



- (51) International Patent Classification:
G06F 17/00 (2006.01)
- (21) International Application Number:
PCT/US2014/045826
- (22) International Filing Date:
8 July 2014 (08.07.2014)
- (25) Filing Language: English
- (26) Publication Language: English
- (30) Priority Data:
61/843,578 8 July 2013 (08.07.2013) US
- (71) Applicant: CUPP COMPUTING AS [NO/US]; 444 Ramona Street, Palo Alto, California 94301 (US).
- (72) Inventors: TOUBOUL, Shlomo; Main 6, Kefar Haim (IL). KAPLAN, Mark; 9/1 Emek Dotan St., 71701 Modi-in (IL).
- (74) Agents: SOCKOL, Marc, A. et al.; Sheppard, Mullin, Richter & Hampton LLP, 379 Lytton Avenue, Palo Alto, California 94301 (US).
- (81) Designated States (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM,

AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

- (84) Designated States (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CL, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Published:

— with international search report (Art. 21(3))



(54) Title: SYSTEMS AND METHODS FOR PROVIDING DIGITAL CONTENT MARKETPLACE SECURITY

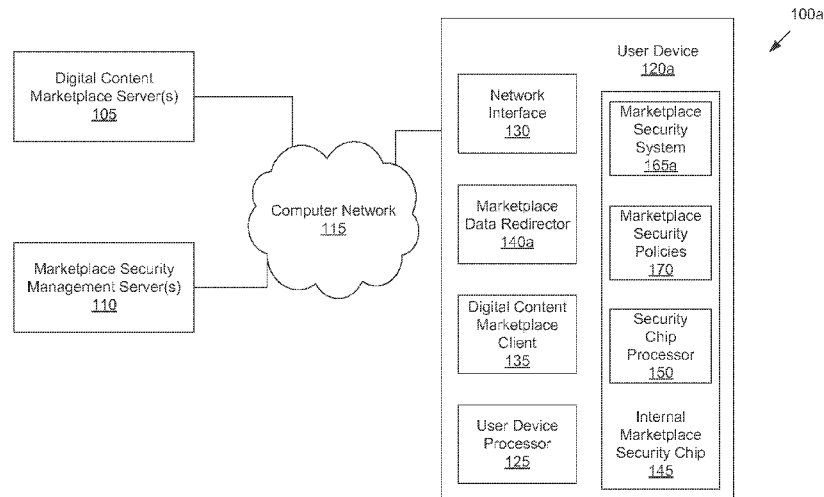


FIGURE 1A

(57) Abstract: A digital content marketplace filter engine may be configured to identify a communication between a digital content marketplace client and a digital content marketplace server. An analysis engine may be configured to review the communication against a digital content marketplace policy. A response engine configured to block, allow or modify the communication to conform to the digital content marketplace policy.

SYSTEMS AND METHODS FOR PROVIDING DIGITAL CONTENT MARKETPLACE SECURITY

TECHNICAL FIELD

[0001] The technical field relates to computer security systems and methods. More specifically, the technical field relates to systems and methods for providing security for a digital content marketplace.

BACKGROUND

[0002] Digital content marketplaces provide convenient distribution platforms for digital content. In many digital content marketplaces, a digital content marketplace client on an end user's device typically allows digital content to be downloaded and initially accessed by the device. Many mobile and traditional operating systems include or are affiliated with some form of digital content marketplace.

[0003] However, many digital content marketplaces face security issues, since many do not closely monitor publishers or digital content. These digital content marketplaces leave users vulnerable to digital content that contains malicious code. As a result, most digital content marketplaces provide little control for end users or Information Technology (IT) departments to further manage access. It would be helpful if systems and methods existed that could secure digital content marketplaces to protect end users from malicious code and allow end users and IT departments greater control.

SUMMARY

[0004] In a system, a digital content marketplace filter engine may be configured to identify a communication between a digital content marketplace client and a digital content marketplace server. An analysis engine may be configured to review the communication against a digital content marketplace policy. A response engine configured to block, allow or modify the communication to conform to the digital content marketplace policy.

[0005] In some embodiments, the communication comprises a search request for one or more digital content items. The communication may include search results in response to a search request for digital content items.

[0006] In an embodiment, the digital content marketplace policy may include a whitelist or a blacklist of digital content items. The digital content marketplace policy may include at least one attribute associated with each digital content item. The at least one attribute may include title, publisher, size, hardware requirements, metadata or tags. Moreover, the digital content marketplace policy may include at least one budget factor. Further, the at least one budget factor may include a maximum price per digital content item, a maximum budget per time period, or a maximum number of downloads per time period.

[0007] In various embodiments, the digital content marketplace policy includes at least one metric associated with each digital content item. The at least one metric includes number of downloads, user rating, or popularity.

[0008] In a method, communication between a digital content marketplace client and a digital content marketplace server may be identified. The communication may be reviewed against a digital content marketplace policy. The communication may be blocked, allowed, or modified to conform to the digital content marketplace policy.

[0009] In some embodiments, the communication comprises a search request for one or more digital content items. The communication may include search results in response to a search request for digital content items.

[0010] In an embodiment, the digital content marketplace policy may include a whitelist or a blacklist of digital content items. The digital content marketplace policy may include at least one attribute associated with each digital content item. The at least one

attribute may include title, publisher, size, hardware requirements, metadata or tags. Moreover, the digital content marketplace policy may include at least one budget factor. Further, the at least one budget factor may include a maximum price per digital content item, a maximum budget per time period, or a maximum number of downloads per time period.

[0011] In various embodiments, the digital content marketplace policy includes at least one metric associated with each digital content item. The at least one metric includes number of downloads, user rating, or popularity.

[0012] A system may include: means for identifying a communication between a digital content marketplace client and a digital content marketplace server; means for reviewing the communication against a digital content marketplace policy; and means for blocking, allowing or modifying the communication to conform to the digital content marketplace policy.

[0013] Other features and embodiments are apparent from the accompanying drawings and from the detailed description.

BRIEF DESCRIPTION OF THE DRAWINGS

- [0014] FIG. 1A depicts an example digital content marketplace security environment, according to some embodiments.
- [0015] FIG. 1B depicts an example digital content marketplace security environment, according to some embodiments.
- [0016] FIG. 1C depicts an example digital content marketplace security environment, according to some embodiments.
- [0017] FIG. 2 depicts an example marketplace security system, according to some embodiments.
- [0018] FIG. 3 depicts an example search request security analysis engine, according to some embodiments.
- [0019] FIG. 4 depicts an example search results security analysis engine, according to some embodiments.
- [0020] FIG. 5 depicts an example digital content security analysis engine, according to some embodiments.
- [0021] FIG. 6 depicts example security policies, according to some embodiments.
- [0022] FIG. 7 is a flowchart of an example security method for search requests directed to a digital content marketplace.
- [0023] FIG. 8 is a flowchart of an example security method for search results from a digital content marketplace.
- [0024] FIG. 9 is a flowchart of an example security method for digital content from a digital content marketplace accessed by the user device.
- [0025] FIG. 10 depicts an example of a search request and search results, according to some embodiments.
- [0026] FIG. 11 depicts an example digital device, according to some embodiments.

DETAILED DESCRIPTION

[0027] FIG. 1A depicts an example digital content marketplace security environment 100a, according to some embodiments. The digital content marketplace security environment 100a may include a digital content marketplace server 105, a marketplace security management server 110, a computer network 115, and a user device 120a. As will be discussed herein, the digital content marketplace security environment 100a uses the marketplace security system 165a and the marketplace security policies 170 to provide security for communications between the user device 120a and the digital content marketplace server 105.

[0028] The digital content marketplace server(s) 105 may include a digital device configured to distribute digital content to the user device 120a. “Digital content,” as referred to herein, may refer to any item of content that can be represented in a format compatible with a digital device. Examples of digital content include digital applications compatible with digital devices, digital books, digital music, and digital video. In some embodiments, the digital content marketplace server(s) 105 allows digital content publishers to publish digital content. Digital content publishers may include publishers affiliated with the entity that manages the digital content marketplace server(s) 105 as well as third-party publishers who are not affiliated with the entity that manages the digital content marketplace server(s) 105. The digital content marketplace server(s) 105 may allow users to access published digital content. For example, the digital content marketplace server(s) 105 may allow users to download, install, and/or stream digital applications, digital books, digital music, and digital video.

[0029] The digital content marketplace server(s) 105 may store and/or index digital content and may allow users to perform searches and take other actions with respect to digital content. More particularly, the digital content marketplace server(s) 105 may allow users to search for digital content that has been published. In some embodiments, the digital content marketplace server(s) 105 provides categories of digital content for users to browse. The digital content marketplace server(s) 105 may also provide metrics about digital content, such as sizes of digital content, resources consumed by digital content, ratings, downloads and other metrics about the digital content.

[0030] The digital content marketplace server(s) 105 may be associated with a specific operating platform of the user device 120, such a specific operating system of the user device

120. For example, the digital content marketplace server(s) 105 may be associated with a mobile operating system such as the iOS operating system, the Android operating system, and the Windows Phone operating system. The digital content marketplace server(s) 105 may also be associated with a Mac-based operating system, a Linux-based operating system, or a Windows-based operating system. The digital content marketplace server(s) 105 may be a server corresponding to the iOS App Store, the Mac App Store, the iTunes Store, the Kindle Store, the Google Play Store, the Windows Phone Store, or the Windows Store. In some embodiments, the digital content marketplace server(s) 105 need not be affiliated with an operating platform of the user device 120. For example, the digital content marketplace server(s) 105 may be maintained by a vendor of digital content (such as Amazon or Netflix) that distributes digital content but does not maintain an operating platform for the user device 120.

[0031] The marketplace security management server(s) 110 may include a digital device configured to manage the marketplace security system 165a and/or the marketplace security policies 170. The marketplace security management server(s) 110 may install the marketplace security system 165a and/or the marketplace security policies 170. The marketplace security management server(s) 110 may also maintain a master list of security policies with the latest security policy definitions. The master list of security policies may be used to update the marketplace security policies 170. In some embodiments, the marketplace security management server(s) 110 is managed by an entity that provides Information Technology (IT) services. Examples of such an entity include a member of the IT department of an enterprise, a parent of a user of the user device 120a, and an entity maintaining the security of the computer network 115. The entity providing the IT services corresponds to the entity managing the digital content marketplace server(s) 105 in an embodiment. Although FIG. 1A depicts the marketplace security management server(s) 110 as residing on a different device than the user device 120a, this depiction is by way of illustration only. In some embodiments, the marketplace security management server(s) 110 resides on the application marketplace server(s) 105, user device 120a, or some other known or convenient digital device. In specific implementations, the marketplace security management server(s) 110 include a standalone application, a set of Application Programming Interfaces (APIs), or a web portal.

[0032] The computer network 115 may include a medium that couples digital devices to one another. The computer network 115 may include technologies such as Ethernet,

802.11x, worldwide interoperability for microwave access WiMAX, 2G, 3G, 4G, CDMA, GSM, LTE, digital subscriber line (DSL), and/or the like. The computer network 115 may further include networking protocols such as multiprotocol label switching (MPLS), transmission control protocol/Internet protocol (TCP/IP), User Datagram Protocol (UDP), hypertext transport protocol (HTTP), simple mail transfer protocol (SMTP), file transfer protocol (FTP), and/or the like. The data exchanged over the computer network 115 can be represented using technologies and/or formats including hypertext markup language (HTML) and extensible markup language (XML). In addition, all or some links can be encrypted using conventional encryption technologies such as secure sockets layer (SSL), transport layer security (TLS), and Internet Protocol security (IPsec). Though element 115 is labeled a “computer network” in FIG. 1, it is noted that in various embodiments, the element 115 may refer to any medium that facilitates digital devices to other digital devices, or components of digital devices to other components of digital devices. In various embodiments, the element 115 may refer to a bus, cable, or other device used to couple components of a digital device to one another.

[0033] The user device 120a may include a digital device that allows a user to interact with digital content published by the digital content marketplace server(s) 105. The user device 120a may include a mobile phone, a Personal Data Assistant (PDA), a tablet computing device, a laptop computer, a desktop computer, or some combination thereof. The user device 120a may include a user device processor 125, a network interface 130, a digital content marketplace client 135, a marketplace data redirector(s) 140a, and an internal marketplace security chip 145.

[0034] The user device processor 125 may include a shared or dedicated processor configured to execute instructions loaded in a memory of the user device 120a. The user device processor 125 may include a general purpose processor that executes an operating system, processes, and applications loaded into the memory of the user device 120a. The user device processor 125 may provide instructions to execute the network interface 130, the digital content marketplace client 135, and the marketplace data redirector(s) 140a.

