

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

NETSKOPE, INC.,
Petitioner,

v.

FORTINET, INC.,
Patent Owner.

IPR2023-00458
Patent 9,280,678 B2

Before JAMES P. CALVE, THOMAS L. GIANNETTI, and
STEPHEN E. BELISLE, *Administrative Patent Judges*.

CALVE, *Administrative Patent Judge*.

DECISION
Granting Institution of *Inter Partes* Review
35 U.S.C. § 314

I. BACKGROUND

Netskope, Inc. (“Petitioner”) filed a petition requesting an *inter partes* review of claims 1–3, 6, 8–17, and 21–27 (the “challenged claims”)¹ of U.S. Patent No. 9,280,678 B2 (“the ’678 patent”) (Ex. 1001). Paper 2, 5 (“Pet.”). Fortinet, Inc. (“Patent Owner”) filed a Preliminary Response. Paper 6 (“Prelim. Resp.”).

We have authority to determine whether to institute an *inter partes* review. *See* 35 U.S.C. § 314 (2018); 37 C.F.R. § 42.4(a) (2022) (“The Board institutes the trial on behalf of the Director.”). An *inter partes* review may not be instituted “unless . . . the information presented in the petition . . . shows that there is a reasonable likelihood that the petitioner would prevail with respect to at least 1 of the claims challenged in the petition.” 35 U.S.C. § 314(a). Upon consideration of the evidence and arguments in the record, we determine that the information presented shows a reasonable likelihood that Petitioner would prevail with respect to at least one of the challenged claims. We therefore grant institution of an *inter partes* review.

A. *Related Proceedings*

The parties identify the following proceeding involving the ’678 patent: *Netskope, Inc. v. Fortinet, Inc.*, No. 3:22-cv-01852-TLT (N.D. Cal.). Pet. 5; Paper 3, 2. Petitioner identifies the following *inter partes* reviews in which Petitioner challenges other patents of Patent Owner: IPR2022-01587, IPR2023-00030, IPR2023-00175, IPR2023-00456, IPR2023-00457, and IPR2023-00459. Pet. 5.

¹ Petitioner asserts the challenged claims are claims 1–3, 6, 8–19, and 21–27 (Pet. 7) but makes no substantive arguments against claims 18 and 19 and seeks to cancel claims 1–3, 6, 8–17, and 21–27 in the Introduction (*id.* at 5).

B. Real Parties in Interest

Petitioner identifies Netskope, Inc. as the real party in interest. Pet. 5. Patent Owner identifies Fortinet, Inc. as the real party in interest. Paper 3, 2.

C. The '678 Patent (Ex. 1001)

The '678 patent provides vendor independent secure cloud storage distribution and aggregation systems by interposing a cloud storage gateway device between third-party cloud storage platforms and enterprise users who access those platforms. Ex. 1001, 2:9–16. The gateway includes application programming interfaces (APIs) that facilitate storage of files, issue search requests for files, and retrieve content of files on the cloud storage platforms. *Id.* at 2:11–17. The cloud storage gateway device also assigns a file storage policy to each user. *Id.* at 2:17–18. “The assigned file storage policy defines access rights, storage diversity requirements and a type of encryption to be applied to files for the corresponding user.” *Id.* at 2:19–22.

The gateway system “implement[s] a policy based framework for encrypting, storing, accessing, querying and managing data across one or more cloud platforms.” Ex. 1001, 3:25–28. In one embodiment,

a searchable encryption gateway framework provides assignment of a policy from a group of policies stored in a policy database to one or more users such that the policy not only defines the manner in which the users can access and process content stored on the cloud, but can also configure the mode in which the data is encrypted, stored, searched, and accessed to ensure secure and vendor independent cloud management.

Id. at 3:28–35. “Cloud storage service providers” are companies that provide computer storage space and management to other companies and include Dropbox, Google Drive, and Amazon Web Services. *Id.* at 6:9–14.

Figure 1 of the '678 patent is reproduced below to illustrate an exemplary network architecture of such a system. Ex. 1001, 6:51–52.

