February 23, 2015

SECURE TRAFFIC METERING WITH A ROUTER

Swaminathan Krishnamurthy

Nick Arini

SECURE TRAFFIC METERING WITH A ROUTER

Program providers supply content to viewers over various communications networks. Content may include broadcast television programs and video programs streamed, for example, over the Internet. Sponsors provide sponsored content to promote products and services.

Sponsors may use one or more different media (e.g., television, radio, print, online) to promote the products and services. Sponsors may create a promotional campaign that uses sponsored content segments appearing in different media. Thus, viewers may be exposed to sponsored content segments in a first media, a second media, and so on.

Program providers may be interested in knowing what content segments are accessed or viewed by which viewers. One way to determine this "viewing history" is by sampling a large population and making inferences about the viewing history based on the sample results. One way to sample a viewing population is through the use of individual panelists (viewers in the sample population) and metering devices that record and report on the individual panelists' viewing history. For example, an individual panelist (i.e., a viewer) may agree to installation of a meter at the panelist's residence. The meter records the individual panelist's television viewing and Internet activity, and reports the data to a remote server. Note that this approach works in a household having more than one viewer. For example, each household member may be recruited as a panelist. Alternately, a subset of the household members may participate as panelists.

In contrast to metering individual panelists, viewing history data may be collected by a single metering device installed at a household. For example, a television set top box (STB) may record television viewing data. This approach cannot distinguish viewing by individual household members, but may be less costly to implement.

Sponsors may want to know how effective their promotional campaigns are. · One way to determine effectiveness is to measure media consumption metrics such as an amount of time an individual spends exposed to the media, a number of times a specific content segment has seen

and/or heard by the individual, and the number of exposures to sponsored content segments among the different media, for example.

Reach is an example of a media consumption metric. Reach is a binary metric; either an individual has been exposed to the media (for example, exposed to a sponsored content segment) or the individual has not been so exposed. Reach may be defined on an individual basis or over a population group. Reach also may be defined over multiple media types. Reach may be measured by a panel and overall reach of the population from which the panel is drawn may be estimated or inferred from the panel data.

Encryption systems may be used to prevent unwanted access to sensitive information that is transmitted over public pathways and networks such as the Internet. One such encryption system is a public key encryption system, widely used to add security to, for example, data packets, including video program data packets, transmitted over the Internet between a server and a client.

As noted above, program providers supply content to viewers over various communications networks. Internet program providers may send video programs over the Internet to a client media device such as a laptop computer, an Internet- enabled television, a tablet, and a smartphone. The video programs often are encrypted using public key encryption, to prevent unauthorized access to the video programs.

Internet-based analytics services may have an interest in measuring media consumption metrics, such as reach, associated with delivery of content over the Internet. One measurement mechanism involves use of metering devices at the client. Some clients are metered as part of a voluntary participation in a panel. The metering may occur at a gateway or router at the client. However, the router may not be able to access the content of encrypted Internet content. As a result, the media consumption metric measurement may not accurately reflect actual media consumption.

An analytics service may invoke Internet-based metering by installing a meter at a gateway or router at the media entry point of a physical viewing location such as a home. In one aspect, the meter is placed in homes of recruited panelists with their permission. The meter logs unsecured traffic from all the Internet clients (e.g., a laptop or desktop computer, an Internet-enabled television, a tablet, a game box, and a smartphone in the home). This centralized, or gateway-based approach to Internet metering of in-home usage has advantages over alternatives such as individual client metering installations in that complex and intrusive software is not required on all clients that are required to be metered, and the meter may kept up-to-date when browsers and operating systems are updated. Once installed, such a router or gateway-based meter may be non-intrusive and comprehensive, which may lead to more accurate and complete data collection, and fewer and less significant support issues with correspondingly less churn (and hence cost) in the panel.