[0035] The network interface 130 may include hardware, firmware, and/or software configured to receive data from the computer network 115 and provide data to the computer

network 115. The network interface 130 may be compatible with the transmission protocols of the computer network 115 and other portions of the user device 120a.

[0036] The digital content marketplace client 135 may include hardware, firmware, and/or software configured to provide access to the digital content marketplace server(s) 105. In an embodiment, the digital content marketplace client 135 provides facilitates search for digital content on the digital content marketplace server(s) 105. The digital content marketplace client 135 may also receive search results of digital content on the digital content marketplace server(s) 105. The digital content marketplace client 135 may further provide the ability to view categories of digital content and metrics associated with digital content.

[0037] The digital content marketplace client 135 may facilitate installation and/or access of digital content on the user device 120a. For example, the digital content marketplace client 135 may download and initiate installation of applications from the digital content marketplace server(s) 105. As another example, the digital content marketplace client 135 may download or initiate streaming digital books, digital music, or digital video that the user device 120a has been authorized to access. The digital content marketplace client 135 may also facilitate installation of processes and/or applications (digital book readers, digital music or digital video players, etc.) that are required to access the digital content items. Examples of the digital content marketplace client 135 include portions of the iOS App Store client application, the Mac App Store client application, the iTunes client application, the Kindle Reader, the Google Play client application, the Windows Phone Store client application, and the Windows Store client application.

[0038] The marketplace data redirector(s) 140a may include hardware, firmware, and/or software to redirect the data going to and coming from the digital content marketplace client 135 to the internal marketplace security chip 145. In some embodiments, the marketplace data redirector(s) 140a identifies marketplace communications (Hypertext Transfer Protocol (HTTP) communications, API calls, Wi-Fi communications, Ethernet communications, Bluetooth communications, etc.) to and from the digital content marketplace client 135. The marketplace data redirector(s) 140a may further redirect these marketplace communications to the internal marketplace security chip 145. For instance, the marketplace data redirector(s) 140a may redirect to the internal marketplace security chip 145 all requests to search digital content in the digital content marketplace server(s) 105. As another example, the

marketplace data redirector(s) 140a may redirect to the internal marketplace security chip 145 results of the search requests coming from the digital content marketplace server(s) 105. As yet another example, the marketplace data redirector(s) 140a may redirect to the internal marketplace security chip 145 all requests to install, update, and/or modify digital content on the user device 120a. In various embodiments, the marketplace data redirector(s) 140a is implemented using a library of code that is executed by the user device processor 125.

[0039] Although FIG. 1A depicts the marketplace data redirector(s) 140a with a single element, it is noted that various embodiments, the marketplace data redirector(s) 140a includes multiple may employ more than one library of code. For example, the marketplace data redirector(s) 140a may include a first marketplace data redirector that processes all data passing between the digital content marketplace client 135 and the digital content marketplace server(s) 105. The first marketplace data redirector may redirect all search requests and search results relating to digital content to the internal marketplace security chip 145. The marketplace data redirector(s) 140a may also include a second marketplace data redirector that processes all data passing between the digital content marketplace client 135 and an installer on the user device 120a. The second marketplace data redirector may redirect requests to install, modify, or update digital content to the internal marketplace security chip 145.

[0040] The internal marketplace security chip 145 may include hardware coupled to an internal port or embedded within the user device 120a. In an embodiment, the internal marketplace security chip 145 is implemented as a non-volatile memory card, such as a Secure Digital (SD) card. For example, the internal marketplace security chip 145 may be implemented as a standard SD card, a miniSD card, or a microSD card. The internal marketplace security chip 145 may also be implemented in other known or convenient formats, such as in a SmartMedia (SM) or a Personal Computer Memory Card International Association (PCMCIA) card. The internal marketplace security chip 145 may include a security chip processor 150, a marketplace security system 165a, and marketplace security policies 170.

[0041] The security chip processor 150 may include a shared or dedicated processor configured to execute the processes associated with the internal marketplace security chip 145. The security chip processor 150 may be separate and independent of the user device processor 125 described herein. In an embodiment, the security chip processor 150 is a secure processor. More specifically, the security chip processor 150 may implement encryption and other

security algorithms to ensure the contents of the internal marketplace security chip 145 are protected from unauthorized access. The security chip processor 150 may store use secure memory of the internal marketplace security chip 145 for its operations. In an embodiment, the security chip processor 150 may provide instructions to execute the marketplace security system 165a.

[0042] The marketplace security system 165a may include hardware, firmware, and/or software to provide security for the data going to and coming from the digital content marketplace client 135. The marketplace security system 165a may be a miniature server, based on commercial hardware (with Intel's Xscale as the core), Linux OS and network services, and an open-source firewall. The marketplace security system 165a may be based on an embedded OS, such as a version of embedded Linux. The marketplace security system 165a may receive the marketplace communications from the marketplace data redirector(s) 140a. The marketplace security system 165a may further evaluate the marketplace communications in accordance with the marketplace security policies 170, as describe herein. Based on the marketplace security policies 170, the marketplace security system 165a may determine whether to allow, deny, or modify the marketplace communications based on the marketplace security policies 170. To continue the foregoing examples, the marketplace security system 165a may determine whether to allow, deny, or modify a particular search request and/or particular search results based on the marketplace security policies 170. The marketplace security system 165a may further determine whether to allow, deny, or modify installation of digital content based on the marketplace security policies 170. In an embodiment, the marketplace security system 165a may be executed by the security chip processor 150, and may be controlled by the marketplace security management server(s) 110. FIG. 2 shows the marketplace security system 165a in greater detail.

[0043] The marketplace security policies 170 may include hardware, firmware, and/or software datastores configured to support the marketplace security system 165a. In an embodiment, the marketplace security policies 170 include policies related to the types of search requests, search results, and digital content that are to be allowed, denied, or modified. For example, the marketplace security policies 170 may include policies related to acceptable and/or unacceptable search requests and acceptable and/or unacceptable search results. The marketplace security policies 170 may also include policies related to acceptable and/or unacceptable digital content types, policies related to malware definitions, and policies that

implement content analysis and risk assessment definitions. In various embodiments, the marketplace security policies 170 include policies related to of acceptable and/or unacceptable metrics about digital content. The marketplace security policies 170 may further include policies related to Digital Rights Management (DRM) definitions and/or other information relating to whether digital content is to be allowed, denied, or modified. The marketplace security policies 170 may be controlled and may receive updates from the marketplace security management server(s) 110. FIG. 6 shows the marketplace security policies 170 in greater detail.

[0044] FIG. 1B depicts an example digital content marketplace security environment 100b, according to some embodiments. The digital content marketplace security environment 100b includes a digital content marketplace server 105, a marketplace security management server 110, a computer network 115, and a user device 120b. The digital content marketplace server 105, the marketplace security management server 110, and the computer network 115 may be similar to their counterparts in FIG. 1A.

[0045] The user device 120b includes a user device processor 125, a network interface 130, a digital content marketplace client 135, a marketplace security system 165, and marketplace security policies 170. The user device processor 125, the network interface 130 and the digital content marketplace client 135 may be similar to their counterparts in FIG. 1A.

[0046] In an embodiment, the marketplace security system 165b implements the features of the marketplace data redirector(s) 140a and the marketplace security system 165a, which are discussed in conjunction with FIG. 1A. More specifically, the marketplace security system 165b may include hardware, firmware, and/or software to intercept data going to and coming from the digital content marketplace client 135. The marketplace security system 165b may further include hardware, firmware, and/or software to provide security for the data going to and coming from the digital content marketplace client 135. In various embodiments, the marketplace security system 165b may be executed using the user device processor 125. In an embodiment, the marketplace security policies 170 are stored in memory of the user device 120b. The user device 120b may store the marketplace security policies 170 using portions of memory secured from unauthorized access.

[0047] FIG. 1C depicts an example digital content marketplace security environment 100c, according to some embodiments. The digital content marketplace security environment

100c includes a digital content marketplace server 105, a marketplace security management server 110, a computer network 115, a user device 120c, and an external marketplace security chip 155. The digital content marketplace server 105, the marketplace security management server 110, and the computer network 115 are similar to their counterparts in FIG. 1A.

[0048] The user device 120c includes a user device processor 125, a network interface 130, a digital content marketplace client 135, and a marketplace data redirector(s) 140c. The user device processor 125, the network interface 130 and the digital content marketplace client 135 may be similar to their counterparts in FIG. 1A. In an embodiment, the marketplace data redirector(s) 140c includes hardware, firmware, and/or software to redirect the data going to and coming from the digital content marketplace client 135 to the external marketplace security chip 155.

[0049] The external marketplace security chip 155 may include hardware coupled to an external port of the user device 120c. In some embodiments, the external marketplace security chip 155 is coupled to the user device 120c using a Universal Serial Bus (USB) port, a network interface, or a data port.

[0050] The external marketplace security chip 155 may include an external security processor 160, a marketplace security system 165c, and marketplace security policies 170. The external security processor 160 may include shared or dedicated processor configured to execute the processes associated with the external marketplace security chip 155. The external security processor 160 may be separate and independent of the user device processor 125, and may comprise a secure processor. The external security processor 160 may implement encryption and other security algorithms to ensure the contents of the external marketplace security chip 155 are protected from unauthorized access. The external security processor 160 may store use secure memory of the external marketplace security chip 155 for its operations. In an embodiment, the external security processor may provide instructions to execute the marketplace security system 165c. The marketplace security system 165c and the marketplace security policies 170 may operate similarly to their counterparts in FIG. 1A.

[0051] FIG. 2 depicts an example marketplace security system 165, according to some embodiments. The marketplace security system 165 may correspond to the marketplace security system 165a, shown in FIG. 1A; the marketplace security system 165b, shown in FIG. 1B; or the marketplace security system 165c, shown in FIG. 1C. The marketplace security

system 165 may include a marketplace data redirector interface engine 205, a digital content marketplace filter engine 210, a search request security analysis engine 215, a security policy interface engine 220, a search request response engine 225, a search results security analysis engine 230, a search results response engine 235, a digital content security analysis engine 240, a digital content security response engine 245, and a digital content marketplace client interface engine 250. One or more of the engines in the marketplace security system 165 may include shared or dedicated hardware, software, and/or firmware configured to perform functions described herein. In various embodiments, the marketplace security system 165 is implemented using a library of code that is executed by the user device processor 125. The marketplace security system 165 may be implemented using hardware, software, and/or firmware that can interface with the marketplace data redirector(s) 140 and/or the digital content marketplace client 135, shown in FIGS. 1A, 1B, and 1C.

[0052] The marketplace data redirector interface engine 205 may interface with the marketplace data redirector(s) 140 (shown as the marketplace data redirector(s) 140a in FIG. 1A and the marketplace data redirector(s) 140c in FIG. 1C). The marketplace data redirector interface engine 205 may send data to and receive data from the marketplace data redirector(s) 140. In some embodiments, the marketplace data redirector interface engine 205 incorporates some or all of the features of the marketplace data redirector(s) 140. For example, in embodiments (such as the embodiment depicted in FIG. 1B) where the user device 120 does not have a marketplace data redirector(s) 140, the marketplace data redirector interface engine 205 may identify marketplace communications to and from the digital content marketplace client 135 and may redirect these marketplace communications to the digital content marketplace filter engine 210. The marketplace data redirector interface engine 205 may provide to the digital content marketplace filter engine 210 requests to search digital content in the digital content marketplace server(s) 105, results of the search requests coming from the digital content marketplace server(s) 105, and/or requests to install and/or modify digital content on the user device 120a.

[0053] The digital content marketplace filter engine 210 may filter communications to and communications from the digital content marketplace client 135. More specifically, the digital content marketplace filter engine 210 may identify which communications fall under the marketplace security policies 170. For instance, the digital content marketplace filter engine 210 may filter search requests relating to searches for digital content on the digital content

marketplace server(s) 105. As another example, the digital content marketplace filter engine 210 may filter the results of searches for digital content. As yet another example, the digital content marketplace filter engine 210 may filter requests to install, update, modify, etc. digital content. The digital content marketplace filter engine 210 may provide filtered communications to the other engines of the marketplace security system 165. For example, the digital content marketplace filter engine 210 may provide search requests to the search request security analysis engine 215. The digital content marketplace filter engine 210 may further provide results of search requests to the search results security analysis engine 230. Moreover, the digital content marketplace filter engine 210 may provide requests to install, update, modify, etc. digital content to the digital content security analysis engine 240.