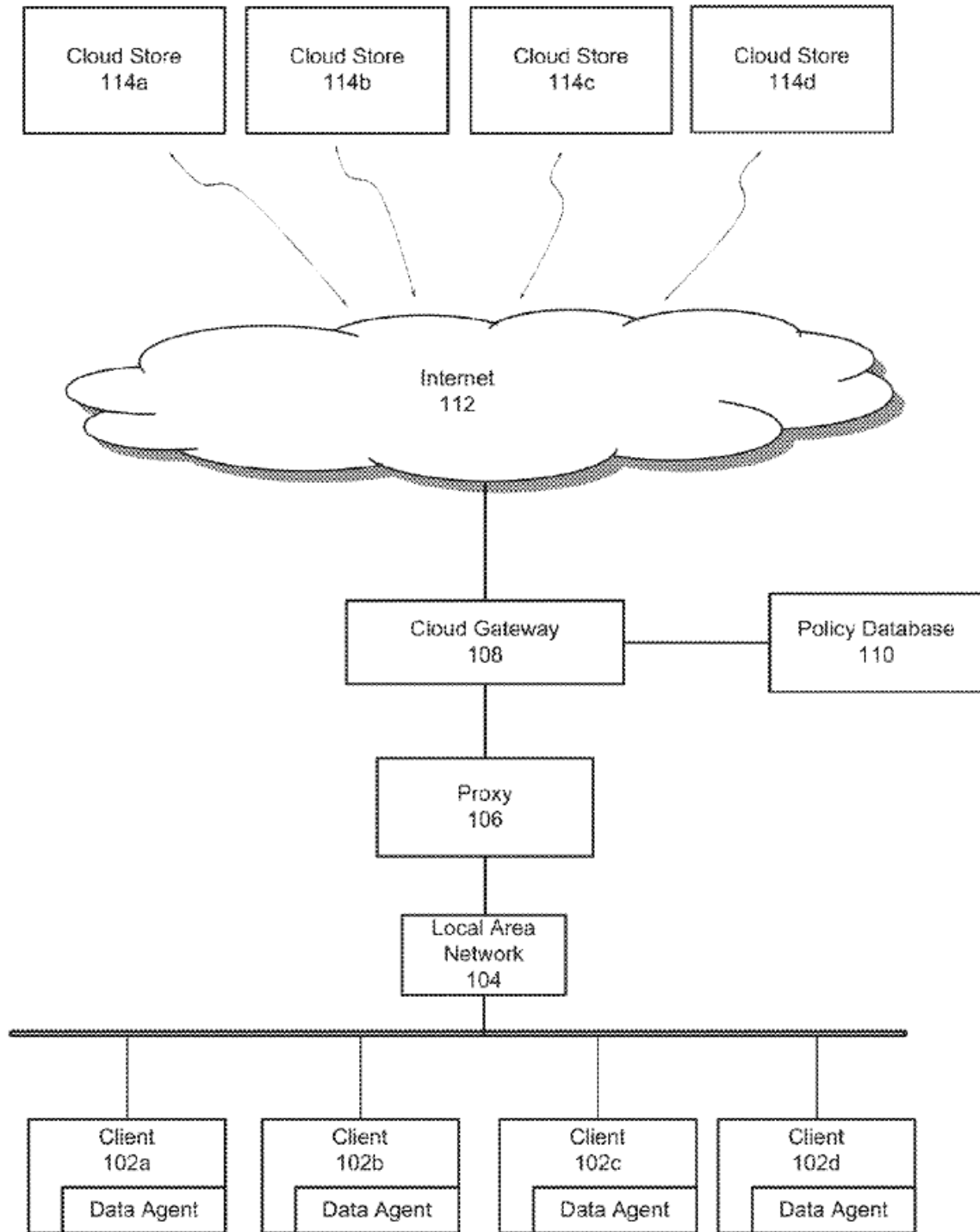


Fig. 1

Figure 1 of the '678 patent depicts clients 102a–d operatively and communicatively coupled to one other via local area network (LAN) 104. Ex. 1001, 6:51–56. Clients 102 also couple to cloud stores 114a–d through gateway device 108 and Internet 112. *Id.* at 7:5–9. Gateway device 108 acts as an interface between clients 102 and cloud stores 114 to handle client file/data read/write requests and to identify the appropriate cloud stores 114 to access to process the requests. *Id.* at 7:9–14. Figure 2 of the '678 patent is reproduced below to illustrate functional modules of the gateway device.

