

PROXY SERVER FOR RELAYING AND EXTRACTING DATA BETWEEN
MOBILE APPLICATION AND APPLICATION SERVER, BIG DATA
EXTRACTION SYSTEM INCLUDING THE PROXY SERVER, AND BIG DATA
EXTRACTION METHOD USING THE PROXY SERVER

5

BACKGROUND OF THE INVENTION

Field of the Invention

The present disclosure relates to an apparatus for
extracting data of a mobile application.

10

Description of the Related Art

The rapidly increasing proliferation of smartphones is
a driving force behind the dramatic shift from a Web-based
Internet environment to a mobile Internet environment.
Accordingly, mobile applications have placed themselves as a
critical medium for overall economic activities including
purchase and payment, beyond simple provisioning of search
results.

15

To extract big data on various activities made with
smartphones, data transmitted and received between a mobile
application and an application service should first be
collected, refined, and subjected to final analysis.

20

Compared to extraction of big data in a legacy Web-
based Internet environment such as a Web browser, however,
it is not easy to extract data from applications in a mobile

25

environment, because the mobile environment in which applications are executed involves closed rendering, unlike a Web browser.

In this regard, the inventor has developed and
5 completed the invention through long-time studies and error and trial in order to solve the problem.

SUMMARY OF THE INVENTION

Therefore, the present disclosure has been made in
10 view of the above problems, and it is an object of the present disclosure to provide a technique of easily extracting data transmitted and received between a mobile application and an application server.

In accordance with an aspect of the present
15 disclosure, a proxy server for relaying and extracting data between a mobile application and an application server includes a virtual certificate provider configured to transmit a virtual certificate in response to an authentication request from the mobile application
20 executed in a mobile application emulator, a real certificate requester configured to forward the authentication request of the mobile application to the application server, and request a real certificate to the application server, and a big data collector configured to
25 collect data transmitted and received between the mobile

application and the application server, using the virtual certificate and the real certificate.

Preferably, the big data collector may be configured to acquire original request data received from the mobile application, using the virtual certificate, and acquire
5 original response data received from the application server, using the real certificate.

Preferably, the big data collector may be configured to, upon receipt of a virtual secure socket layer (SSL)
10 request packet from the mobile application, acquire original request data by decoding the virtual SSL request packet, using the virtual certificate, and encode the original request data to a real SSL request packet, using the real certificate, and to, upon receipt of a real SSL
15 response packet from the application server, acquire original response data by decoding the real SSL response packet, using the real certificate, and encode the original response data to a virtual SSL response packet, using the virtual certificate.

20 In accordance with another aspect of the present disclosure, a big data extraction system for relaying and extracting data between a mobile application and an application server includes a mobile application emulator configured to enable execution of the mobile application
25 even in a heterogeneous terminal other than a mobile

terminal, and a proxy server for relaying and extracting data between the mobile application and the application server.

Preferably, the big data extraction system may
5 further include a macro device configured to sense a screen of the mobile application, and input specific information to the mobile application by performing an input operation including a touch operation and a text input operation.

10 In accordance with another aspect of the present disclosure, a big data extraction method for relaying and extracting data between a mobile application and an application server includes establishing primary authentication with the mobile application executed in a
15 mobile application emulator, using a virtual certificate by a proxy server acting as a virtual application server for the mobile application, establishing secondary authentication with the application server, using a real certificate by the proxy server acting as a virtual mobile
20 application for the application server, and collecting data transmitted and received between the mobile application and the application server, using the virtual certificate and the real certificate by the proxy server.

In accordance with another aspect of the present
25 disclosure, a big data extraction method for relaying and

extracting data between a mobile application and an application server includes transmitting an authentication request by the mobile application executed in a mobile application emulator, transmitting a virtual certificate to the mobile application in response to the authentication request by a proxy server that relays data transmitted and received between the mobile application and the application server, establishing primary authentication with the proxy server, using a virtual certificate by the mobile application, forwarding the authentication request to the application server by the proxy server, storing a real certificate issued by the application server by the proxy server, establishing secondary authentication with the application server, using the real certificate by the proxy server, and acquiring original request data received from the mobile application, using the virtual certificate, and acquiring original response data received from the application server, using the real certificate, during a process of relaying data transmitted and received between the mobile application and the application server by the proxy server.

In accordance with another aspect of the present disclosure, a big data extraction method for relaying and extracting data between a mobile application and an

application server includes receiving a first request packet from the mobile application by a proxy server that relays data between the mobile application and the application server, acquiring original request data by
5 decoding the first request packet, using a virtual certificate by the proxy server, encoding the original request data to a second request packet, using a real certificate by the proxy server, transmitting the second packet to the application server by the proxy server,
10 receiving a first response packet from the application server by the proxy server, acquiring original response data by decoding the first response packet, using the real certificate by the proxy server, encoding the original response data to a second response packet, using the
15 virtual certificate by the proxy server, and transmitting the second response packet to the mobile application by the proxy server.