[0054] The search request security analysis engine 215 may identify portions of a search request that are relevant to determining whether the search request is likely to obtain unauthorized digital content. In some embodiments, a search request is in plain text format. In these embodiments, the search request security analysis engine 215 parses the plain text of the search request, and identifies digital content names, digital content publishers, and/or digital content categories. The search request security analysis engine 215 may further identify levels and/or types of access to the digital content marketplace server(s) 105 sought by a search request. The search request security analysis engine 215 may analyze whether the search request requests paid digital content and/or how much those items of paid digital content cost. The search request security analysis engine 215 may provide the information from the search requests to the security policy interface engine 220. FIG. 3 shows the search request security analysis engine 215 in greater detail.

[0055] The security policy interface engine 220 may provide relevant portions of the marketplace security policies 170 to the other engines of the marketplace security system 165. More specifically, the security policy interface engine 220 may obtain portions of the marketplace security policies 170 relating to the types of digital content marketplace search requests and/or search results that should be allowed or denied. The security policy interface engine 220 may also obtain portions of the marketplace security policies 170 to analyze digital content, as described further herein. In some embodiments, the security policy interface engine 220 is used to update the marketplace security policies 170. More specifically, the security policy interface engine 220 may receive updates to definitions, white- and/or black-lists, and/or other portions of the marketplace security policies 170 from the marketplace security

management server(s) 110. The security policy interface engine 220 may provide these updates to the marketplace security policies 170 to ensure the security policies reflect the most recent definitions and lists.

[0056] The search request response engine 225 may decide whether a search request violates the marketplace security policies 170. The search request response engine 225 may interface with the search request security policy 605, shown in FIG. 6 and discussed further herein. For example, the search request response engine 225 may compare digital content names, publishers, and/or categories in the search request with white and/or black lists in the marketplace security policies 170. The search request response engine 225 may further compare the levels and/or types of access sought by a search request with levels and/or types of access deemed acceptable by the marketplace security policies 170. In some embodiments, the search request response engine 225 determines whether a search request for paid content is deemed acceptable by the marketplace security policies 170.

[0057] The search request response engine 225 may provide instructions to allow, deny, or modify the search request based on whether the search request violates the marketplace security policies 170. The search request response engine 225 may deny an unpermitted search request access to the computer network 115 and/or the digital content marketplace server(s) 105. The search request response engine 225 may also replace an unpermitted search request with another search request that is similar to the unpermitted search request, but that is in conformance with the marketplace security policies 170. As an example, the search request response engine 225 may replace search terms related to an unpermitted search request for network optimizing software with new search terms seeking a permitted type of software. As another example, the search request response engine 225 may remove inappropriate search terms (e.g., gambling-oriented or adult-oriented search terms) from a search. In some embodiments, the search request response engine 225 instructs the digital content marketplace client interface engine 250 whether a particular search request is to be allowed, denied, or modified.

[0058] The search results security analysis engine 230 may identify portions of search results that are relevant to determining whether a set of search results violates the marketplace security policies 170. In some embodiments, the search results security analysis engine 230 parses search results from the digital content marketplace server(s) 105. The search results

security analysis engine 230 may further analyze the parsed search results for digital content names, digital content publishers, digital content categories, levels and/or types of access sought by digital content, whether digital content is paid or free, how much paid digital content would cost, metrics related to the digital content, etc. The search results security analysis engine 230 may provide the relevant portions of search results to the search results response engine 235 and/or the digital content security analysis engine 240. FIG. 4 shows the search results security analysis engine 230 in greater detail.

[0059] The search results response engine 235 may decide whether specific search results violate the marketplace security policies 170. The search results response engine 235 may interface with the search results security policy 610, shown in FIG. 6 and discussed further herein. In some embodiments, the search results response engine 235 analyzes the digital content names, digital content publishers, digital content categories, levels and/or types of access sought by digital content, whether digital content is paid or free, how much paid digital content would cost, etc. provided by the search results security analysis engine 230 for compliance with the marketplace security policies 170. The search results response engine 235 may determine whether to allow, deny, or modify specific search results. The search results response engine 235 may suggest specific modifications to the search results. For example, the search results response engine 235 may remove unauthorized digital content identifiers or may substitute authorized digital content identifiers for unauthorized digital content in a search results page. The search results response engine 235 may instruct the digital content marketplace client interface engine 250 accordingly.

[0060] The digital content security analysis engine 240 may analyze digital content for compliance with the marketplace security policies 170. In some embodiments, the digital content security analysis engine 240 verifies attributes of digital content. “Attributes” of digital content may include properties of digital content or anything that can provide a description of digital content. Examples of attributes of digital content include titles, publishers, sizes, hardware requirements, metadata, and/or tags associated with digital content. The digital content security analysis engine 240 may also analyze digital content for malware, perform content analysis and/or risk assessment algorithms, and determine appropriate digital content metrics. Digital content “metrics,” as used herein, may refer to measures related to how digital content is distributed. Examples of digital content metrics include popularity of digital content, ratings related to digital content, and the number of times digital content has

been downloaded. The digital content security analysis engine 240 may further evaluate digital content for compliance with DRM rules (e.g., to ensure digital content is only accessed with an appropriate license). In various embodiments, the digital content security analysis engine 240 provides its analysis of the digital content before the digital content is installed on the user device 120.

[0061] The digital content security response engine 245 may decide whether specific digital content violates the marketplace security policies 170. The digital content security response engine 245 may interface with one or more of the digital content attribute verification policy 615, the digital content malware analysis security policy 620, the content analysis policy 625, and the digital rights management policy 630, shown in FIG. 6 and discussed further herein. The digital content security response engine 245 may verify attributes (names, publishers, publication dates, costs, etc.) of digital content, may evaluate the digital content for malware, and may perform content analysis on the digital content. The digital content security response engine 245 may also instruct the digital content marketplace client interface engine 250 to block and/or modify installation of non-compliant digital content. As a result, the digital content security analysis engine 240 may advantageously prevent installation of digital content that does not comply with the marketplace security policies 170. FIG. 5 shows the digital content security analysis engine 240 in greater detail.

[0062] The digital content marketplace client interface engine 250 may interface with the digital content marketplace client 135. The digital content marketplace client interface engine 250 may provide modified search requests, modified search results, and/or modified digital content to the user device 120 to display digital content that complies with the marketplace security policies 170. For example, the digital content marketplace client interface engine 250 may provide modified search requests to the user device 120 based on instructions from the search request response engine 225. As another example, the digital content marketplace client interface engine 250 may provide modified search results to the user device 120 based on corresponding instructions from the search results response engine 235. Moreover, the digital content marketplace client interface engine 250 may provide modified digital content to the user device 120 based on instructions from the digital content security response engine 245. In some embodiments, the digital content marketplace client interface engine 250 may instruct security software on the user device 120 to modify the search request, search results and/or digital content, before the digital content is presented and/or installed.

[0063] FIG. 3 depicts an example search request security analysis engine 215, according to some embodiments. The search request security analysis engine 215 may include a search request parsing engine 305, a search request attribute analysis engine 310, a search request access analysis engine 315, a search request budget analysis engine 320, search request metrics analysis engine 325, and a search request digital rights management engine 330. One or more of the engines in the search request security analysis engine 215 may include shared or dedicated hardware, software, and/or firmware configured to perform functions described herein.

[0064] The search request parsing engine 305 may parse a search request for language related to digital content, for digital content access levels, and for digital content budgets. In an embodiment, the search request is in plain text format. The search request parsing engine 305 may remove irrelevant characters (non-alphanumeric symbols, server names, hypertext functional strings, etc.) when performing parsing. The search request parsing engine 305 may provide the parsed search request to the search request attribute analysis engine 310, the search request access analysis engine 315, and/or the search request budget analysis engine 320.

[0065] The search request attribute analysis engine 310 may extract attributes of digital content from a parsed search request. For example, the search request attribute analysis engine 310 may identify digital content names, digital content publishers, the publication date of digital content, and digital content categories in a parsed search request. The search request attribute analysis engine 310 may provide the extracted information to the search request response engine 225 as discussed herein.

[0066] The search request access analysis engine 315 may analyze whether the search request is requesting digital content requiring secure resources of the user device 120. More specifically, the search request access analysis engine 315 may analyze whether the search request is seeking digital content that requires additional security to install (e.g., digital content that can modify operating system processes, digital content that interfaces with device drivers, digital content that is automatically loaded on startup, and digital content that requires administrator privileges to install). The search request access analysis engine 315 may provide the extracted information to the search request response engine 225 as discussed herein.

[0067] The search request budget analysis engine 320 may analyze whether the search request seeks paid content. In an embodiment, the search request budget analysis engine 320

analyzes whether the search request contains the word “free” (or some other word indicating free content), the word “paid” (or other word indicating paid content), currency symbols, etc. The search request budget analysis engine 320 may further evaluate the search request for the presence of words that indicate paid and/or premium content, such as “paid,” “purchase,” or “premium.” The search request budget analysis engine 320 may provide the extracted information to the search request response engine 225 as discussed herein.

[0068] The search request metrics analysis engine 325 may analyze metrics related to a search request. The search request metrics analysis engine 325 may identify installation sizes and/or memory and other resources digital content in a search request is likely to consume. The search request metrics analysis engine 325 may further identify ratings (e.g., points, stars likes, positive reviews, and/or negative reviews). The search request metrics analysis engine 325 may provide the extracted information to the search request response engine 225, as discussed herein.

[0069] The search request digital rights management engine 330 may evaluate a search request for compliance with digital rights management policies. In some embodiments, the search request digital rights management engine 330 evaluates digital content in search requests for the presence or absence of watermarks, licenses, and other tamper-prevention technologies. The search request digital rights management engine 330 may interface with the digital rights management policy 630, shown in FIG. 6 and discussed herein. In various embodiments, the search request digital rights management engine 330 provides information about whether a search request complies with the digital rights management policy 630 to the search request response engine 225, as discussed herein.

[0070] FIG. 4 depicts an example search results security analysis engine 230, according to some embodiments. The search results security analysis engine 230 may include a search results parsing engine 405, a search results attribute analysis engine 410, a search results access analysis engine 415, a search results budget analysis engine 420, a search results metrics analysis engine 425, and a search results digital rights management engine 430. One or more of the engines in the search results security analysis engine 230 may include shared or dedicated hardware, software, and/or firmware configured to perform functions described herein.

[0071] The search results parsing engine 405 may parse search results for information related to digital content, for digital content access levels, for digital content budgets, and for digital content metrics. In some embodiments, the search results are in a binary encoded format. The search results parsing engine 405 may convert the search results to a text string, may remove irrelevant characters, and may extract the relevant information from the search results. The search results parsing engine 405 may provide the parsed search results to the search results attribute analysis engine 410, the search results access analysis engine 415, the search results budget analysis engine 420, and/or the digital content metrics analysis engine.

[0072] The search results attribute analysis engine 410 may extract information about digital content (e.g., digital content names, digital content publishers, and digital content categories) provided by the search results. The search results attribute analysis engine 410 may provide the extracted information to the search results response engine 235 as discussed herein.

[0073] The search results access analysis engine 415 may analyze whether the search results include digital content requiring secure resources of the user device 120. The search results access analysis engine 415 may determine whether search results are providing digital content that requires additional security to install. The search results access analysis engine 415 may provide the extracted information to the search results response engine 235 as discussed herein.

[0074] The search results budget analysis engine 420 may analyze whether the search results include paid content, and if so, prices and other information related to the paid content. More specifically, the search results budget analysis engine 420 may analyze whether the search results include the words “free” or “paid,” currency symbols, etc. The search results budget analysis engine 420 may provide the extracted information to the search results response engine 235 as discussed herein.

[0075] The search results metrics analysis engine 425 may analyze metrics related to digital content in the search results. More specifically, the search results metrics analysis engine 425 may identify installation sizes and/or memory and other resources digital content is likely to consume. The search results metrics analysis engine 425 may further identify ratings related to digital content. For example, the search results metrics analysis engine 425 may identify points, stars, or likes digital content has received. The search results metrics analysis

engine 425 may further identify positive and/or negative reviews of digital content. The search results metrics analysis engine 425 may provide the extracted information to the search results response engine 235 as discussed herein.