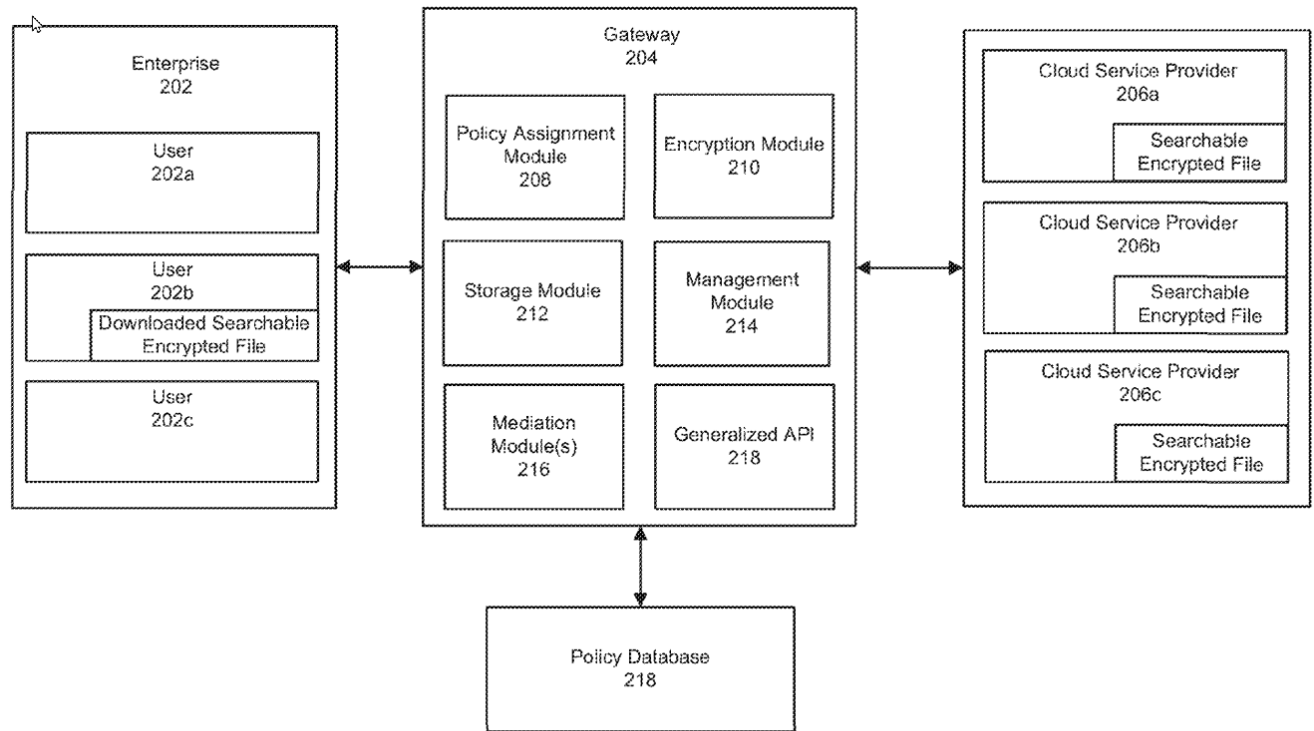


Fig. 2

Figure 2 depicts a policy-based framework using gateway 204 and its functional modules to interface transactions and execute instructions for the read/write/search of content between enterprise users 202 and cloud service providers 206 based on users' roles and responsibilities that require different access rights and privileges to access data and content. Ex. 1001, 8:27–65.

Policy assignment module 208 assigns policies from policy database 218 to a user or group of users 202 based on their roles, responsibilities, and enterprise practices. It defines the way that data, metadata, and other content is accessed and processed by each user or group of users 202a–c. Ex. 1001, 9:11–19. Each policy “defines the manner in which files can be uploaded, stored, downloaded, searched, and/or processed in the context of one or more cloud platforms,” and also includes “any other configurable aspect of the mode in which the user 202 accesses data stored or to be stored in the namespaces, directories, folders, files or other storage containers of one or more cloud platforms.” *Id.* at 9:19–26. A “[p]olicy assigned to a user 202 can *also be configured* to manage access rights relating to encryption and decryption of content.” *Id.* at 9:34–36 (emphasis added).

Encryption module 210 encrypts files to upload or store on a cloud platform(s) “based on the policies assigned by the policy assignment module 208.” Ex. 1001, 9:53–56. “[G]ateway 204 can share encryption/decryption keys based on the policy assigned to the user,” but it does not share details of private or public keys with any user 202 who is not authorized by a policy to encrypt files to store in cloud containers. *Id.* at 9:61–67. Encryption module 210 can encrypt each file or file part using cryptographic key data so the encrypted content is searchable across and within cloud platforms so that encryption architecture is independent of a provider of the cloud platform. *Id.* at 10:1–6. Encryption module 210 also allows users 202, based on their assigned policy, to download searchable encrypted files onto a local device for offline applications. *Id.* at 10:6–10. Searchable encrypted files may encrypt the name of a file as part of the folder name, or hashes of search terms may be used as file names in searchable indices. *Id.* at 10:29–38.

D. Challenged Claims

Claims 1 and 16 are independent. Claims 2, 3, 6 and 8–15 depend from claim 1. Claims 17 and 21–27 depend from claim 16. Ex. 1001, 19:57–22:22.

Claim 1 is reproduced below with Petitioner’s annotations added to identify each limitation (*see* Pet. 23–49 (providing Petitioner’s contentions for the unpatentability of claim 1 under Ground 1)).

1[pre] A method comprising:

1[a][i] assigning to one or more users, by a gateway device, a policy for managing access to and processing a file to be stored on one or more cloud platforms, *1[a][ii]* wherein the policy defines access rights of the one or more users;

1[b] encrypting, by the gateway device, using cryptographic key information defined by the policy, content of the file to produce a searchable encrypted file by:

1[b][i] dividing the file into a plurality of chunks;

1[b][ii] creating namespaces for one or more of the plurality of chunks; and

1[b][iii] configuring the namespaces of the one or more chunks such that content of the file is encrypted in a manner that makes it searchable;

1[c] storing, by the gateway device, the searchable encrypted file on the one or more cloud platforms based on the policy; and

1[d] managing access to the searchable encrypted file by the one or more users based on the policy.

Ex. 1001, 19:57–20:8.

E. Asserted Grounds of Unpatentability

Petitioner asserts unpatentability on the following grounds (Pet. 7):

Ground	Challenged Claim(s) ²	35 U.S.C. §	Reference(s)
1	1–3, 8–14, 16, 17, 21–27	103 ³	Cidon ⁴ , Shikfa ⁵ , Herrmann ⁶
2	6	103	Cidon, Shikfa, Herrmann, Fellenstein ⁷
3	15	103	Cidon, Shikfa, Herrmann, Hirai ⁸
4	1–3, 8–17, 21–27	103	Auradkar ⁹ , Chiueh ¹⁰ , Chambers ¹¹
5	6	103	Auradkar, Chiueh, Chambers, Inoue ¹²

Petitioner also relies on a Declaration of Dr. Wenke Lee. Ex. 1002.

Patent Owner relies on a Declaration of Dr. John Black Jr. Ex. 2001.