Current gateway-based metering, however, is not capable of capturing secured traffic because the gateway sits in the middle of the server-client transaction. A current solution uses client-side metering for secured traffic and gateway-based metering for unsecured traffic. This current solution is becoming less practical with the ever-increasing use of encryption for Internet-delivered traffic.

To overcome the above-noted problems, and other problems, with metering Internet traffic, disclosed herein are systems and methods that enable such secured traffic to be metered at a router or gateway.

As noted above, with current router-based metering, the inability of a router to capture secured Internet (e.g., HTTPS-protocol) traffic results from the fact that public key encryption is established between the client (e.g., a browser on a computer) making a resource request (e.g., a request for streaming video programs) and a remote, HTTPS-secured server delivering the results of the request for the streaming video programs. Such a request and reply may be encrypted, respectively, at the client and the remote server. Establishing this encryption may prevent

unauthorized eavesdropping on the communications between the client and the remote server by any entity in the client-server path. One such entity in this path is a router, and associated router meter, used to collect media consumption data from panelists. The router will pass the request and reply, but without a private key of the client, the router (and any other entity on the server-client path (ISP switches for example)) cannot read or otherwise make sense of the encrypted traffic. Thus, while encryption serves a useful function, encryption also prevents gateway-based metering of content delivered over the Internet.

In the above-described scenario of a router meter used to collect panelist traffic, the router ordinarily could have "permission" from the client(s) to "view" the encrypted traffic. Disclosed herein are systems and methods that allow the router to decrypt the traffic after it leaves the client. Such decryption may be completed "off-line", and the encrypted traffic is passed from the client, through the router, and to the server without affecting the normal request delivery process. To achieve this decryption at the router, the herein disclosed systems and methods enable the client to share its private keys securely with the router. In an embodiment, such sharing of private keys is accomplished by establishing a public key link between the client and the router and sending the client's private key over the link. The client then may delegate authority to the router to decrypt certain types of content (but not necessarily all) for logging purposes without affecting the actual client request (because the logging is done out of band).

To delegate such decryption authority to the router, the herein disclosed systems and methods may establish a local certificate authority. The thus-created certificate authority then may generate certificates "on-the-fly" whenever metering of encrypted traffic is desired. In an embodiment a system and method that generates certificates on-the-fly combines the functions of a proxy server (e.g., a squid proxy server) with a dynamic secured socket layer (SSL) certificate generation feature. In this embodiment, each client behind the in-home router would explicitly "trust" the proxy server to be the certificate authority. In an aspect, the proxy server is established at a remote server, such as an analytics system server.

In an alternate embodiment, the router is established as a certificate authority, and may

generate keys for all local clients on the router rather than having the certificates generated on the clients.

Once the router has access to the private keys of a client, the router may decrypt the secure requests (e.g. secure Internet queries) and log the queries in the usual flow of metered traffic reported to an analytics service.

Figure 1 illustrates an example environment in which personal analytics and usage controls may be implemented. In Figure 1, environment 10 includes viewing locations 20, sponsor 40, program provider 60, and analytics service 70, all of which communicate using communications network 50. Although Figure 1 shows these entities as separate and apart, at least some of the entities may be combined or related. For example, the sponsor 40 and program provider 60 may be part of a single entity. Other combinations of entities are possible.

The viewing location 20 includes first media device 24 and second media device 26 through which viewers 22 are exposed to media from sponsor 40 and program provider 60. A viewing location 20 may be the residence of the viewer 22, who operates media devices 24 and 26 to access, through router 25, resources such as Web sites and to receive television programs, radio programs, and other media. The media devices 24 and 26 may be fixed or mobile. For example, media device 24 may be an Internet connected "smart" television (ITV); a "basic" or "smart" television connected to a set top box (STB) or other Internet- enabled device; a Blu-ray™ player; a game box; and a radio, for example. Media device 26 may be a tablet, a smart phone, a laptop computer, or a desk top computer, for example. The media devices 24 and 26 may include browsers. A browser may be a software application for retrieving, presenting, and traversing resources such as at the Web sites. The browser may record certain data related to the Web site visits. The media devices 24 and 26 also may include applications. The panelist 22 may cause the media devices 24 or 26 to execute an application, such as a mobile banking application, to access online banking services. The applications may involve use of a browser or other means, including cellular means, to connect to the online banking services.