[0076] The search results digital rights management engine 430 may evaluate search results for compliance with digital rights management policies. In some embodiments, the search results digital rights management engine 430 evaluates digital content in search results for the presence or absence of watermarks, licenses, and other tamper-prevention technologies. For example, the search results digital rights management engine 430 may identify pirated or tampered digital content in search results. The search results digital rights management engine 430 may interface with the digital rights management policy 630, shown in FIG. 6 and discussed herein. In various embodiments, the search results digital rights management engine 430 provides information about whether search results comply with the digital rights management policy 630 to the search results response engine 235, as discussed herein.

[0077] FIG. 5 depicts an example digital content security analysis engine 240, according to some embodiments. The digital content security analysis engine 240 may include a attribute verification engine 505, a malware analysis engine 510, a content analysis engine 515, and a digital rights management engine 520. One or more of the engines in the digital content security analysis engine 240 may include shared or dedicated hardware, software, and/or firmware configured to perform functions described herein.

[0078] The attribute verification engine 505 may verify attributes of digital content based on known attributes of digital content. In an embodiment, the attribute verification engine 505 may interface with the digital content attribute verification policy 615, shown in FIG. 6 and discussed further herein. The attribute verification engine 505 may verify the title of digital content with titles known in the marketplace security policies 170 to correspond to the digital content. In some embodiments, the attribute verification engine 505 verifies a publisher of digital content in accordance with the security policy. The attribute verification engine 505 may further verify digital content descriptions or other attributes. The attribute verification engine 505 may provide the digital content security response engine 245 with information relating to whether or not digital content was successfully verified.

[0079] The malware analysis engine 510 may analyze digital content for malware. The malware analysis engine 510 may interface with the digital content malware analysis security

policy 620, shown in FIG. 6 and discussed further herein. The malware analysis engine 510 may perform a virus scan of digital content. The malware analysis engine 510 may also analyze digital content for the presence of spyware, Trojan horses, keylogging software, adware, worms, and other types of malware. The malware analysis engine 510 may further perform Uniform Resource Locator (URL) categorization and/or filtering to limit access to unauthorized categories of URLs. In some embodiments, the malware analysis engine 510 verifies scripts, controls, and/or components of digital content in accordance with the marketplace security policies 170. The malware analysis engine 510 may provide the digital content marketplace client interface engine 250 with information relating to whether the digital content contained malware, and if so, the types of remedial actions to be taken. The malware analysis engine 510 may, for instance, recommend digital content be cleaned of malware, or digital content not be installed at all. The malware analysis engine 510 may provide information about the malware analysis to the digital content security response engine 245, as discussed herein.

[0080] The content analysis engine 515 may analyze digital content for the presence of content types that could compromise the security of the user device 120. The content analysis engine 515 may interface with the content analysis policy 625, shown in FIG. 6 and discussed further herein. The content analysis engine 515 may further analyze whether text or pictures in digital content contains inappropriate materials, such as gambling-oriented or adult-oriented materials. The content analysis engine 515 may provide the digital content marketplace client interface engine 250 with information relating to whether or not the digital content should be installed, cleaned, or modified. The content analysis engine 515 may provide content information to the digital content security response engine 245, as discussed herein.

[0081] The digital rights management engine 520 may evaluate digital content for compliance with digital rights management policies. In some embodiments, the digital rights management engine 520 evaluates digital content for the presence or absence of watermarks, licenses, and other tamper-prevention technologies. The digital rights management engine 520 may further identify pirated or tampered digital content. The digital rights management engine 520 may interface with the digital rights management policy 630, shown in FIG. 6 and discussed herein. In various embodiments, the digital rights management engine 520 provides information about whether digital content with the digital rights management policy 630 to the digital content security response engine 245, as discussed herein.

[0082] FIG. 6 depicts example marketplace security policies 170, according to some embodiments. The marketplace security policies 170 may include a search request security policy 605, a search results security policy 610, a digital content attribute verification policy 615, a digital content malware analysis security policy 620, a content analysis policy 625, and a digital rights management policy 630.

[0083] The search request security policy 605 may include a policy having white- and/or black-lists related to digital content marketplace search requests. For instance, the search request security policy 605 may include white- and/or black-lists of specific digital content or digital content publishers. The search request security policy 605 may further include rules relating to acceptable and/or unacceptable search words, phrases, and/or terms. For instance, the search request security policy 605 may provide lists that filtering of inappropriate search terms. In some embodiments, the search request security policy 605 includes rules relating to acceptable and/or unacceptable resources digital content in search requests may potentially require. More specifically, the search request security policy 605 may include lists of maximum allowed sizes of digital content; and maximum processor, memory, and/or network utilization allowed. The search request security policy 605 may further include rules relating to acceptable and/or unacceptable budgets the digital content in search requests may potentially require. As a result, the search request security policy 605 may include rules that specify whether paid content is allowed, or specify maximum allowable prices of paid digital content.

[0084] The search results security policy 610 may include a policy having security rules relating to authorized and/or unauthorized digital content marketplace search results. The search results security policy 610 may include security rules relating to authorized and/or unauthorized digital content, digital content publishers, words, terms, phrases, resources, and budgets. The search results security policy 610 may further include security rules relating to authorized and/or unauthorized metrics. More specifically, the search results security policy 610 may include security rules relating to authorized and/or unauthorized installation sizes, memory, ratings, points, stars, number of downloads and positive and/or negative reviews.

[0085] The digital content attribute verification policy 615 may include a policy containing definitions of verified attributes of digital content. The digital content attribute verification policy 615 may include titles of digital content, the names of publishers of digital

content, digital content descriptions, and other information that can be used to verify the identity of digital content. Some or all of this information may be obtained from

[0086] The digital content malware analysis security policy 620 may include a policy having malware definitions. In an embodiment, the digital content malware analysis security policy 620 includes antivirus and antispyware policies based on Clam Antivirus (AV), and/or additional antivirus and antispyware engines, such as McAfee, Kaspersky, Pandamay, or other free or subscription-based engines. The digital content malware analysis security policy 620 may further include Intrusion Detection System (IDS) and/or Intrusion Prevention System (IPS) policies to inspect signatures, protocols, and anomalies in digital content. The digital content malware analysis security policy 620 may also include URL Categorization Filtering policies that filter categories of URLs, such as gambling, news, adult content, webmail, etc.

[0087] The content analysis policy 625 may include a policy containing definitions of malicious content types. The content analysis policy 625 may include scripts, controls, components, etc. that are known to be malicious. The content analysis policy 625 may further include definitions that can identify gambling-oriented or adult-oriented materials in digital content. In some embodiments, the content analysis policy 625 implements dedicated High Risk Content Filtering (HRCF) algorithms that perform deep content analysis to verify content types. For example, the content analysis policy 625 may detect whether mimes, ActiveX controls, or scripts in digital content are different from what they say they are. The content analysis policy 625 may include definitions common to the digital content malware analysis security policy 620 for automatic rule adjustment based on URL categories. More specifically, the content analysis policy 625 may analyze digital content associated with higher risk URLs more stringently than digital content associated with lower risk URLs. In some embodiments, the content analysis policy 625 includes policies to strip pieces of malicious code from digital content.

[0088] The digital rights management policy 630 may include a policy relating to digital rights management. The digital rights management policy 630 may include information about watermarks or other technology that limits access to digital content without an appropriate license.

[0089] FIG. 7 is a flowchart of an example method 700 of providing security to a user device for search requests directed to a digital content marketplace. The method 700 is

discussed in conjunction with the elements of the digital content marketplace security environment 100, the marketplace security system 165, and the search request security analysis engine 215, shown in FIGS. 1-3. It is noted the steps in FIG. 7 are by way of illustration only, and that the method 700 may include elements not explicitly depicted, and that all elements are not necessary to perform the method 700.

[0090] At step 705, the digital content marketplace filter engine 210 identifies a search request directed to the digital content marketplace server(s) 105. More specifically, the digital content marketplace filter engine 210 may receive a character string corresponding to a search request. The character string may have been manually entered into a user interface of the digital content marketplace client 135 or may have been automatically generated by a process of the digital content marketplace client 135. In some embodiments, the search request includes language about digital content that is being sought. For example, the search request may include language such as the title of the digital content, the publisher of the digital content, or the publication date of the digital content.

[0091] At step 710, the search request parsing engine 305 parses the search request for language to analyze with a marketplace security policy, such as the marketplace security policies 170. The search request parsing engine 305 may parse the search request for relevant characters and/or character strings and may remove irrelevant characters, whitespaces, etc. from the search request. The search request parsing engine 305 may provide the parsed search request to one or more of the search request attribute analysis engine 310, the search request access analysis engine 315, and the search request budget analysis engine 320.

[0092] At step 715, the search request attribute analysis engine 310 analyzes the language for attributes of digital content to be evaluated for compliance with the marketplace security policy. More particularly, the search request attribute analysis engine 310 may identify the digital content names, publishers, publication dates, and categories in the language of the parsed search request.

[0093] At step 720, the search request access analysis engine 315 analyzes the language for a level of access sought by digital content to be evaluated for compliance with the marketplace security policy. In an embodiment, the search request access analysis engine 315 may review the parsed language of the search request to see if the search request is seeking digital content that requires additional security to install. The search request access analysis

engine 315 may provide extracted access level information to the search request response engine 225.

[0094] At step 725, the search request budget analysis engine 320 analyzes the language for a budget factors associated with digital content to be evaluated for compliance with the marketplace security policy. More specifically, the search request budget analysis engine 320 may analyze the language of the parsed search request for words that indicate paid and/or free content, currency symbols, or other language indicating budget factors of the search request.

[0095] At step 730, the search request response engine 225 determines whether to allow, deny, or modify the search request. In various embodiments, the search request response engine 225 evaluates the search request in accordance with the search request security policy 605, discussed herein. The search requests may be compared to white-lists of permitted searches and/or black-lists of unpermitted search requests. At least portions of the search request may be replaced or cleaned with other language. The search request response engine 225 may provide the determination to the digital content marketplace client interface engine 250.

[0096] At step 735, the digital content marketplace client interface engine 250 instructs the digital content marketplace client 135 to allow, deny, or modify the search request based on the determination. The digital content marketplace client interface engine 250 may call APIs on the digital content marketplace client 135 that allow, deny, or modify the search request. For example, the digital content marketplace client interface engine 250 may allow the search request by calling a function on the digital content marketplace client 135 that sends the search to the computer network 115. The digital content marketplace client interface engine 250 may deny the search request by blocking that same function. The digital content marketplace client interface engine 250 may modify the search request by replacing or cleaning the search request with other language.

[0097] FIG. 8 is a flowchart of an example method 800 of providing security to a user device for search results from a digital content marketplace. The method 800 is discussed in conjunction with the elements of the digital content marketplace security environment 100, the marketplace security system 165, and the search results security analysis engine 230, shown in FIGS. 1, 2, and 4. It is noted the steps in FIG. 8 are by way of illustration only, and that the

method 800 may include elements not explicitly depicted, and that all elements are not necessary to perform the method 800.

[0098] At step 805, the digital content marketplace filter engine 210 identifies search results from the digital content marketplace server(s) 105. The digital content marketplace filter engine 210 may identify search results that are directed to the digital content marketplace client 135. The digital content marketplace filter engine 210 may provide these search results to the search results parsing engine 405 in a binary encoded format, or other known or convenient format.

[0099] At step 810, the search results parsing engine 405 identifies digital content in the search results to be evaluated for compliance with a marketplace security policy. The search results parsing engine 405 may identify digital content names in the search results. In some embodiments, the search results parsing engine 405 identifies all known digital content names in the search results. The search results parsing engine 405 may also identify a limited set of digital content in the search results. The search results parsing engine 405 may provide the list of identified digital content to the other engines of the search results security analysis engine 230.

[0100] At step 815, the search results attribute analysis engine 410 evaluates attributes of the identified digital content for compliance with the marketplace security policy. The search results attribute analysis engine 410 may compare the attributes of the identified digital content with white-lists of permitted digital content and/or black-lists of unpermitted content in the search results security policy 610. In various embodiments, the search results attribute analysis engine 410 may evaluate the names, publishers, and/or categories associated with the identified digital content to see if the identified digital content should be allowed and/or disallowed.

[0101] At step 820, the search results access analysis engine 415 evaluates one or more levels of access of the identified digital content for compliance with the marketplace security policy. More specifically, the search results access analysis engine 415 may determine, based on the search results security policy 610, whether the identified digital content seeks an appropriate level of access to the user device 120.

[0102] At step 825, the search results budget analysis engine 420 evaluates budget factors of the identified digital content for compliance with the marketplace security policy. The search results budget analysis engine 420 may compare the identified digital content with known budget factors to see if the identified digital content comports with any digital content budget factors.