² Petitioner lists claims 18 and 19 in Grounds 1 and 4, but no substantive arguments are provided for either claim. *See* Pet. 7, 15–69, 72–135.

³ The Leahy-Smith America Invents Act (“AIA”) revised 35 U.S.C. § 103 effective on March 16, 2013. Because the ’678 patent has an effective filing date after March 16, 2013, we use the AIA version of 35 U.S.C. § 103.

⁴ US 2014/0013112 A1, published Jan. 9, 2014 (Ex. 1004, “Cidon”).

⁵ US 2014/0359282 A1, published Dec. 4, 2014 (Ex. 1006, “Shikfa”).

⁶ US 2003/0055994 A1, published Mar. 20, 2003 (Ex. 1005, “Herrmann”).

⁷ US 2005/0010593 A1, published Jan. 13, 2005 (Ex. 1007, “Fellenstein”).

⁸ US 6,622,248 B1, issued Sept. 16, 2003 (Ex. 1008, “Hirai”).

⁹ US 2011/0119481 A1, published May 19, 2011 (Ex. 1009, “Auradkar”).

¹⁰ US 2013/0159694 A1, published June 20, 2013 (Ex. 1011, “Chiueh”).

¹¹ US 2014/0068030 A1, published Mar. 6, 2014 (Ex. 1010, “Chambers”).

¹² US 2003/0063321 A1, published Apr. 3, 2003 (Ex. 1012, “Inoue”).

II. DISCUSSION

A. *Level of Ordinary Skill in the Art*

The parties substantially agree on the level of ordinary skill in the art. Petitioner asserts that a skilled artisan “would have had a B.S. in computer science, computer engineering, or electrical engineering, with at least two years’ experience in computer networking/security.” Pet. 15. Patent Owner asserts that a skilled artisan “would have had a Bachelor of Science degree in electrical engineering and/or computer science, and two years of work or research experience in the fields of network and data security, or a Master’s degree in electrical engineering and/or computer science and one year of work or research experience in related fields.” Prelim. Resp. 15–16. Patent Owner asserts that the positions set forth in the Preliminary Response would be the same under either parties’ proposal. *Id.* at 16. We adopt Petitioner’s proposal as more consistent with the prior art and the ’678 patent. Our decision would be the same under either formulation.

B. *Claim Interpretation*

We interpret claims “using the same claim construction standard that would be used to construe the claims in a civil action [held] under 35 U.S.C. 282(b).” 37 C.F.R. § 42.100(b). Under this standard, we construe claims “in accordance with the ordinary and customary meaning of such claim as understood by one of ordinary skill in the art and the prosecution history pertaining to the patent.” *Id.* We construe the claims only to the extent necessary to determine whether to institute *inter partes* review. *See Nidec Motor Corp. v. Zhongshan Broad Ocean Motor Co.*, 868 F.3d 1013, 1017 (Fed. Cir. 2017) (“[W]e need only construe terms ‘that are in controversy, and only to the extent necessary to resolve the controversy.’”).

The parties assert that the claims should be given their ordinary and customary meaning in light of the specification and no claim constructions are necessary at this time. Pet. 15; Prelim. Resp. 16.

We agree that no express claim constructions are required at this time to render our decision.

C. Principles of Law

A patent claim is unpatentable under 35 U.S.C. § 103 if differences between the claimed subject matter and the prior art are such that the subject matter, as a whole, would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. 35 U.S.C. § 103; *KSR Int’l Co. v. Teleflex Inc.*, 550 U.S. 398, 406 (2007). “The combination of familiar elements according to known methods is likely to be obvious when it does no more than yield predictable results.” *KSR*, 550 U.S. at 416. Similarly, “if a technique has been used to improve one device, and a person of ordinary skill in the art would recognize that it would improve similar devices in the same way, using the technique is obvious unless its actual application is beyond his or her skill.” *Id.* at 417.

The question of obviousness is resolved based on underlying factual determinations including: (1) the scope and content of the prior art; (2) any differences between the claimed subject matter and the prior art; (3) the level of ordinary skill in the art; and (4) when in evidence, objective evidence of non-obviousness. *Graham v. John Deere Co.*, 383 U.S. 1, 17–18 (1966). Neither party presents any objective evidence of non-obviousness at this stage of the proceeding.

D. Ground 1: Alleged Obviousness Over Cidon, Shikfa, Herrmann

Petitioner asserts unpatentability of claims 1–3, 8–14, 16, 17, and 21–27 under 35 U.S.C. § 103 over Cidon, Shikfa, and Herrmann. Pet. 7, 15–69.¹³

1. Cidon (Ex. 1004)

Cidon discloses management server 100 that stores encrypted files in segments using policies for file placement, access, and sharing as shown in Figure 2, reproduced below. Ex. 1004 ¶¶ 10, 102, 108, 206–212, 221–223.