The viewing location 20 may include a monitor 27 that records and reports data collected in connection with request for and delivery of sponsored content segments 42 and programs 62 to the viewer 22. The example monitor 27 may be incorporated into router 25 through which certain media (e.g., Internet-based content and content requests) received at or emanating from the viewing location 20 passes.

The sponsor 40 operates server 44 to provide sponsored content segments that are served with programs 62 provided by the program provider 60. For example, the server 44 may provide sponsored content segments to serve with broadcast television programming. The sponsored content segments 42 may include audio, video, and animation features. The sponsored content segments 42 may be in a rich media format. The sponsor 40 may provide a promotional campaign that includes sponsored content segments to be served across different media types or a single media type. The cross-media sponsored content segments 42 may be complementary; that is, related to the same product or service.

The network 50 may be any communications network that allows the transmission of signals, media, messages, voice, and data among the entities shown in Figure 1, including radio, linear broadcast (over-the-air, cable, and satellite) television, on-demand channels, over-the-top media, including streaming video, movies, video clips, and games, and text, email, and still images, and transmission of signals, media, messages, voice, and data from a media device to another media device, computer, or server. The network 50 includes the Internet, cellular systems, and other current and future mechanisms for transmission of these and other media. The network 50 may be both wired and wireless. The network 50 may be all or a portion of an enterprise or secured network. In an example, the network 50 may be a virtual private network (VPN) between the program provider 60 and the media devices 24 and 26. While illustrated as a single or continuous network, the network 50 may be divided logically into various sub-nets or virtual networks, so long as at least a portion of the network 50 may facilitate communications among the entities of Figure 1.

The program provider 60 delivers programs for consumption by the viewer. The programs

62 may be streaming video programs from Internet Web sites. The programs 62 may be delivered to the media devices 24 and 26 as encrypted data packets using public key encryption. The programs 62 may include provisions for serving and displaying sponsored content segments 42. The program provider 60 may receive the sponsored content segments 42 from the sponsor and incorporate the sponsored content segments into the programs 62. Alternately, the viewer's media devices may request a sponsored content segment 42 when those media devices display a program 62.

The program provider 60 operates server 64 to serve programs and to implement usage control system 200. The system 200 may provide an interface that allows the viewer 22 to initiate content requests.

The analytics service 70 may be established to collect information related to Internet content requested by and delivered to the viewer 22. In the example of Figure 1, the viewer 22 is a recruited panelist and has agreed to such information collection by the analytics service 70. The analytics service 70 may provide the meter 27 established or installed at the viewing location 20.

The analytics service 70 operates analytics server 70, which in turn implements data collection system 300. One aspect of the system 300, as described below, it to provide for capture of secure traffic emanating from the media devices 24 and 26 (i.e. clients) by the meter 27. In an aspect, the system 300 may implement a proxy server as a certificate authority. In another aspect, the system 300 may be used to establish the router 25 as a certificate authority.

In executing the processes of Figure 1, and as otherwise disclosed herein, individual viewer (panelist) and household demographic data and Internet activity (as well as other media consumption such as and television viewing, for example) may be collected and used. In situations in which the systems disclosed herein may collect and/or use personal information about viewers, or may make use of personal information, the viewers may be provided with an opportunity to control whether programs or features collect viewer information (e.g., information

about a viewer's social network, social actions or activities, profession, a viewer's preferences, or a viewer's current location), or to control whether and/or how to receive media, including advertisements, from an server that may be more relevant or of interest to the viewer. In addition, certain data may be treated in one or more ways before it is stored or used, so that personally identifiable information is removed. For example, a viewer's identity may be treated so that no personally identifiable information can be determined for the viewer, or a viewer's geographic location may be generalized where location information is obtained (such as to a city, ZIP code, or state level), so that a particular location of a viewer cannot be determined. Thus, the viewer may have control over how information is collected about the viewer and used by a server.