[0103] At step 825, the search results metrics analysis engine 425 evaluates metrics of the identified digital content for compliance with the marketplace security policy. More specifically, the search results metrics analysis engine 425 evaluate installation sizes, memory and/or other resources, ratings, points, stars, likes, etc. for the identified digital content. The search results metrics analysis engine 425 may provide the extracted information to the search results response engine 235 as discussed herein.

[0104] At step 830, the search results response engine 235 determines whether to allow, deny, or modify at least portions of the search response. The search results response engine 235 may evaluate the search results in accordance with the search results security policy 610, discussed herein. The search results may be compared to white-lists of permitted searches and/or black-lists of unpermitted search results. At least portions of the search results may be replaced with other language. The search results response engine 235 may provide the determination to the digital content marketplace client interface engine 250.

[0105] At step 835, the digital content marketplace client interface engine 250 instructs the digital content marketplace client 135 to allow, deny, or modify the search results based on the determination. More specifically, the digital content marketplace client interface engine 250 may call APIs on the digital content marketplace client 135 that allow, deny, or modify the search results. For example, the digital content marketplace client interface engine 250 may allow the search results by calling a function on the digital content marketplace client 135 that displays the search results on the user interface of the user device 120. The digital content marketplace client interface engine 250 may deny the search results by blocking the user interface display function. The digital content marketplace client interface engine 250 may modify the search results by replacing or cleaning the search results with other language.

[0106] FIG. 9 is a flowchart of an example method 900 of providing security to a user device for digital content from a digital content marketplace accessed by the user device. The method 900 is discussed in conjunction with the elements of the digital content marketplace

security environment 100, the marketplace security system 165, and the digital content security analysis engine 240, shown in FIGS. 1, 2, and 5. It is noted the steps in FIG. 9 are by way of illustration only, and that the method 900 may include elements not explicitly depicted, and that all elements are not necessary to perform the method 900.

[0107] At step 905, the digital content marketplace filter engine 210 identifies an attempt to access digital content from the digital content marketplace server(s) 105. For example, the digital content marketplace filter engine 210 may identify an attempt to install digital content on the user device 120. The digital content marketplace filter engine 210 may also identify an attempt to automatically or manually update or modify digital content on the user device 120.

[0108] At step 910, the attribute verification engine 505 verifies one or more attributes of the digital content using the marketplace security policies 170. The attribute verification engine 505 may use the digital content attribute verification policy 615 for this step. The attribute verification engine 505 may verify the digital content name, publisher, etc. By verifying this information, the attribute verification engine 505 prevents phishing attempts and other schemes using spoofed file names and/or content types.

[0109] At step 915, the malware analysis engine 510 performs malware analysis on the digital content using the marketplace security policies 170. The digital content may perform the malware analysis using the digital content malware analysis security policy 620. The malware analysis engine 510 may scan the digital content for viruses, spyware, adware, and other malware.

[0110] At step 920, the content analysis engine 515 performs content analysis on the digital content using the marketplace security policies 170. The content analysis engine 515 may evaluate the scripts, controls, components, etc. in the digital content using the content analysis policy 625.

[0111] At step 925, the digital content access analysis engine 525 evaluates a level of access of the digital content for compliance with the marketplace security policies 170. At step 930, the digital content budget analysis engine 530 evaluates budget factors of the digital content for compliance with the marketplace security policies 170.

[0112] At step 930, the digital content security response engine 245 determines whether to allow, deny, or modify the attempt to access the digital content. At step 935, the digital content marketplace client interface engine 250 instructs the digital content marketplace client 135 to allow, deny, or modify the attempt to access the digital content. If the access attempt is an attempt to install the digital content, the digital content marketplace client interface engine 250 may call APIs that allow or block the installation processes accordingly. The digital content marketplace client interface engine 250 may also modify the access attempt by installing similar or cleaned digital content in place of the digital content that was evaluated.

[0113] FIG. 10 depicts an example of a search request 1005 and search results 1010, according to some embodiments. As shown, the search request 1005 is in text format. The search results 1010 have been translated from binary encoded format to a text format. The search results 1010 include various attributes of the application “Angry Birds,” such as title, package, name, creator, the developer, price, the offer, type, version, code. The search results 1010 further show the rating and the number of downloads of the application.

[0114] FIG. 11 depicts an example of a digital device 1100, according to some embodiments. The digital device 1100 comprises a processor 1105, a memory system 1110, a storage system 1115, a communication network interface 1120, an Input/output (I/O) interface 1125, a display interface 1130, and a bus 1135. The bus 1135 may be communicatively coupled to the processor 1105, the memory system 1110, the storage system 1115, the communication network interface 1120, the I/O interface 1125, and the display interface 1130.

[0115] In some embodiments, the processor 1105 comprises circuitry or any processor capable of processing the executable instructions. The memory system 1110 comprises any memory configured to store data. Some examples of the memory system 1110 are storage devices, such as RAM or ROM. The memory system 1110 may comprise the RAM cache. In various embodiments, data is stored within the memory system 1110. The data within the memory system 1110 may be cleared or ultimately transferred to the storage system 1115.

[0116] The storage system 1115 comprises any storage configured to retrieve and store data. Some examples of the storage system 1115 are flash drives, hard drives, optical drives, and/or magnetic tape. In some embodiments, the digital device 1100 includes a memory system 1110 in the form of RAM and a storage system 1115 in the form of flash data. Both the memory system 1110 and the storage system 1115 comprise computer readable media which

may store instructions or programs that are executable by a computer processor including the processor 1105.

[0117] The communication network interface (com. network interface) 1120 may be coupled to a data network. The communication network interface 1120 may support communication over an Ethernet connection, a serial connection, a parallel connection, or an ATA connection, for example. The communication network interface 1120 may also support wireless communication (e.g., 802.11 a/b/g/n, WiMAX, LTE, 3G, 2G). It will be apparent to those skilled in the art that the communication network interface 1120 may support many wired and wireless standards.

[0118] The optional input/output (I/O) interface 1125 is any device that receives input from the user and output data. The display interface 1130 is any device that may be configured to output graphics and data to a display. In one example, the display interface 1130 is a graphics adapter.

[0119] It will be appreciated by those skilled in the art that the hardware elements of the digital device 1100 are not limited to those depicted in FIG. 11. A digital device 1100 may comprise more or less hardware elements than those depicted. Further, hardware elements may share functionality and still be within various embodiments described herein. In one example, encoding and/or decoding may be performed by the processor 1105 and/or a co-processor located on a GPU.

[0120] In an embodiment, the processor 1105 may correspond to the user device processor 125 of the user device 120. The processor 1105 may also correspond to the security chip processor 150 of the internal marketplace security chip 145, or the external security processor 160 of the external marketplace security chip 155. In some embodiments, the storage system 1115 may store the marketplace security policies 170 and/or other information relevant to the security of the digital content marketplace server(s) 115.

[0121] The above-described functions and components may be comprised of instructions that are stored on a storage medium such as a computer readable medium. The instructions may be retrieved and executed by a processor. Some examples of instructions are software, program code, and firmware. Some examples of storage medium are memory devices, tape, disks, integrated circuits, and servers. The instructions are operational when

executed by the processor to direct the processor to operate in accord with some embodiments. Those skilled in the art are familiar with instructions, processor(s), and storage medium.

[0122] For purposes of explanation, numerous specific details are set forth in order to provide a thorough understanding of the description. It will be apparent, however, to one skilled in the art that embodiments of the disclosure can be practiced without these specific details. In some instances, modules, structures, processes, features, and devices are shown in block diagram form in order to avoid obscuring the description. In other instances, functional block diagrams and flow diagrams are shown to represent data and logic flows. The components of block diagrams and flow diagrams (e.g., modules, blocks, structures, devices, features, etc.) may be variously combined, separated, removed, reordered, and replaced in a manner other than as expressly described and depicted herein.

[0123] Reference in this specification to “one embodiment,” “an embodiment,” “some embodiments,” “various embodiments,” “certain embodiments,” “other embodiments,” “one series of embodiments,” or the like means that a particular feature, design, structure, or characteristic described in connection with the embodiment is included in at least one embodiment of the disclosure. The appearances of, for example, the phrase “in one embodiment” or “in an embodiment” in various places in the specification are not necessarily all referring to the same embodiment, nor are separate or alternative embodiments mutually exclusive of other embodiments. Moreover, whether or not there is express reference to an “embodiment” or the like, various features are described, which may be variously combined and included in some embodiments, but also variously omitted in other embodiments. Similarly, various features are described that may be preferences or requirements for some embodiments, but not other embodiments.

[0124] The language used herein has been principally selected for readability and instructional purposes, and it may not have been selected to delineate or circumscribe the inventive subject matter. It is therefore intended that the scope be limited not by this detailed description, but rather by any claims that issue on an application based hereon. Accordingly, the disclosure of the embodiments is intended to be illustrative, but not limiting, of the scope, which is set forth in the following claims.

CLAIMS

1. A system comprising:
a digital content marketplace filter engine configured to identify a communication between a digital content marketplace client and a digital content marketplace server;
an analysis engine configured to review the communication against a digital content marketplace policy; and
a response engine configured to block, allow or modify the communication to conform to the digital content marketplace policy.
2. The system of claim 1, wherein the communication comprises a search request for one or more digital content items.
3. The system of claim 1, wherein the communication includes search results in response to a search request for digital content items.
4. The system of claim 1, wherein the digital content marketplace policy includes a whitelist or a blacklist of digital content items.
5. The system of claim 1, wherein the digital content marketplace policy includes at least one attribute associated with each digital content item.
6. The system of claim 5, wherein the at least one attribute includes title, publisher, size, hardware requirements, metadata or tags.
7. The system of claim 1, wherein the digital content marketplace policy includes at least one budget factor.
8. The system of claim 7, wherein the at least one budget factor includes a maximum price per digital content item, a maximum budget per time period, or a maximum number of downloads per time period.
9. The system of claim 1, wherein the digital content marketplace policy includes at least one metric associated with each digital content item.
10. The system of claim 9, wherein the at least one metric includes number of downloads, user rating, or popularity.

11. A method comprising:
 - identifying a communication between a digital content marketplace client and a digital content marketplace server;
 - reviewing the communication against a digital content marketplace policy; and
 - blocking, allowing or modifying the communication to conform to the digital content marketplace policy.
12. The method of claim 11, wherein the communication comprises a search request for one or more digital content items.
13. The method of claim 11, wherein the communication includes search results in response to a search request for digital content items.
14. The method of claim 11, wherein the digital content marketplace policy includes a whitelist or a blacklist of digital content items.
15. The method of claim 11, wherein the digital content marketplace policy includes at least one attribute associated with each digital content item.
16. The method of claim 15, wherein the at least one attribute includes title, publisher, size, hardware requirements, metadata or tags.
17. The method of claim 11, wherein the digital content marketplace policy includes at least one budget factor.
18. The method of claim 17, wherein the at least one budget factor includes a maximum price per digital content item, a maximum budget per time period, or a maximum number of downloads per time period.
19. The method of claim 11, wherein the digital content marketplace policy includes at least one metric associated with each digital content item.
20. The method of claim 19, wherein the at least one metric includes number of downloads, user rating, or popularity.
21. A system comprising:

means for identifying a communication between a digital content marketplace client and a digital content marketplace server;

means for reviewing the communication against a digital content marketplace policy;
and

means for blocking, allowing or modifying the communication to conform to the digital content marketplace policy.