BRIEF DESCRIPTION OF THE DRAWINGS

20 The above and other objects, features and other advantages of the present invention will be more clearly understood from the following detailed description taken in conjunction with the accompanying drawings, in which:

FIG. 1 is a block diagram illustrating a preferred
25 embodiment of a big data extraction system according to

the present disclosure;

FIG. 2 is a block diagram illustrating a preferred embodiment of a proxy server according to the present disclosure; and

5 FIG. 3 is a flowchart illustrating a preferred embodiment of a big data extraction method according to the present disclosure.

DETAILED DESCRIPTION OF THE INVENTION

10 Reference will now be made in detail to the preferred embodiments of the present disclosure, examples of which are illustrated in the accompanying drawings. Wherever possible, the same reference numbers will be used throughout the drawings to refer to the same or like parts.

15 It is difficult to extract data exchanged between a mobile application and an application server. Specifically, the difficulty arises from the following reason.

 Compared to a Web browser, a mobile application involves closed rendering (including a user interface (UI)).
20 A Web page basically renders common UI components such as an input, a button, a list, and an image. Navigation between Web pages is carried out based on hyperlinks, or navigation between uniform resource locators (URLs) is carried out based on tags. In contrast, the mobile application supports
25 interactive UIs in consideration of user experience (UX)

beyond limitations of Web-based common UI components.
Therefore, since the mobile application uses much more
complicated rendering than the Web browser, data should also
be extracted from the mobile application in a highly
5 sophisticated method.

Moreover, Web browser-based analytic tools are
available only restrictively to the mobile application.
Since Web browsers are based on hypertext markup language
(HTML) and JavaScript, a variety of tools with which to
10 analyze them are provided. However, such conventional tools
are not viable for the mobile application.

Further, to collect data for upgraded versions of
mobile applications, developers should bother with
additional analysis of the applications and reconfiguration
15 of collection techniques.

However, the present disclosure proposes an apparatus
and method for extracting data exchanged between a mobile
application and an application server as follows, overcoming
the above technical challenges.

20 FIG. 1 is a block diagram illustrating a preferred
embodiment of a big data extraction system according to the
present disclosure.

Referring to FIG. 1, a big data extraction system 100
according to the present disclosure includes a mobile
25 application emulator 300, a proxy server 200, and a macro

device 400.

The mobile application emulator 300 is a device that enables execution of a mobile application even in a heterogeneous terminal other than a mobile terminal. In a preferred embodiment, the mobile application emulator 300 may be a computing device such as a personal computer (PC). A mobile application from which big data is to be extracted is installed in the mobile application emulator 300, and operates in the same manner as one installed in a mobile terminal.

The mobile application emulator 300 is configured such that the installed mobile application communicates with an application server 10 through the proxy server 200 of the present disclosure.

The proxy server 200 relays data between the mobile application installed in the mobile application emulator 300 and the application server 10. The proxy server 200 generally refers to a server functioning to relay data between a client and a server. In addition to data relay, the proxy server 200 may extract relayed data in the present disclosure. Particularly, the proxy server 200 of the present disclosure may extract original data even from data which has been encoded and transmitted and received between the mobile application and the application server 10 by decoding the data. This is because the proxy server 200 has

respective certificates used to decode encoded data from both parties. In the present disclosure, it is made clear that the proxy server 200 should be understood as a server that executes a function of extracting original data from encoded data, concurrently with relaying the data, not limited by the name and term "proxy server".

The macro device 400 inputs intended information and actions to the mobile application. The macro device 400 may sense a screen of the mobile application, and inputs specific information to the mobile application by performing an input operation including touch and text input. Although the macro device 400 and the mobile application emulator 300 may be configured separately, they may also be incorporated into one device.

Now, a description will be given of an embodiment of data extraction in the big data extraction system 100.

The proxy server 200 provides a virtual public certificate to the mobile application in response to an authentication request from the mobile application.

The macro device 400 performs an intended input operation to the mobile application in order to collect specific information from the mobile application.

The mobile application encodes a request packet, using a virtual public certificate, and transmits the encoded request packet to the proxy server 200.

The proxy server 200 decodes the request packet, using a virtual private certificate, thereby obtaining original request data.

5 The proxy server 200 encodes the original request data, using a real public certificate received from the application server 10, and transmits the encoded request data to the application server 10.

10 Upon receipt of a response from the application server 10, the proxy server 200 decodes the response and stores the decoded response as original response data. The proxy server 200 encodes the original response data, using the virtual certificate, and transmits the encoded response data to the mobile application.

