., Cheung, D.W., Kao, B. and Mamoulis, N.: Secure kNN Computation on Encrypted Databases, *Proc. 35th ACM SIGMOD*, pp.139–152 (2009).
[26] Li, J., Wang, Q., Wang, C., Cao, N., Ren, K. and Lou, W.: Fuzzy keyword search over encrypted data in cloud computing, *Proc. INFOCOM 2010*, pp.1–5 (2010).
[27] Wang, C., Ren, K., Yu, S. and Urs, K.M.R. Achieving Usable and Privacy-assured Similarity Search over Outsourced Cloud Data, *Proc. INFOCOM 2012*, pp.451–459 (2012).
[28] Boldyreva, A. and Chenette, N.: Efficient Fuzzy Search on Encrypted Data, IACR Cryptology ePrint Archive 2014/235 (2014).
[29] Liu, C., Zhu, L., Li, L. and Tan, Y.: Fuzzy Keyword Search On Encrypted Cloud Storage Data With Small Index, *Proc. IEEE CCIS2011* (2010).
[30] Poh, G.S., Chin, J.-J., Yau, W.-C., Choo, K.-K.R. and Mohamad, M.S.: Searchable Symmetric Encryption: Designs and Challenges, *ACM Comput. Surv.*, Vol.50, No.3, Article 40 (May 2017).
[31] Boneh, D., Di Crescenzo, G., Ostrovsky, R. and Persiano, G.: Public key encryption with keyword search, *EUROCRYPT*, LNCS, Vol.3027, pp.506–522 (2004).
[32] Bösch, C., Hartel, P., Jonker, W. and Peter, A.: A Survey of Provably Secure Searchable Encryption, *ACM Comput. Surv.*, Vol.47, No.2, Article 18 (Aug. 2014).
[33] Enron Email Dataset, available from ⟨https://www.cs.cmu.edu/~enron/⟩.
[34] Chiba minimum wages table — togane-shi homepage (online), available from ⟨http://www.city.togane.chiba.jp.e.gh.hp.transer.com/0000000307.html⟩.
[35] Rashtian, H., Boshmaf, Y., Jaferian, P. and Beznosov, K.: To Befriend Or Not? A Model of Friend Request Acceptance on Facebook, *SOUPS 2014* (2014).
[36] Stobert, E. and Biddle, R.: The Password Life Cycle: User Behaviour in Managing Passwords, *SOUPS 2014* (2014).
[37] Alghamdi, D., Flechais, I. and Jirotka, M.: Security Practices for Households Bank Customers in the Kingdom of Saudi Arabia, *SOUPS 2015* (2015).
[38] Dosono, B., Hayes, J. and Wang, Y.: I'm Stuck!: A Contextual Inquiry of People with Visual Impairments in Authentication, *SOUPS 2015* (2015).
[39] Dunphy, P., Vlachokyriakos, V., Thieme, A., Nicholson, J., McCarthy, J. and Olivier, P.: Social Media As a Resource for Understanding Security Experiences: A Qualitative Analysis of #Password Tweets, *SOUPS 2015* (2015).
[40] Kang, R., Dabbish, L., Fruchter, N. and Kiesler, S.: My Data Just Goes Everywhere: User Mental Models of the Internet and Implications for Privacy and Security, *SOUPS 2015* (2015).
[41] Khan, H., Hengartner, U. and Vogel, D.: Usability and Security Perceptions of Implicit Authentication: Convenient, Secure, Sometimes Annoying, *SOUPS 2015* (2015).
[42] Sundaramurthy, S.C., Bardas, A.G., Case, J., Ou, X. and Wesch, M., McHugh, J. and Rajagopalan, S.R.: A Human Capital Model for Mitigating Security Analyst Burnout, *SOUPS 2015* (2015).
[43] Fagan, M. and Khan, M.M.H.: Why Do They Do What They Do?: A Study of What Motivates Users to (Not) Follow Computer Security Advice, *SOUPS 2016* (2016).
[44] Torabi, S. and Beznosov, K.: Sharing Health Information on Facebook: Practices, Preferences, and Risk Perceptions of North American Users, *SOUPS 2016* (2016).
[45] Conway, D., Taib, R., Harris, M., Yu, K., Berkovsky, S. and Chen, F.: A Qualitative Investigation of Bank Employee Experiences of Information Security and Phishing, *SOUPS 2017* (2017).
[46] Gallagher, K., Patil, S. and Memon, N.: New Me: Understanding Expert and Non-Expert Perceptions and Usage of the Tor Anonymity Network, *SOUPS 2017* (2017).
[47] Ruoti, S., Monson, T., Wu, J., Zappala, D. and Seamons, K.: Weighing Context and Trade-offs: How Suburban Adults Selected Their Online Security Posture, *SOUPS 2017* (2017).
[48] Nielsen, J. and Landauer. T.K.: A mathematical model of the finding of usability problems, *Proc. INTERACT '93 and CHI '93 Conference on Human Factors in Computing Systems*, *CHI '93*, pp.206–213, ACM (1993).

Tatsuya Midorikawa received his B.E. and M.E. degrees from Toho University in 2016 and 2018, respectively. He joined IOS Co., Ltd. in 2018. He received IPSJ Yamashita SIG Research Award in 2017.

Akihiro Tachikawa received his B.E. and M.E. degrees from Toho University in 2017 and 2019, respectively. He joined DCOM in 2019.

Akira Kanaoka received his Ph.D. degree in engineering from University of Tsukuba, Japan in 2004. He worked at SECOM Co., Ltd. from 2004 to 2007, and at University of Tsukuba from 2007 to 2013. He is currently an associate professor of Department of Information Science, Faculty of Science, Toho University. His research interests include usable security and privacy.