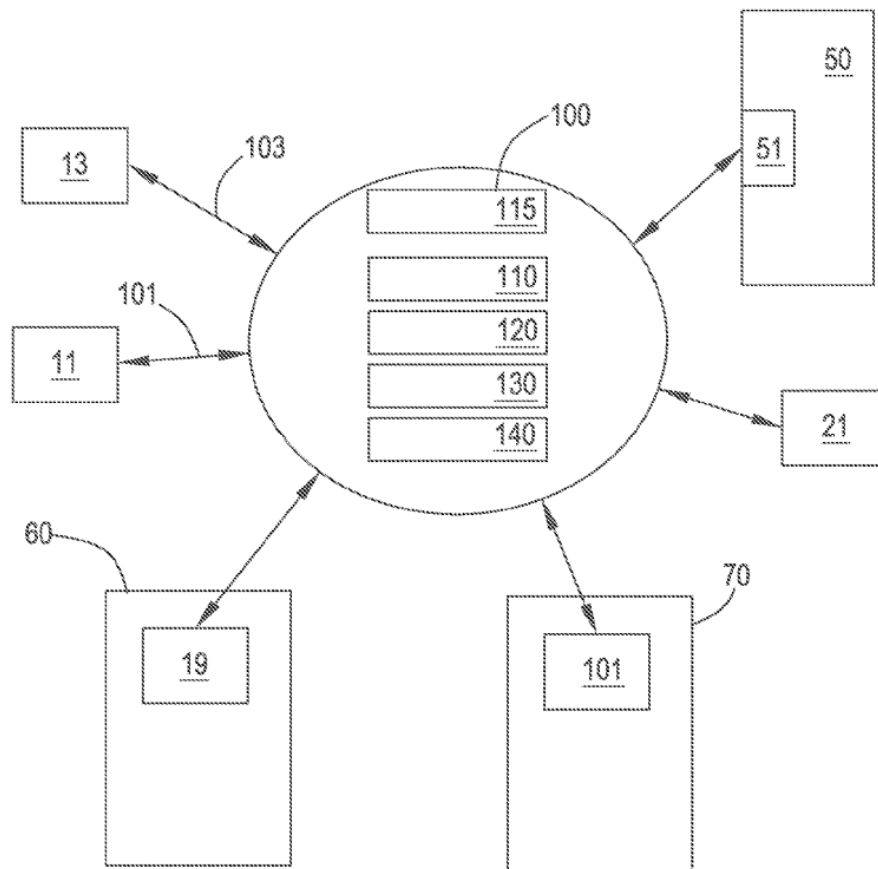


FIG. 2

¹³ Petitioner lists claims 1–3, 8–14, and 16–27 as the challenged claims in Ground 1 (Pet. 15) but provides no substantive argument for claims 18–20 (*id.* at 15–69). *Cf., id.* at 5 (seeking to cancel claims 1–3, 6, 8–14, 16–19, and 21–27), 7 (listing claims 1–3, 8–14, 16–19, and 21–27 for Ground 1).

Figure 2 depicts management server 100 that encrypts cloud files and controls access to the files by providing decryption keys. Ex. 1004 ¶ 102. System metadata module 115 manages file metadata. *Id.* ¶¶ 105, 106. IP Policy Enforcement Module 120 allows administrators to organize users into groups and assign different access policies to each group. *Id.* ¶ 108. Data Manager and Login Module 130 processes requests to access a secure file. *Id.* ¶ 109. Encryption Key Manager 140 generates, stores, and retrieves encryption keys. *Id.* ¶ 110. Policies specify placement of files in specific directories, access and sharing permissions, copy control, and encryption. Ex. 1004 ¶¶ 206–212. Files may be segmented, and each segment may be encrypted and stored. *Id.* ¶¶ 305, 309, 383, Fig. 13.

2. Shikfa (Ex. 1006)

Shikfa's broker system encrypts and searches encrypted documents using encryption keys and indexes as shown in Figure 2, reproduced below.