Figure 2A illustrates an example of a system that enables a router to decrypt encrypted Internet traffic sent between a client and a server. In Figure 2A, system 300 is implemented on the analytics server 74. The system 300 may be stored in non-transitory, computer-readable storage medium 72 and is loaded by processor 75 into memory 76 and executed. The system 300 may be accessed by other machines through input/output (I/O) 78.

In Figure 2A, system 300 may be used for the collection, measurement, and analysis of media consumption metrics related to Internet-based media. For example, the system 300 may collect, measure, and analyze Internet requests emanating from the viewing location 20 of Figure 1, and the content supplied in return (for example, by program provider 60). Some or all of the requests emanating from the viewing location 20 may be encrypted, and the system 300 includes components that allow the meter 27 to pass through these requests unaffected but at the same time, to decrypt the requests and process the requests off-line.

In Figure 2A, system 300 includes data collection engine 310, metrics estimation engine 320, and proxy 330.The data collection engine 310 and estimation engine process data received at the analytics service 70 to produce estimates of media consumption for a large population from which a panel (including panelist/viewer) is recruited.

The proxy 330 acts as a trusted certificate authority for the router 25–that is, the proxy is trusted by the media devices 24 and 26 (as well as other registered media devices of the viewer 22 and registered media devices of other panelists.

In operation, when the router 25 detects a secure (HTTPS) request from one of the media devices 24 or 26 to program provider 60, the router 25 notifies the service 70 (the notification going to the proxy 330) and sends the encrypted request to the service 70. The proxy 330 then issues a certificate with the private key of the media device providing the request. The certificate and private key allow the system 300 to decrypt the encrypted request and process its information off-line (e.g., log the information directly with the system 300) while the router 25 sends the originally-encrypted request, unaffected, to the program provider 60.

Figure 2B illustrates an alternate system that enables a router to decrypt encrypted Internet traffic sent between a client and a server. The functions of the components of Figure 2B are similar in many respects to those of Figure 2B. However, system 300 does not issue certificates with private keys. Instead, that function is entrusted to certificate authority module 28 installed on router 25. The router 25 then decrypts the request, and the meter 27 logs the data.

Subsequently, the router 25 may report the logged data to the system 300. However, in reporting the logged data, the router 25 encrypts the logged data (with a different key from that used to decrypt the request) before transmission to the analytics service 70.

Figures 3A – 3C are flowcharts illustrating example methods executed by the systems of Figures 2A and 2B.

Figure 3A illustrates method 400 in which proxy 330 is established at the server 74. In Figure 3A, method 400 begins when the router 25 receives a secure (HTTPS) request from media device 24. The request may be an Internet request submitted to program provider 60. In block 410, the router 25 examines the request header and other non-encrypted aspects of the request and

determines that the request is encrypted. In block 415, the router 25 passes a certificate/private key authorization to the proxy 330. In block 420, the router 25 passes the original request, encrypted, to program provider 60. In block 425, the router passes the encrypted request to the analytics service 70. The method 400 then ends.

Figure 3B illustrates method 500 in which the proxy 330 is established at the server 74. Method 500 begins in block 505 when the proxy 330 receives a signal from the router that a secure request from media device 24 should be decrypted and its content analyzed. In block 510, the proxy 330 issues a certificate and a private key. In block 515, the system 300 receives the encrypted request and decrypts using the private key. In block 520, the system 300 processes the decrypted request.

