Cellphone Usage Support Function based on Operation History

T. Nakagawa[†], T. Yoshikawa[†], C. Doi[†], K.Ohta[†], C. Noda[‡], and H. Inamura[†]

[†]Research Laboratories, NTT DOCOMO, Inc.
[‡]Customer Device Development Department, NTT DOCOMO, Inc.
3-5, Hikari-no-oka, Yokosuka, Kanagawa, JAPAN.

ABSTRACT

In order to securely utilize the operation history collected by a cellphone, we propose an operation history platform that stores operation logs from different applications. As privacy problem can arise when handling sensitive operation history data, the prototype features privacy-aware middleware composed of access control, UIM binding, passcode, and data abstraction modules. Thus, our proposed platform enables various applications to leverage the operation history data, while assuring safety and security to the user.

As an example to utilize the proposed operation history platform, we implemented a demo application whose goal is to enhance children's cellphone literacy by feeding back their daily cellphone usage.

Keywords: operation history, privacy, cellphone literacy

1 Introduction

Various functions that use a cellphone's operation history have been provided to stimulate cellphone usage. For instance, Vivid UI[1] dynamically personalizes the menu according to application usage frequency. Also, "life history viewer" supports quick search and access to user's data by the time-line representation of the data[2]. This function is realized by using operation history data such as E-mail reception or photo taken on the phone.

However, collecting such operation history data creates a security risk, and the challenge is how to preserve privacy while still being able to leverage the richness of the data[3]. Given this background, we developed an operation history platform for cellphones that allows the user's operation history to be stored and utilized in a safe and secure manner. This paper starts by describing privacy-aware middleware that provides several unique functions to protect history data. Next it introduces a demo application that enhances a child's cellphone literacy by utilizing his/her operation history.

2 Operation history platform

2.1 Architecture

Our operation history platform implements functions such as storing and retrieving the operation history data (Figure 1). The operation history data is categorized into middleware-level operation data and application-level operation data.

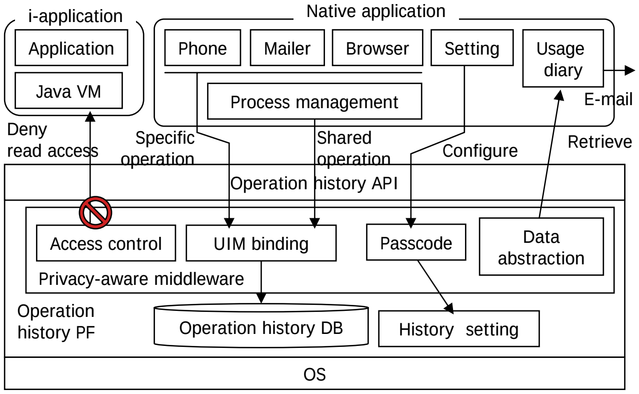


Figure 1: Architecture of operation history platform

- Middleware-level operation data

  The process management module is modified so that the start-up and termination time of each application is recorded. These data are recorded for most applications such as the mailer, browser, and other accessory software modules.

- Application-level operation data

  Major applications such as telephone, browser, mailer, and java virtual machine are modified to record principal operations. For example, the telephone application records details of outgoing and incoming calls. The browser stores the URLs of the web sites visited.

The history data of both categories is stored in common format so that both can be utilized easily when developing applications.

2.2 Privacy-aware middleware

We designed the privacy-aware middleware to prevent improper disclosure of the history data.

- Access control to database

  Operation history data is stored in a database separate from existing history data such as incoming and outgoing calls. The database can't be accessed by any 3rd-party java application, which prevents the leakage of the operation history data by dishonest applications.

- UIM binding

  Each entry of history data includes subscriber's UIM number, and access to previous operation history data is denied in case the original UIM is not inserted. Thus, leakage of history data to third persons is avoided even when the cellphone is given away or lended.

- Passcode for setting protection

  Only the original user who knows personal identification number can change his permission preferences with regard to storage of history data, preventing others from secretly changing the setting.

- Abstraction of history data

  The only data that can be sent outside the device is the output of the data abstraction module in the middleware. The abstraction module provides the total number of application usages or total duration so that the user's detailed behavior is concealed.

3 Demo application

For this paper, we implemented an example application for children approximately 10 to 15 years old. In Japan, the penetration rate of cellphones has reached 31.6% for 6th graders, and 55.2% for 9th graders[4]. This demands that children acquire cellphone literacy to protect themselves from unnecessary troubles.

The primary concept of the prototype application is to notify children if their cellphone usage is compliant with the rule, instead of forcing them to strictly observe the rule. To this end, the application provides a review of daily usage by the ”overuse notification” function and the ”usage diary”. It is possible for parents to intervene in the children's cellphone usage observation, by defining the rule together, and getting feedback on daily usage.