100a

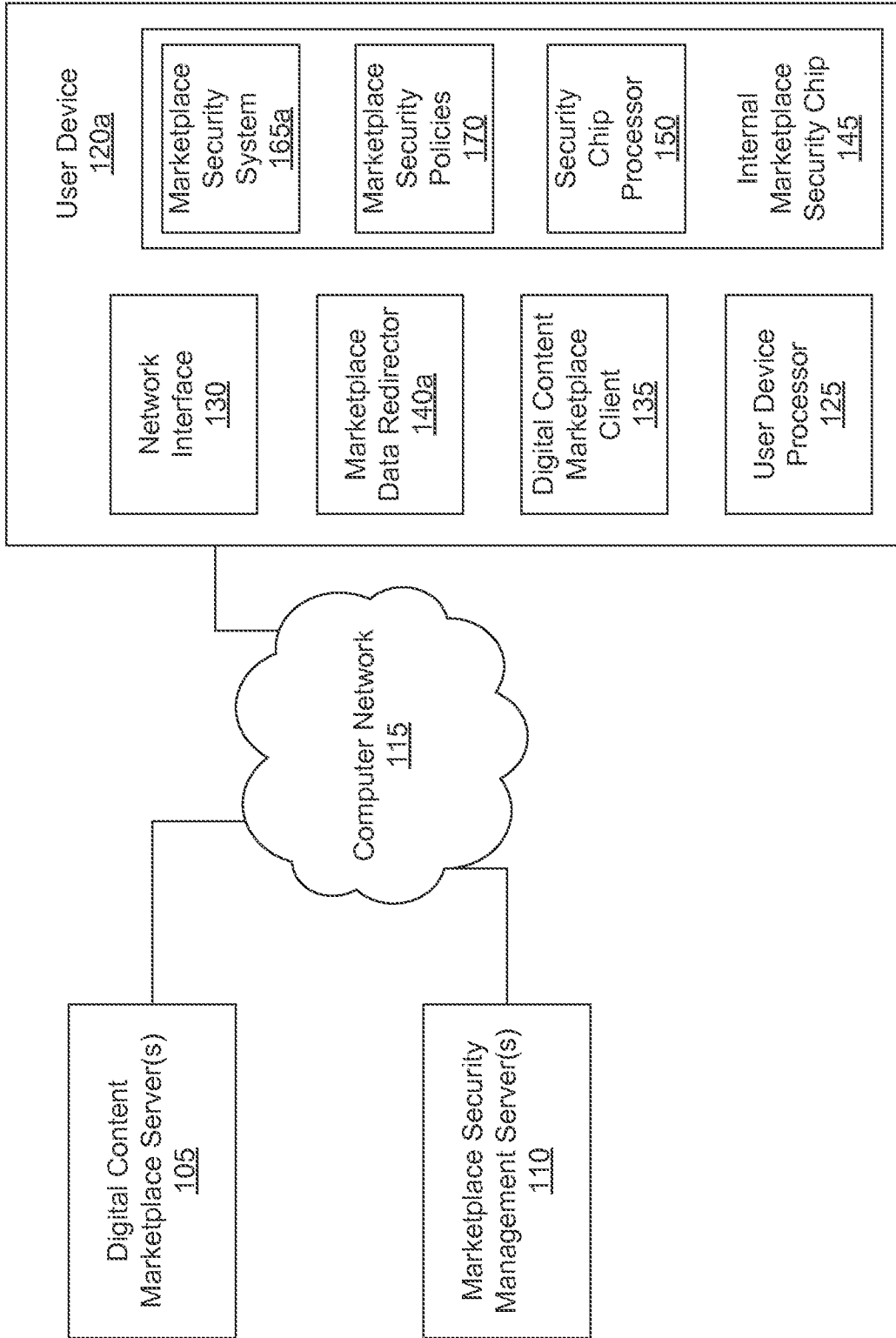


FIGURE 1A

100b

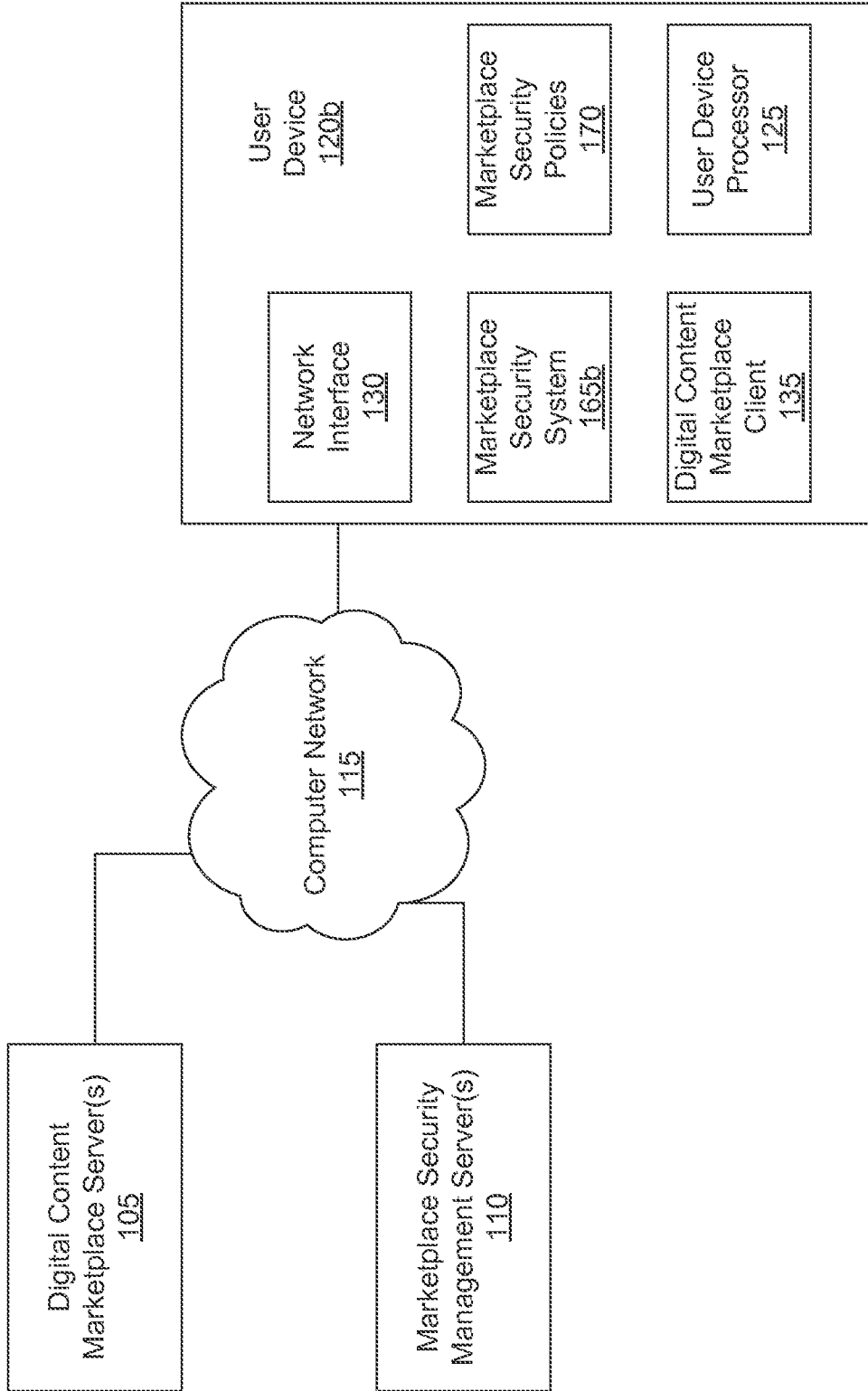


FIGURE 1B

100c

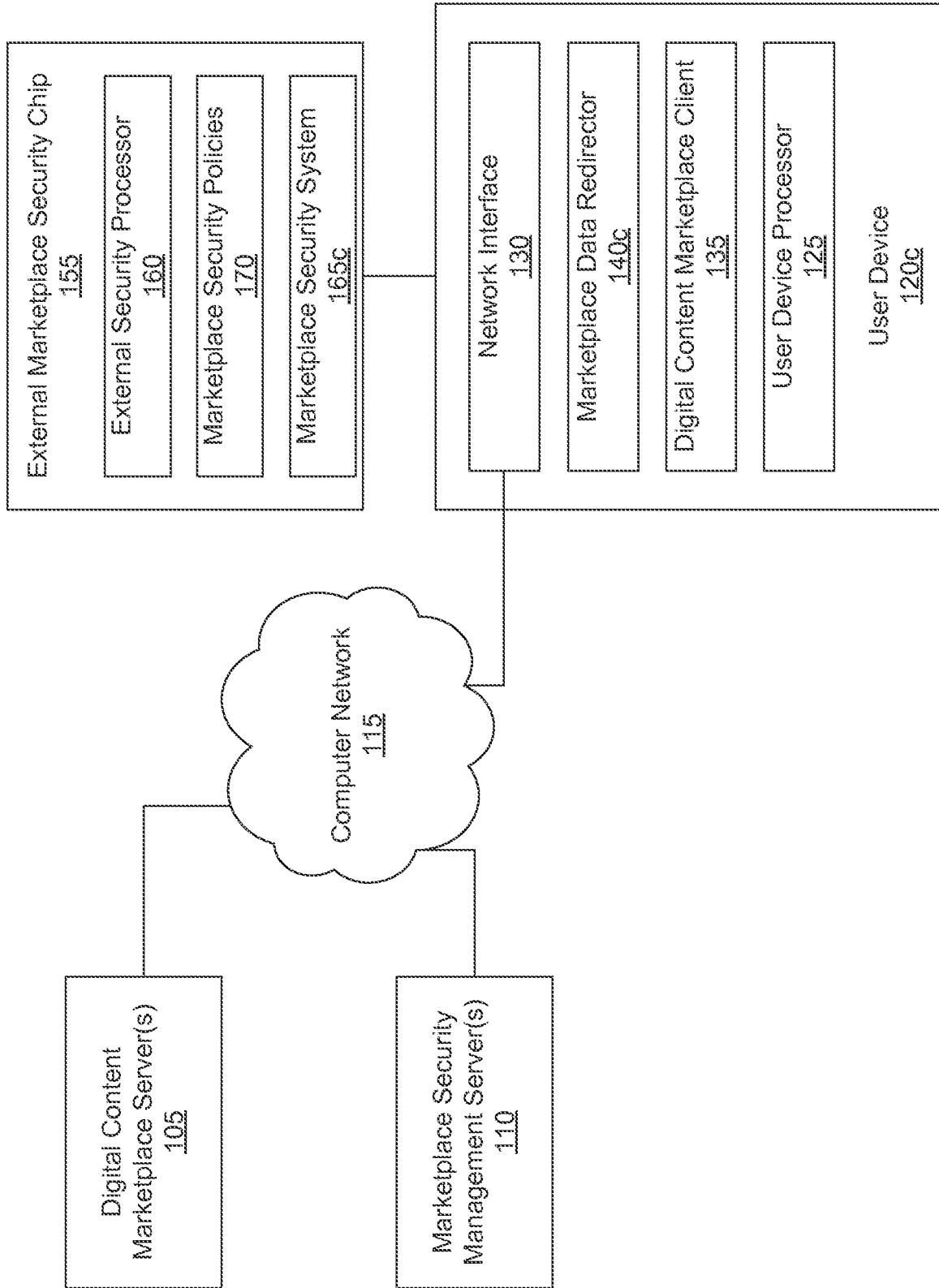


FIGURE 1C

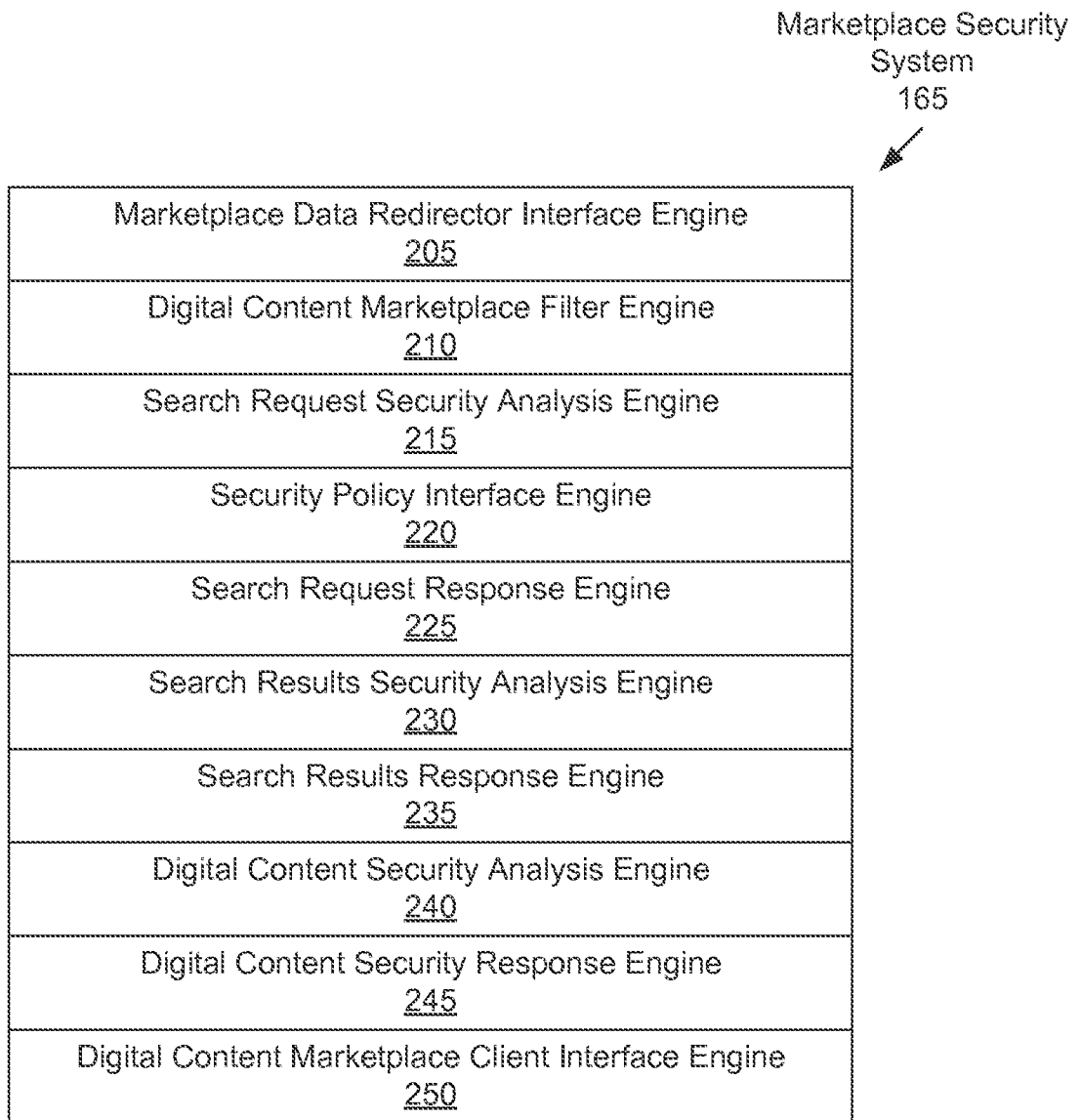



FIGURE 2

Search Request
Security Analysis
Engine
215
↙

Search Request Parsing Engine <u>305</u>
Search Request Attribute Analysis Engine <u>310</u>
Search Request Access Analysis Engine <u>315</u>
Search Request Budget Analysis Engine <u>320</u>
Search Request Metrics Analysis Engine <u>325</u>
Search Request Digital Rights Management Analysis Engine <u>330</u>

FIGURE 3

Search Results
Security Analysis
Engine
230


Search Results Parsing Engine <u>405</u>
Search Results Attribute Analysis Engine <u>410</u>
Search Results Access Analysis Engine <u>415</u>
Search Results Budget Analysis Engine <u>420</u>
Search Results Metrics Analysis Engine <u>425</u>
Search Results Digital Rights Management Analysis Engine <u>430</u>

FIGURE 4

Digital Content Security
Analysis Engine
240
↙

Attribute Verification Engine <u>505</u>
Malware Analysis Engine <u>510</u>
Content Analysis Engine <u>515</u>
Digital Rights Management Engine <u>520</u>

FIGURE 5

Marketplace Security
Policies
170
↙

Search Request Security Policy <u>605</u>
Search Results Security Policy <u>610</u>
Digital Content Attribute Verification Policy <u>615</u>
Digital Content Malware Analysis Security Policy <u>620</u>
Content Analysis Policy <u>625</u>
Digital Rights Management Policy <u>630</u>