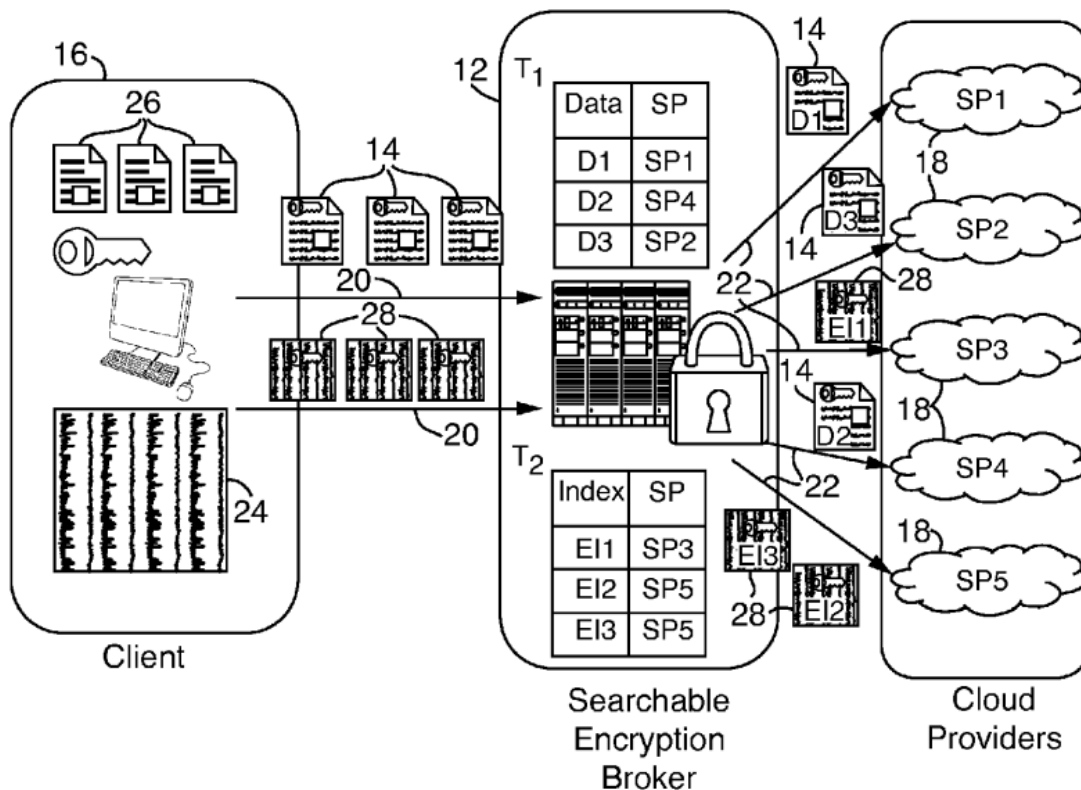


Figure 2 of Shikfa depicts a broker system for searchable encryption. Client 16 encrypts documents 26, generates indexes 24 for documents 26, encrypts indexes 24, and stores encrypted documents and indexes in cloud storage providers 18. Ex. 1006 ¶¶ 3, 10, 12, 29. Broker server 12 receives encrypted documents 14, encrypted indexes 28, and encryption information and generates a translation table T1 to identify which encrypted document 14 is stored on which cloud storage provider 18. *Id.* ¶¶ 31, 32. Index 28 includes keywords for encrypted documents 14 and pointers to documents containing the keywords. *Id.* ¶ 29. Broker server 12 may store encrypted indexes 28 locally or send them to cloud storage providers 18. *Id.* ¶ 32.

To search for encrypted document 14 that contains certain keywords, client 16 generates encrypted search query 30 for the keywords using the searchable encryption mechanism that encrypted indexes 28 and sends the encrypted query 30 to broker server 12. Ex. 1006 ¶ 34. Broker server 12 uses the searchable encryption mechanism that was used to encrypt query 30 and to encrypt indexes 28 as input to identify (via identifiers D1, D2, D3) encrypted documents 14 that satisfy the encrypted search query. *Id.* ¶¶ 34–36. Broker server 12 thereby allows clients 16 to store secure, encrypted documents 14 on cloud storage providers 18 and also provides searchable encryption so clients 16 can search and retrieve encrypted documents by using translation tables T1, T2 or encrypted indexes 28. *Id.* ¶ 37.

3. *Herrmann (Ex. 1005)*

Herrmann discloses a gateway server 350 that controls access of client machines to protected data resources 390 by verifying access is authorized as illustrated in Figure 3, which is reproduced below. Ex. 1005 ¶ 60.