Figure 3C illustrates method 600 in which router 25 is established as a local certificate authority. Method 600 begins in block 605 when the router 25 receives an encrypted request from the media device 24. In block 610, the router 25 examines the header and other unencrypted parts of the request and determines the request is encrypted and should be decrypted and measured. In block 615, the router 25 issues a certificate with a private key. In block 620, the router 25 passes the request, unaffected, to the program provider 60. In block 625, the router 25 decrypts the request. In block 630, the meter 27 logs the data from the decrypted request. In block 635, the router encrypts the logged dataand sends to the server 74.

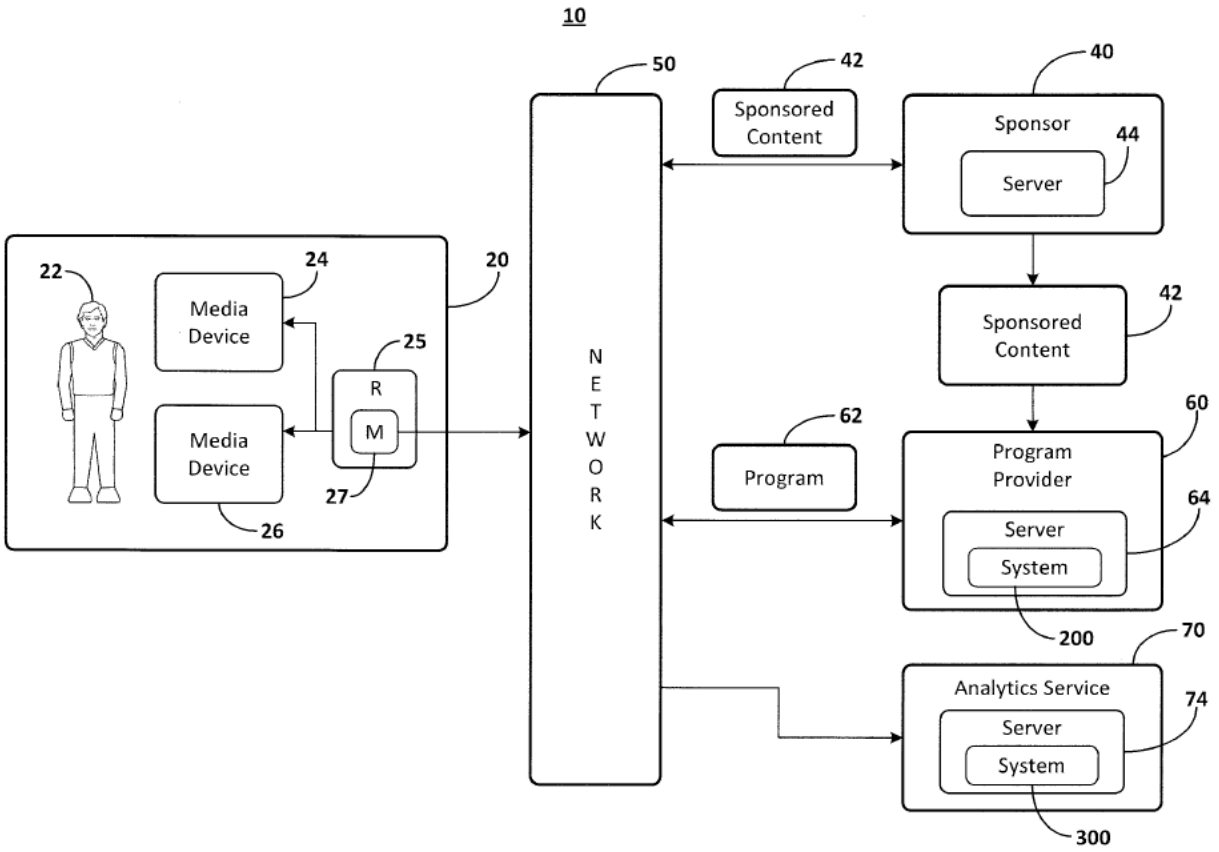

FIG. 1

Figure 1 illustrates an example of an environment in which encrypted traffic may be metered with a router.