FIGURE 6

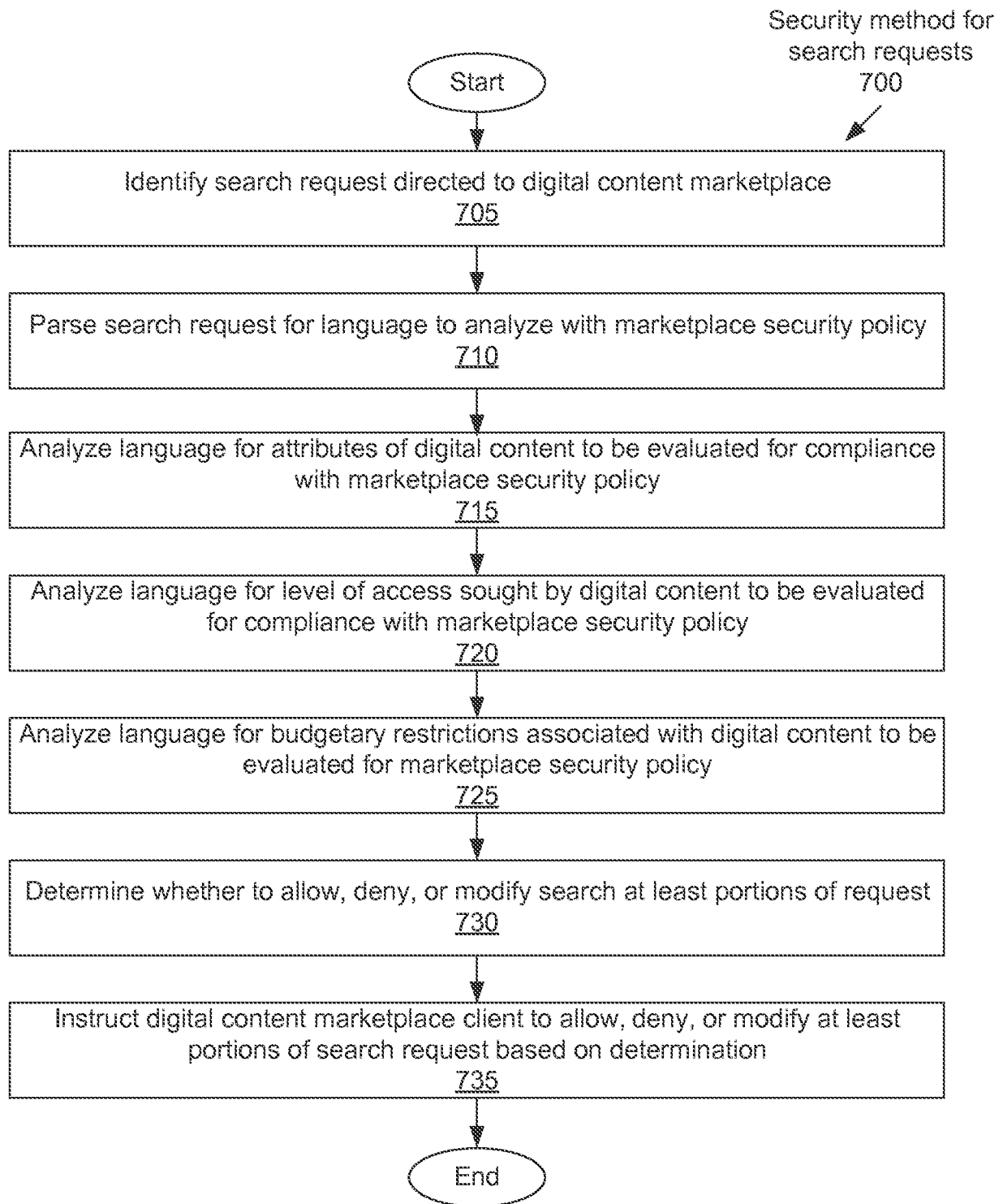


FIGURE 7

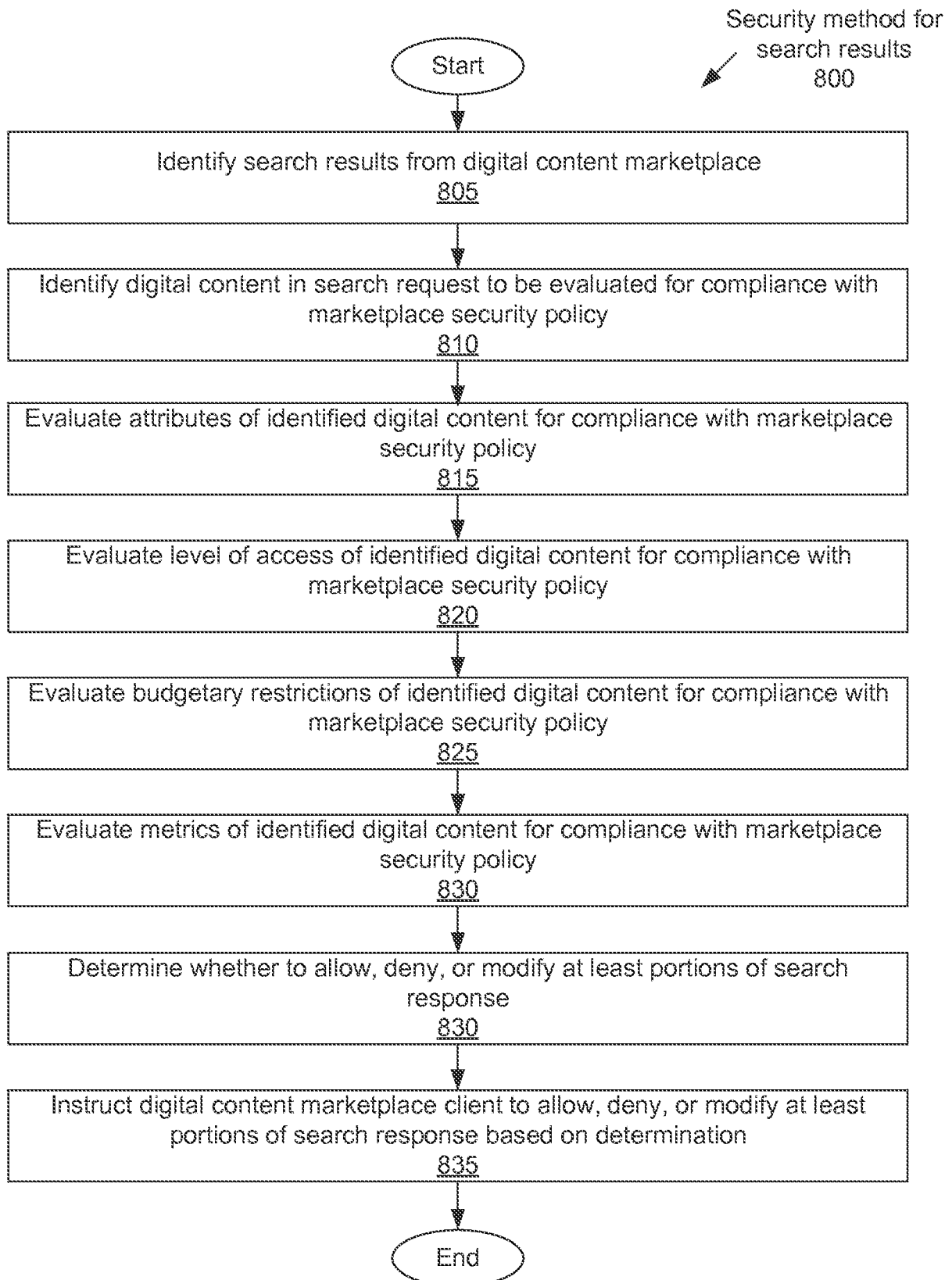


FIGURE 8

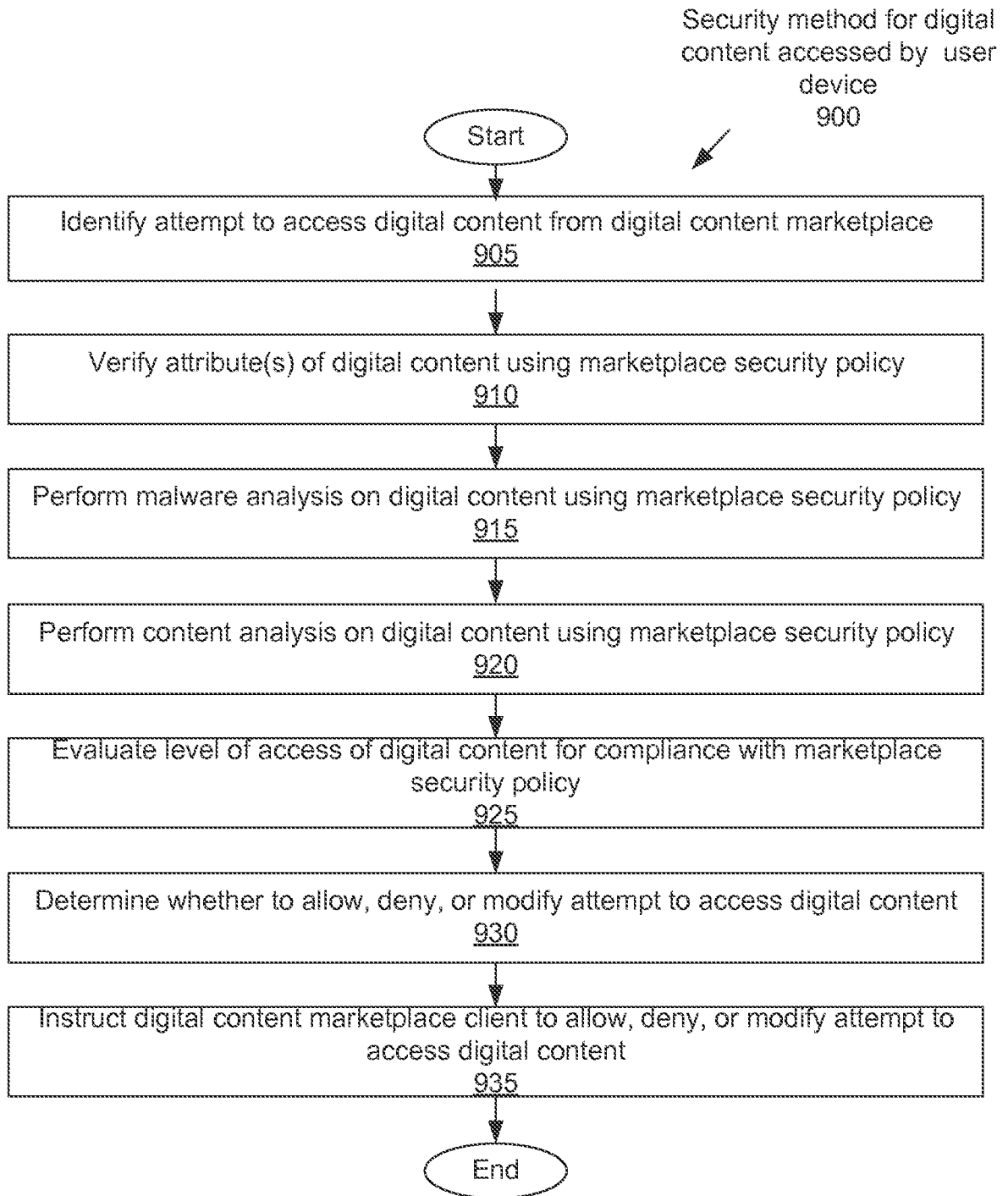


FIGURE 9

1005



GET <https://android.clients.google.com/fdfe/search?q=angry%20bird>

1010



Title	Package name	Creator	Super Dev	Price	Offer Type	Version Code	Size	Rating	Downloads
Angry Birds	com.rovio.angrybirds	Rovio	Mobile Ltd.	Free	1	200	40.4MB	4.59	100,000,000+
Angry Birds Rio	com.rovio.angrybirdsrio	Rovio	Mobile Ltd.	Free	1	1610	32.6MB	4.63	50,000,000+
Angry Birds Space	com.rovio.angrybirdspace	Rovio	Mobile Ltd.	Free	1	1520	46.1MB	4.57	50,000,000+

FIGURE 10

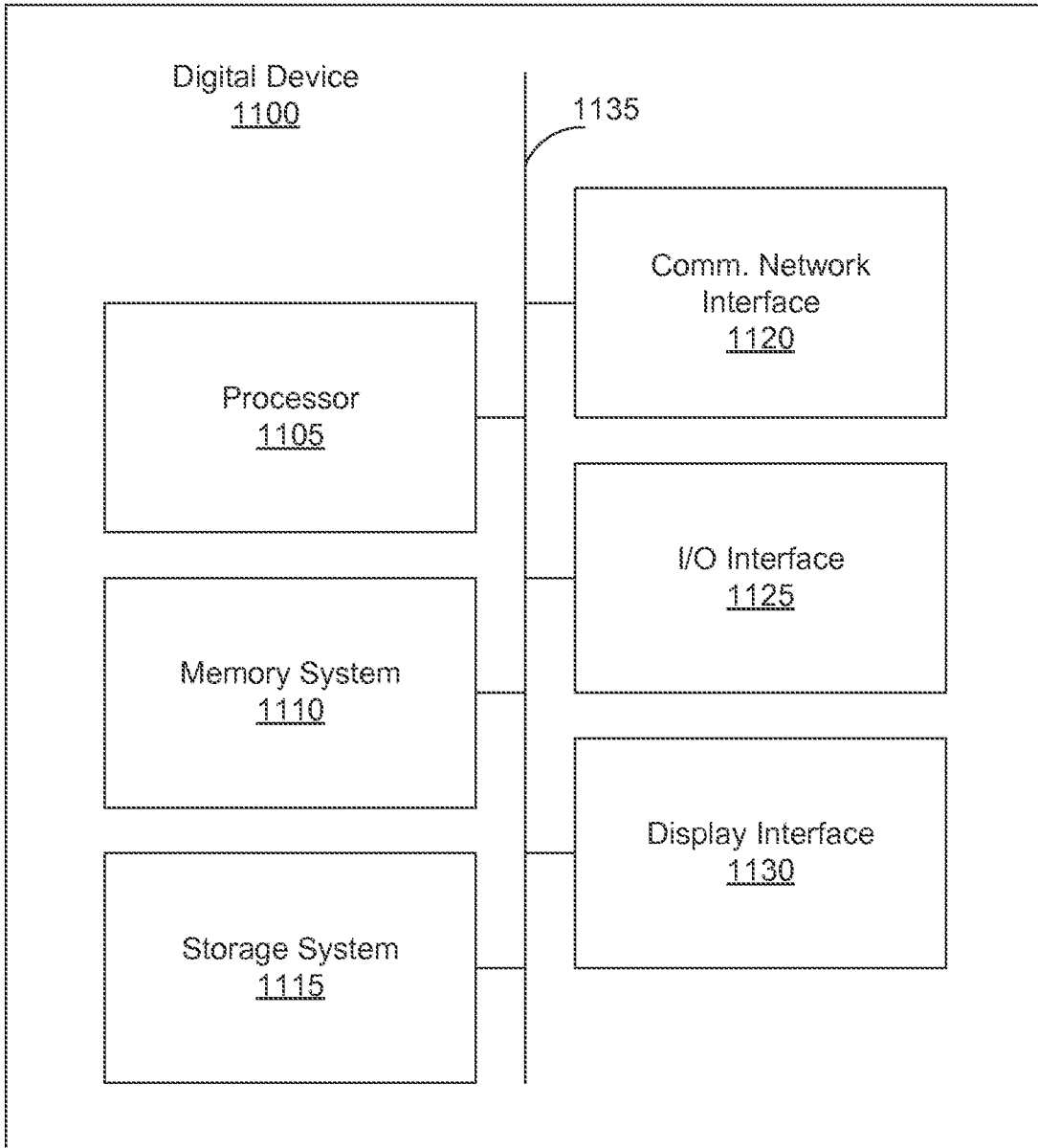


FIGURE 11

INTERNATIONAL SEARCH REPORT

International application No.

PCT/US 14/45826

<p>A. CLASSIFICATION OF SUBJECT MATTER IPC(8) - G06F 17/00 (2014.01) CPC - H04L 63/20 According to International Patent Classification (IPC) or to both national classification and IPC</p>														
<p>B. FIELDS SEARCHED</p> <p>Minimum documentation searched (classification system followed by classification symbols) USPC: 726/1; IPC(8): G06F 17/00 (2014.01); CPC: H04L 63/20</p> <p>Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched USPC: 726/1; 709/217; 726/2 (Keyword limited; terms below); IPC(8): G06F 17/00 (2014.01) (Keyword limited; terms below); CPC: H04L 63/20; H04L 63/102; G06F 21/6218 (Keyword limited; terms below)</p> <p>Electronic data base consulted during the international search (name of data base and, where practicable, search terms used) PatBase; Google (Scholar, Patents, Web) Terms used: content software store shop merchant marketplace filter client server authenticate identify policy block allow modify search request whitelist blacklist metadata title publisher size "system requirements" "hardware requirements" metric user review rating</p>														
<p>C. DOCUMENTS CONSIDERED TO BE RELEVANT</p> <table border="1"> <thead> <tr> <th>Category*</th> <th>Citation of document, with indication, where appropriate, of the relevant passages</th> <th>Relevant to claim No.</th> </tr> </thead> <tbody> <tr> <td>X --- Y</td> <td>US 2012/0240236 A1 (WYATT et al.), 20 September 2012 (20.09.2012), entire document, especially Abstract; para [0097], [0122], [0134], [0184], [0213], [0241], [0251], [0253], [0262], [0271], [0276]</td> <td>1-6, 9-16, 19-21 ----- 7-8, 17-18</td> </tr> <tr> <td>Y</td> <td>US 2012/0239739 A1 (MANGLIK et al.), 20 September 2012 (20.09.2012), entire document, especially Abstract; para [0045]-[0046]</td> <td>7-8, 17-18</td> </tr> <tr> <td>A</td> <td>US 2012/0233695 A1 (MAHAFFEY et al.), 13 September 2012 (13.09.2012), entire document</td> <td>1-21</td> </tr> </tbody> </table>			Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.	X --- Y	US 2012/0240236 A1 (WYATT et al.), 20 September 2012 (20.09.2012), entire document, especially Abstract; para [0097], [0122], [0134], [0184], [0213], [0241], [0251], [0253], [0262], [0271], [0276]	1-6, 9-16, 19-21 ----- 7-8, 17-18	Y	US 2012/0239739 A1 (MANGLIK et al.), 20 September 2012 (20.09.2012), entire document, especially Abstract; para [0045]-[0046]	7-8, 17-18	A	US 2012/0233695 A1 (MAHAFFEY et al.), 13 September 2012 (13.09.2012), entire document	1-21
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.												