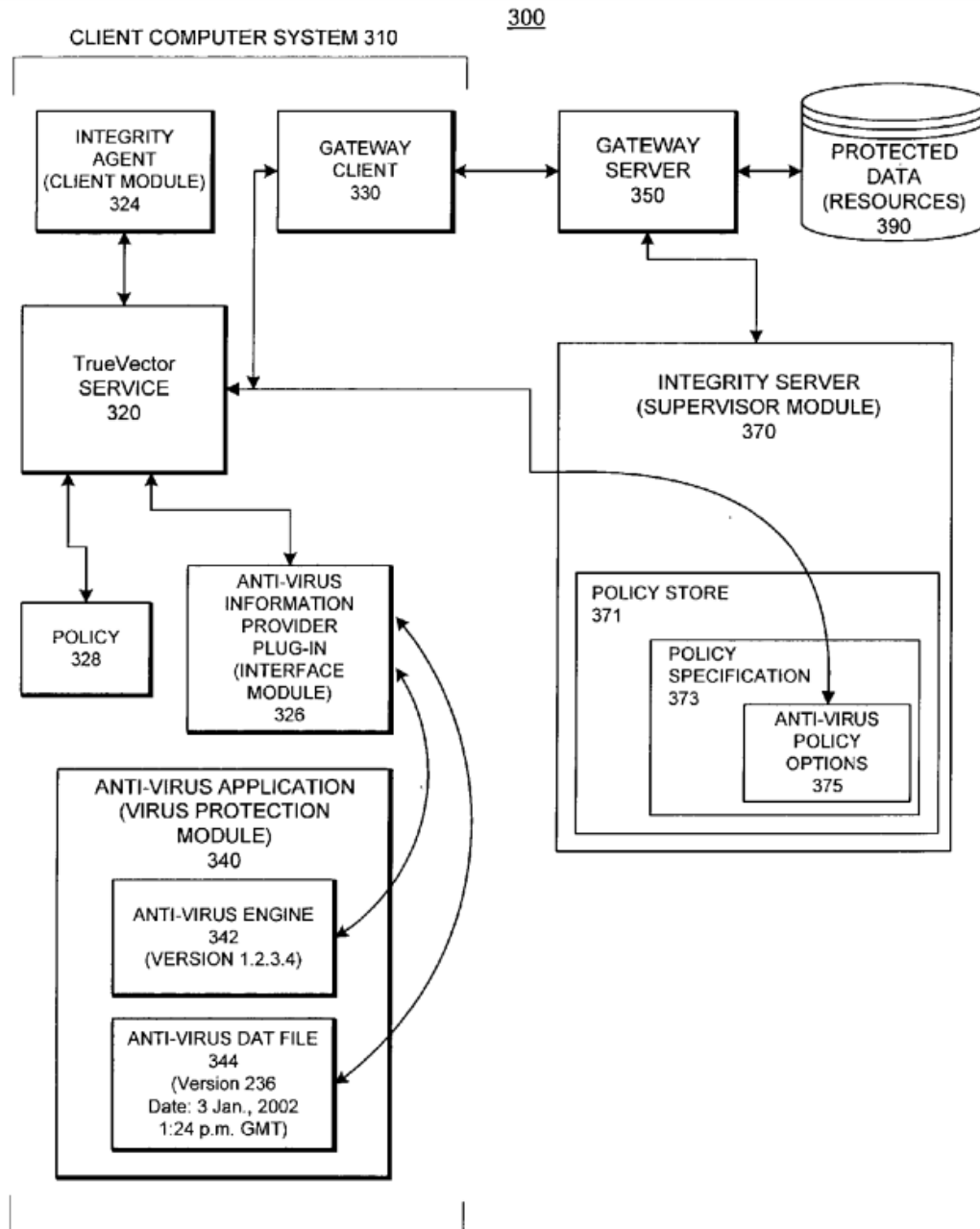


FIG. 3

Figure 3 depicts gateway client 330 of client computer 310 connected to gateway server 350 to access protected data 390. Gateway server 350 grants access when integrity server 370 indicates access is permissible under a policy specification applicable to client computer 310. Ex. 1005 ¶¶ 60, 67.

4. *Independent Claim 1*

a. *1[pre]: “A method comprising:”*

Petitioner asserts that Cidon discloses a method of “encrypting a file” by segmenting the file into multiple file segments, encrypting each file segment to yield multiple encrypted file segments, and sending the multiple encrypted file segments to a storage service. Pet. 23 (citing Ex. 1004 ¶¶ 10, 309, Fig. 15). Petitioner cites Figure 15 of Cidon, which is a flowchart for retrieving a file from storage service 1610, segmenting the file, calculating signatures for each segment, encrypting each file segment, and sending encrypted file segments to storage service 1650. *Id.* This contention, which Patent Owner does not contest at this stage, is supported by record evidence.

b. *1[a][i]: “assigning to one or more users, by a gateway device, a policy for managing access to and processing a file to be stored on one or more cloud platforms”*

Petitioner contends that Cidon discloses a management server that provides access policy configurations for users, implements access policies, and processes files to be stored on cloud platforms. Petitioner contends that Cidon’s management server configures a user access policy and enforces the access policy for secure file access, and the policy dictates whether certain files are encrypted. Petitioner contends that Cidon’s management server allows an administrator to organize users into groups and define different secure file access policies for each group. Pet. 24–25 (citing Ex. 1004 ¶¶ 99, 100, 102, 108, 224, 227; Ex. 1002 ¶¶ 74–79). These contentions, which Patent Owner does not contest at this stage, are supported by record evidence. IT Policy Enforcement Module 120 allows administrators to define access policies for different users and groups. Ex. 1004 ¶ 108.

Petitioner asserts that Herrmann discloses a gateway server 350 that acts as a gateway to protect data or resources 390 and accept access requests to the resources from client machines. Pet. 25 (citing Ex. 1005 ¶ 60, Fig. 3). Petitioner contends that Herrmann’s gateway server 350 verifies that a client computer 310 is authorized to access protected data 390, assigns an access policy to the connection/session between the gateway server 350 and client computer 310 from policy store 371, and maintains an “appropriate policy specification 373 applicable to the client computer 310.” Pet. 26–27 (citing Ex. 1005 ¶¶ 60, 67, 77, claim 16; Ex. 1002 ¶ 79). Policies can be retrieved by a user, group, or computer. *Id.* These contentions, which Patent Owner does not contest at this stage, are supported by record evidence. Gateway server 350 prevents session access until integrity server 370 indicates access is permissible by retrieving policy specification 373 for client computer 310 from policy store 371 to ensure that users comply with security policies, access rights, and anti-virus enforcement. Ex. 1005 ¶¶ 60, 66, 67.

c. Motivation to combine Cidon and Herrmann

Petitioner asserts that a skilled artisan would have added Herrmann’s gateway server and its functions of assigning an access policy and accepting requests for access to resources from clients to Cidon’s management server so “the modified system would have allowed automatic policy assignment and implementation, improving system efficiencies” and “would have allowed better real-time protection” “instead of waiting for an administrator to assign a policy manually.” Pet. 26–29 (citing Ex. 1004, Figs. 2; Ex. 1005 ¶¶ 18, 60, 65, 77, claim 21; Ex. 1010 ¶¶ 66, 82; Ex. 1002 ¶¶ 80–82); *id.* at 22 (combining Herrmann’s gateway with Cidon’s server would allow automatic policy assignment to improve system efficiency and reduce human errors).

d. 1[a][ii]: “wherein the policy defines access rights of the one or more users”

Petitioner contends that Cidon’s management server provides and enforces secure access policy configurations for secure file access and can assign different policies “by user or by group.” Pet. 29 (citing Ex. 1004 ¶¶ 67, 102, 108, 112, 115; Ex. 1002 ¶ 83).

e. Does Cidon disclose a single policy

Patent Owner argues that elements 1[a][ii], 1[b], 1[c], and 1[d] recite a *single* “policy” that defines (1) access rights of users, (2) the file contents to be encrypted “using cryptographic key information defined by the policy,” (3) storing searchable encrypted files on cloud platforms, and (4) managing access to a searchable encrypted file. Prelim. Resp. 17. Patent Owner also asserts that Petitioner treats disparate policies in Cidon “as if they were one and the same.” *Id.* Patent Owner argues that Petitioner combines “access policies” that control access to secure files with “placement policies” that store encrypted files, and these policies are different. *Id.* at 18.