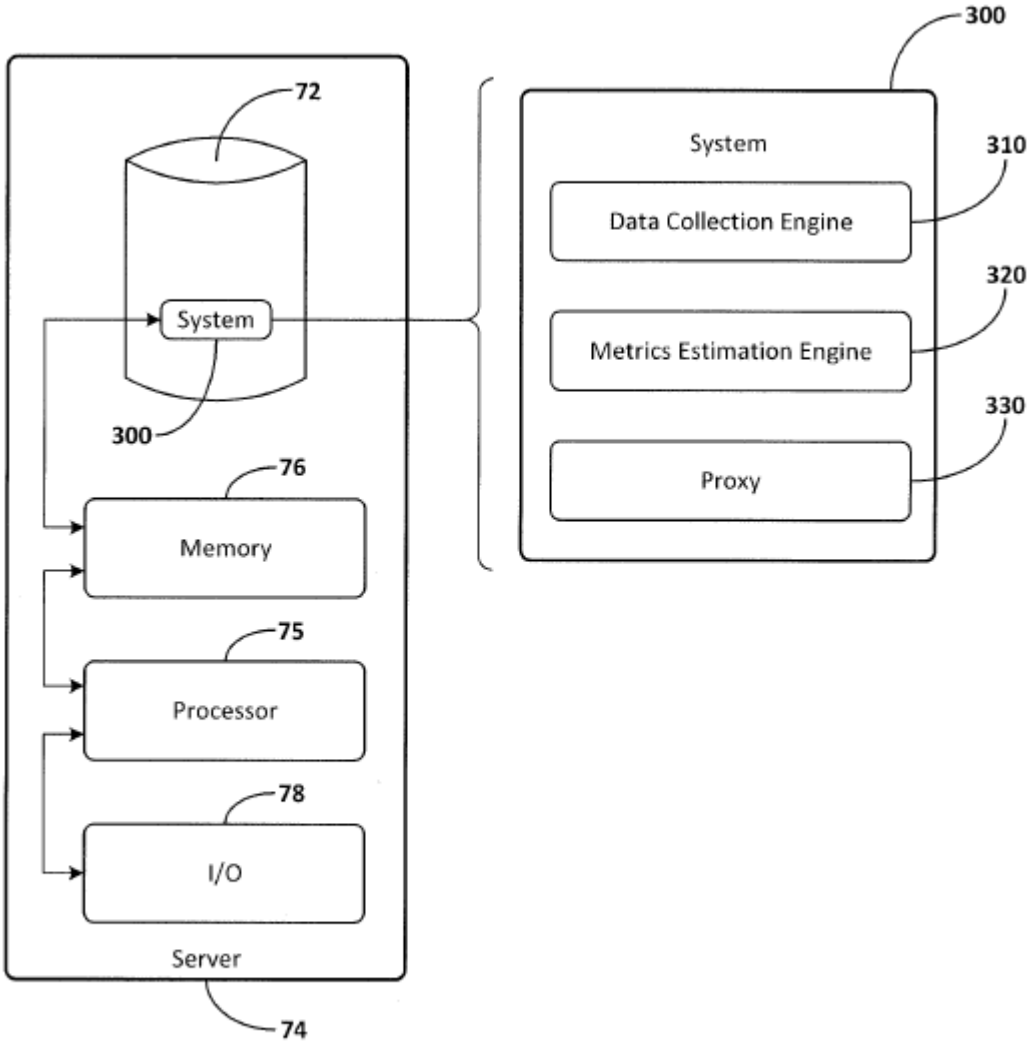

FIG. 2A

Figure 2A illustrates a system for metering of secure traffic at a router.