X --- Y	US 2012/0240236 A1 (WYATT et al.), 20 September 2012 (20.09.2012), entire document, especially Abstract; para [0097], [0122], [0134], [0184], [0213], [0241], [0251], [0253], [0262], [0271], [0276]	1-6, 9-16, 19-21 ----- 7-8, 17-18												
Y	US 2012/0239739 A1 (MANGLIK et al.), 20 September 2012 (20.09.2012), entire document, especially Abstract; para [0045]-[0046]	7-8, 17-18												
A	US 2012/0233695 A1 (MAHAFFEY et al.), 13 September 2012 (13.09.2012), entire document	1-21												
<p><input type="checkbox"/> Further documents are listed in the continuation of Box C. <input type="checkbox"/></p>														
<p>* Special categories of cited documents:</p> <table border="0"> <tr> <td style="vertical-align: top;"> <p>"A" document defining the general state of the art which is not considered to be of particular relevance</p> <p>"E" earlier application or patent but published on or after the international filing date</p> <p>"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)</p> <p>"O" document referring to an oral disclosure, use, exhibition or other means</p> <p>"P" document published prior to the international filing date but later than the priority date claimed</p> </td> <td style="vertical-align: top;"> <p>"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention</p> <p>"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone</p> <p>"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art</p> <p>"&" document member of the same patent family</p> </td> </tr> </table>			<p>"A" document defining the general state of the art which is not considered to be of particular relevance</p> <p>"E" earlier application or patent but published on or after the international filing date</p> <p>"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)</p> <p>"O" document referring to an oral disclosure, use, exhibition or other means</p> <p>"P" document published prior to the international filing date but later than the priority date claimed</p>	<p>"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention</p> <p>"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone</p> <p>"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art</p> <p>"&" document member of the same patent family</p>										
<p>"A" document defining the general state of the art which is not considered to be of particular relevance</p> <p>"E" earlier application or patent but published on or after the international filing date</p> <p>"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)</p> <p>"O" document referring to an oral disclosure, use, exhibition or other means</p> <p>"P" document published prior to the international filing date but later than the priority date claimed</p>	<p>"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention</p> <p>"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone</p> <p>"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art</p> <p>"&" document member of the same patent family</p>													
<p>Date of the actual completion of the international search</p> <p>02 October 2014 (02.10.2014)</p>		<p>Date of mailing of the international search report</p> <p>30 OCT 2014</p>												
<p>Name and mailing address of the ISA/US</p> <p>Mail Stop PCT, Attn: ISA/US, Commissioner for Patents P.O. Box 1450, Alexandria, Virginia 22313-1450 Facsimile No. 571-273-3201</p>		<p>Authorized officer:</p> <p>Lee W. Young</p> <p>PCT Helpdesk: 571-272-4300 PCT OSP: 571-272-7774</p>												