15 FIG. 2 is a block diagram illustrating a preferred embodiment of a proxy server according to the present disclosure.

Referring to FIG. 2, the proxy server 200 of the present disclosure includes a virtual certificate provider 210, a real certificate requester 220, a database (DB) 230, and a big data collector.

20 The proxy server 200 of the present disclosure extracts encoded original data between a mobile application and an application server through double authentication.

25 Primary authentication will first be described. The proxy server 200 behaves as if it were the application

server to the mobile application. That is, the proxy server 200 establishes the primary authentication with the mobile application by providing a virtual certificate in response to an authentication request from the mobile application.

5 In a preferred embodiment, the primary authentication is performed in the virtual certificate provider 210. The virtual certificate provider 210 replies to the authentication request of the mobile application executed in the mobile application emulator, with the virtual
10 certificate, thereby performing the primary authentication. For this purpose, the virtual certificate provider 210 may generate and store the virtual certificate. In a preferred embodiment, the virtual certificate provider 210 may issue a secure socket layer (SSL) certificate, when SSL
15 authentication is needed, and a ROOT certification authority (CA) certificate, when ROOT CA authentication is needed.

 The secondary authentication is described below. The proxy server 200 behaves as if it were the mobile application to the application server. The proxy server 200
20 forwards the authentication request of the mobile application as it is to the application server, and establishes the secondary authentication with the application server by emulating the behavior that the mobile application has taken during the primary authentication. The
25 secondary authentication is performed using a real

certificate provided by the application server.

In a preferred embodiment, the secondary authentication is performed in the real certificate requester 220. The real certificate requester 220 forwards
5 the authentication request of the mobile application to the application server, and requests the real certificate to the application server. The real authentication requester 220 performs the secondary authentication with the application server, using the real certificate. The real certificate
10 requester 220 may store the real certificate.

The DB 230 stores the original request data and original response data decoded by the big data collector. In addition, the DB 230 may store the virtual certificate and the real certificate.

15 The big data collector collects data transmitted and received between the mobile application and the application server, using the virtual certificate and the real certificate. The big data collector acquires original request data received from the mobile application, using the
20 virtual certificate, and original response data received from the application server, using the real certificate. In a specific embodiment, upon receipt of a virtual SSL request packet from the mobile application, the big data collector acquires original request data by decoding the virtual SSL
25 request packet, using the virtual certificate, and encodes

the original request data to a real SSL request packet, using the real certificate. Further, upon receipt of a real SSL response packet from the application server, the big data collector acquires original response data by decoding the real SSL response packet, using the real certificate, and encodes the original response data to a virtual SSL response packet, using the virtual certificate.

This operation will be described in greater detail, taking a specific example.

10 A request packet receiver 241 receives a first request packet from the mobile application.

 If the first request packet is an encoded packet, a first decoder 242 acquires original request data by decoding the first request packet, using a virtual certificate. The first decoder 242 stores the original request data in the DB 230, and at the same time, transmits the original request data to a first encoder 243. The first encoder 243 encodes the original request data to a second request packet, using a real certificate. A request packet transmitter 244 transmits the second request packet to the application server.

 A response packet receiver 245 receives a first response packet from the application server. If the first response packet is an encoded packet, the response packet receiver 245 transmits the first response packet to a second

decoder 246.

The second decoder 246 acquires original response data by decoding the first response packet, using the real certificate. The second decoder 246 transmits the original response data to a second encoder 247, and at the same time, stores the original response data in the DB 230.

The second encoder 247 encodes the original response data to a second response packet, using the virtual certificate. A response packet transmitter 248 transmits the second response packet to the mobile application.

FIG. 3 is a flowchart illustrating a preferred embodiment of a big data extraction method according to the present disclosure.

Referring to FIG. 3, a mobile application transmits an authentication request to a proxy server (S1100). The proxy server attempts primary authentication by transmitting a virtual certificate to the mobile application in response to the authentication request (S1200). The mobile application establishes the primary authentication with the proxy server, regarding the proxy server that has transmitted the virtual certificate as an application server (S1300).

The proxy server forwards the authentication request as it is to the application server (S1400). Since the authentication request received from the proxy server has been issued rightfully from the mobile application, the

application server transmits a real certificate without any doubt in response to the authentication request (S1500). The proxy server establishes secondary authentication with the application server, using the received real certificate
5 (S1600).

After completing the primary authentication and the secondary authentication in this manner, the proxy server may acquire original data from encoded data transmitted and received between the mobile application and the application
10 server. This operation will be described below, taking a specific example.