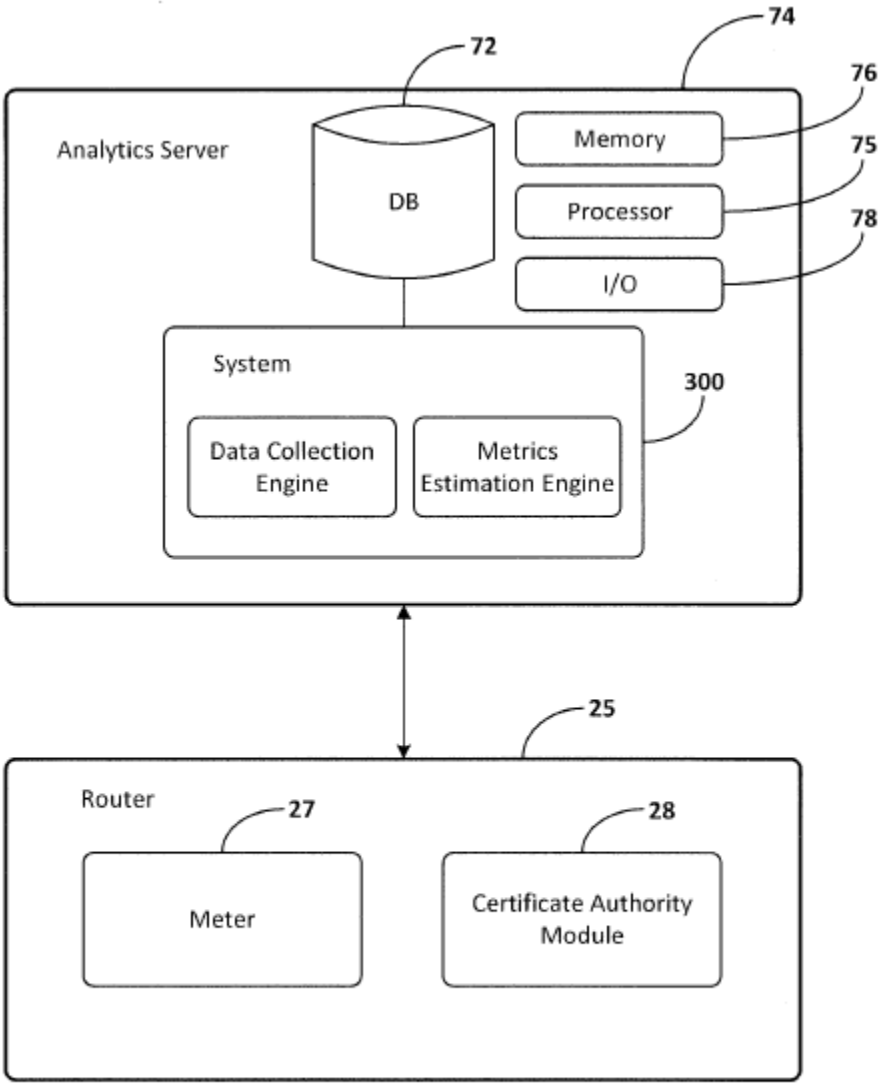

FIG. 2B

Figure 2B illustrates a system for metering of secure traffic at a router.