Figure 2 shows the ”overusage notification”.

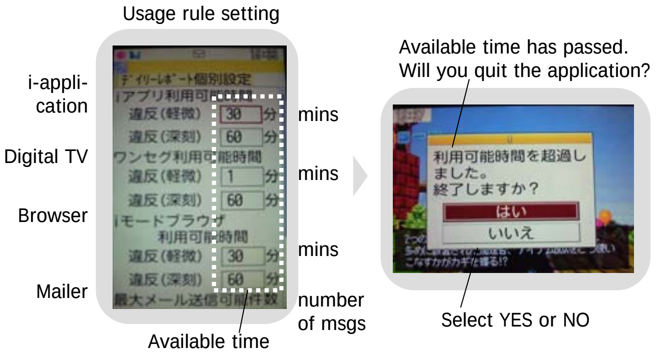
1. Parents discuss with their child the family's rules on cellphone usage, which are then set on the child's cellphone. In the prototype, the child is notified when the time spent on each application reaches predefined threshold. Also the number of outgoing e-mail messages is limited.

2. The child utilizes the cellphone and the operation history is stored in the device.

3. When the total usage time of the target application exceeds the specified limit, a notification dialog pops up on the display. The application remains available even after the notification, for the child's convenience (A future function would shutdown the application on the 2nd notification).

Figure 3 shows the ”usage diary” function. In addition to steps 1 & 2 above, the following step is conducted.

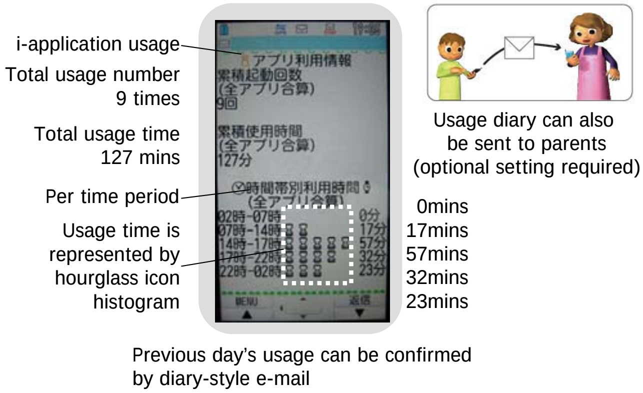
3' Previous day's usage is sent to the child's own cellphone every day. The e-mail contains information such as total number of applications accessed and the total time spent; this data allows the child to reflect on rule compliance. If a parent's e-mail address is set as the destination, the same ”usage diary” e-mail can be shared with the parent.



デイリーレポート個別設定
iアプリ利用可能時間
違反(軽微) 30 分
違反(深刻) 60 分
ワンセグ利用可能時間
違反(軽微) 1 分
違反(深刻) 60 分
iモードブラウザ
利用可能時間
違反(軽微) 30 分
違反(深刻) 60 分
最大メール送信可能件数

利用可能時間を超過しました。
終了しますか？
はい
いいえ

Figure 2: Overuse notification function



アプリ利用情報
累積起動回数
(全アプリ合算)
9回
累積使用時間
(全アプリ合算)
127分
時間帯別利用時間
(全アプリ合算)
02時-07時 0分
07時-14時 17分
14時-17時 57分
17時-22時 32分
22時-02時 23分
MENU
返信

i-application usage
Total usage number
9 times
Total usage time
127 mins
Per time period
Usage time is represented by hourglass icon histogram
0mins
17mins
57mins
32mins
23mins
Usage diary can also be sent to parents (optional setting required)
Previous day's usage can be confirmed by diary-style e-mail

Figure 3: Usage diary function

4 Conclusion

In this paper, we proposed a secure operation history platform to protect the user's privacy while better leveraging the terminal's operation history. We prototyped an example application that helps children learn the proper usage of cellphones. The prototype embodies the concept that it is important for children to learn usage rules by themselves. In the future, we plan on developing a wide range of applications for consumers and corporate users.

REFERENCES

[1] VIVID UI: Acrodea, http://www.acrodea.co.jp/english/index.html (accessed 2009-12-11).

[2] Life history viewer (in Japanese), http://www.n-keitai.com/n-03a/uf03.html (accessed 2009-12-11).

[3] Charu C. Agarwal and Philip S. Yu, editors. Privacy Preserving Data Mining: Models and Algorithms. Springer, 2008.

[4] Survey on children's ICT utilization (in Japanese), http://benesse.jp/berd/center/open/report/ict_riyou/hon/index.html (accessed 2009-12-11).