The mobile application transmits a first request packet to the proxy server (S2100). If the first request packet is an encoded packet, the proxy server acquires
15 original request data by decoding the first request packet, using the virtual certificate (S2200). The proxy server stores the original request data in a DB (S2300). The proxy server encodes the original request data to a second request packet, using the real certificate (S2400). The proxy server
20 transmits the second request packet to the application server (S2500).

The application server transmits a first response packet to the proxy server in response to the second request packet (S3100). If the first response packet is an encoded
25 packet, the proxy server acquires original response data by

decoding the first response packet, using the real
certificate (S3200). The proxy server stores the original
response data in the DB (S3300). The proxy server encodes the
original response data to a second response packet, using the
5 virtual certificate (S3400). The proxy server transmits the
second response packet to the mobile application (S3500).

As is apparent from the above description, the
present disclosure may easily extract data transmitted and
received between a mobile application and an application
10 server.

Although the preferred embodiments of the present
disclosure have been disclosed for illustrative purposes,
those skilled in the art will appreciate that various
modifications, additions and substitutions are possible,
15 without departing from the scope and spirit of the
disclosure as disclosed in the accompanying claims.

WHAT IS CLAIMED IS:

1. A proxy server for relaying and extracting data
between a mobile application and an application server,
5 the proxy server comprising:

a virtual certificate provider configured to transmit
a virtual certificate in response to an authentication
request from the mobile application executed in a mobile
application emulator;

10 a real certificate requester configured to forward
the authentication request of the mobile application to
the application server, and request a real certificate to
the application server; and

a big data collector configured to collect data
15 transmitted and received between the mobile application
and the application server, using the virtual certificate
and the real certificate.

2. The proxy server according to claim 1, wherein
20 the big data collector is configured to acquire original
request data received from the mobile application, using
the virtual certificate, and acquire original response
data received from the application server, using the real
certificate.

25

3. The proxy server according to claim 1, wherein the big data collector is configured to, upon receipt of a virtual secure socket layer (SSL) request packet from the mobile application, acquire original request data by
5 decoding the virtual SSL request packet, using the virtual certificate, and encode the original request data to a real SSL request packet, using the real certificate, and to, upon receipt of a real SSL response packet from the application server, acquire original response data by
10 decoding the real SSL response packet, using the real certificate, and encode the original response data to a virtual SSL response packet, using the virtual certificate.

15 4. A big data extraction system for relaying and extracting data between a mobile application and an application server, the big data extraction system comprising:

a mobile application emulator configured to enable
20 execution of the mobile application even in a heterogeneous terminal other than a mobile terminal; and

the proxy server for relaying and extracting data between the mobile application and the application server according to claim 1.

25

5. The big data extraction system according to claim 4, further comprising a macro device configured to sense a screen of the mobile application, and input specific information to the mobile application by performing an input operation including a touch operation and a text input operation.

6. A big data extraction method for relaying and extracting data between a mobile application and an application server, the big data extraction method comprising:

establishing primary authentication with the mobile application executed in a mobile application emulator, using a virtual certificate by a proxy server acting as a virtual application server for the mobile application;

establishing secondary authentication with the application server, using a real certificate by the proxy server acting as a virtual mobile application for the application server; and

collecting data transmitted and received between the mobile application and the application server, using the virtual certificate and the real certificate by the proxy server.

7. A big data extraction method for relaying and

extracting data between a mobile application and an application server, the big data extraction method comprising:

5 transmitting an authentication request by the mobile application executed in a mobile application emulator;

 transmitting a virtual certificate to the mobile application in response to the authentication request by a proxy server that relays data transmitted and received between the mobile application and the application server;

10 establishing primary authentication with the proxy server, using a virtual certificate by the mobile application;

 forwarding the authentication request to the application server by the proxy server;

15 storing a real certificate issued by the application server by the proxy server;

 establishing secondary authentication with the application server, using the real certificate by the proxy server; and

20 acquiring original request data received from the mobile application, using the virtual certificate, and acquiring original response data received from the application server, using the real certificate, during a process of relaying data transmitted and received between
25 the mobile application and the application server by the

proxy server.

8. A big data extraction method for relaying and extracting data between a mobile application and an application server, the big data extraction method comprising:

receiving a first request packet from the mobile application by a proxy server that relays data between the mobile application and the application server;

10 acquiring original request data by decoding the first request packet, using a virtual certificate by the proxy server;

encoding the original request data to a second request packet, using a real certificate by the proxy server;

15 transmitting the second packet to the application server by the proxy server;

receiving a first response packet from the application server by the proxy server;

20 acquiring original response data by decoding the first response packet, using the real certificate by the proxy server;

encoding the original response data to a second response packet, using the virtual certificate by the proxy server; and

25

transmitting the second response packet to the mobile application by the proxy server.