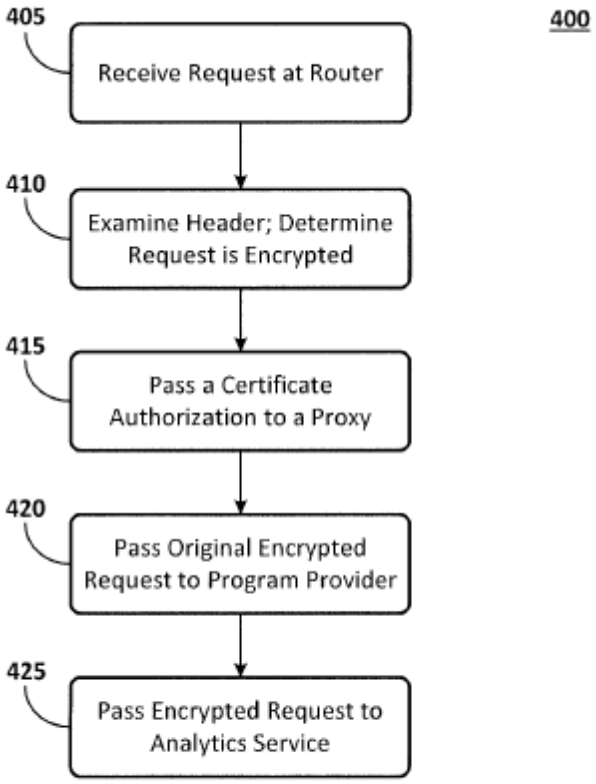

FIG. 3A

Figure 3A is a flowchart illustrating an example method executed by the systems of Figures 2A and 2B.

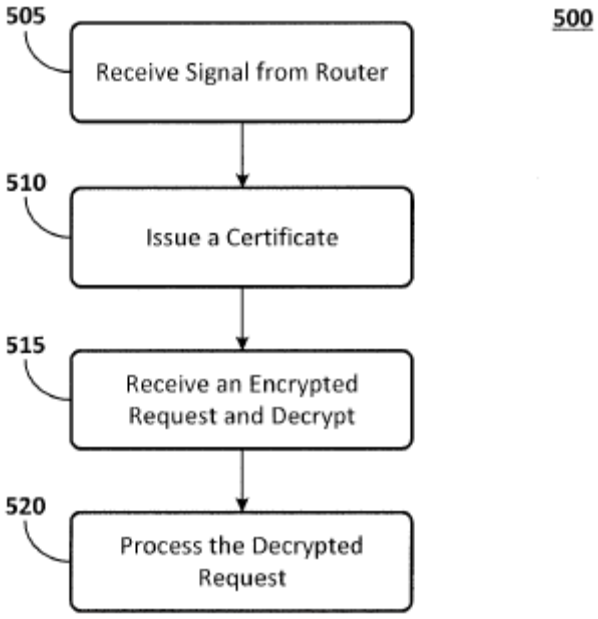

FIG. 3B

Figure 3B is a flowchart illustrating an example method executed by the systems of Figures 2A and 2B.

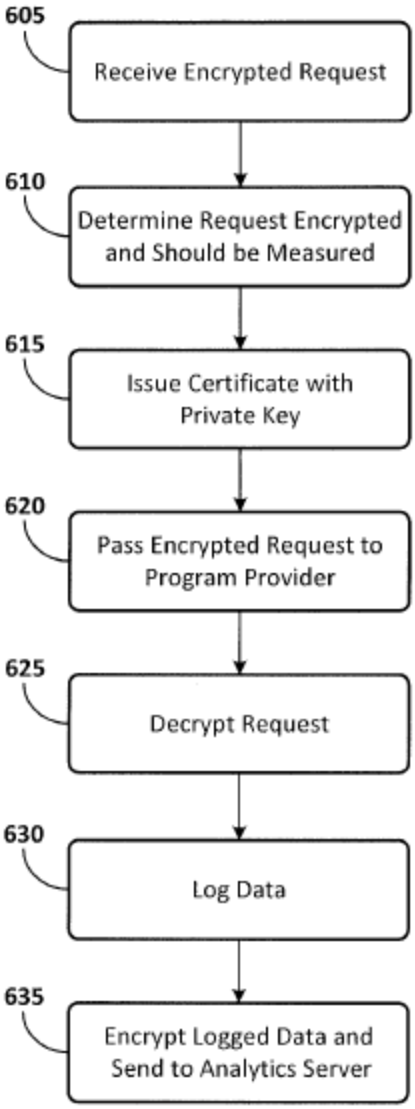

FIG. 3C

Figure 3C is a flowchart illustrating an example method executed by the systems of Figures 2A and 2B.