For reasons that follow, we find these arguments unavailing.

“As a general rule, the words ‘a’ or ‘an’ in a patent claim carry the meaning of ‘one or more.’” *TiVo, Inc. v. EchoStar Commc’ns Corp.*, 516 F.3d 1290, 1303 (Fed. Cir. 2008). “The exceptions to this rule are extremely limited: a patentee must evince a clear intent to limit ‘a’ or ‘an’ to ‘one.’” *Baldwin Graphic Sys., Inc. v. Siebert, Inc.*, 512 F.3d 1338, 1342 (Fed. Cir. 2008) “The subsequent use of definite articles ‘the’ or ‘said’ in a claim to refer back to the same claim term . . . simply reinvoles that non-singular meaning.” *Id.*

01 Communique Lab., Inc. v. LogMeIn, Inc., 687 F.3d 1292, 1297 (Fed. Cir. 2012). At this stage, Patent Owner has not demonstrated a clear intent to limit “a policy” to a single policy as asserted. *See* Prelim. Resp. 3–6, 17–20.

We find insufficient record evidence at this stage that the '678 patent limits “a policy” to a single policy or what such a single policy comprises. A *file storage policy* “defines access rights, storage diversity requirements and a type of encryption to be applied to files for the corresponding user.” Ex. 1001, 2:18–22. It does not define cryptographic key information for element 1[b] or manage access for element 1[d]. A *policy-based framework* for encrypting, storing, accessing, querying, and managing data across cloud platforms can assign a policy that “defines the manner in which the users can access and process content stored on the cloud, [and] the mode in which the data is encrypted, stored, searched, and accessed.” *Id.* at 3:25–34. Policies of this framework do not define cryptographic key information in element 1[b] or manage access to a searchable encrypted file in element 1[d].

A policy of a policy assignment module *can be used to define* how a file is uploaded, stored, searched, downloaded, and/or processed, and it can “*be used to configure* access rights” that dictate how users process uploaded encrypted files. Ex. 1001, 3:45–52. Claim 1 recites that “the policy *defines* access rights of the one or more users” (emphasis added) in element 1[a][ii]. The '678 patent describes a policy of a policy assignment module is “*used to configure* access rights of . . . users.” *Id.* (emphasis added). The policy does not define or configure access rights. It is used to define or configure rights.

An *encryption module* can encrypt files to upload or store on cloud platforms *based on* a policy defined by the policy assignment module and a *selected policy can be used to define* encryption keys. Ex. 1001, 4:1–7. The policy does not *define* cryptographic key information as in element 1[b]; it is used by an encryption module to define encryption keys. On this record, we find insufficient evidence to depart from the general rule described above.

Cidon's management server defines, assigns, manages, and enforces secure access rights to encrypted cloud files. Ex. 1004 ¶ 102. A policy can (1) provide access to file repositories, (2) store file repository information, (3) analyze and encrypt files, (4) store and retrieve encryption keys, (5) provide access policy configuration for secure file access, (6) enforce a secure file access policy, and (7) report file access use and devices used for access. *Id.* Each access policy has a number of components that control secure file access, encryption, storage, and management. *Id.* ¶¶ 102, 108.

Cidon's management server 100 includes an IT Policy Enforcement Module 120 that allows enterprise administrators to define and enforce the policies for accessing secure files by different users/groups. Ex. 1004 ¶ 108. Different encryption parameters are used to encrypt different files associated with different users and groups. *Id.* ¶¶ 324, 326; *see* Pet. 24–25, 30–34.

Cidon also defines placement policies that control (1) file placement (storage) in specific directories, (2) file access and sharing permissions, (3) encrypting file content, and (4) managing user access. Ex. 1004 ¶¶ 206–217. A placement policy defines directories to store files, access and sharing permissions, copying, and file encryption. *Id.* ¶¶ 206–212. A policy covers *user* “[a]ccess and sharing permissions” to files. *Id.* ¶¶ 210, 212. A policy detects and handles access violations by alerting *users* and administrators so they can *change the policy*. *Id.* ¶¶ 213–217. Although *files* are placed in directories (Prelim. Resp. 18; Ex. 2001 ¶ 63), *a policy* controls and manages *user access* to encrypted files, encryption, and policy changes as claimed (Ex. 1004 ¶¶ 206–217). At this stage, Petitioner has made a sufficient showing that Cidon teaches or suggests a policy of element 1[a][ii].

- f. *1[b]: “encrypting, by the gateway device, using cryptographic key information defined by the policy, content of the file to produce a searchable encrypted file by:”*

Petitioner asserts that a skilled artisan would have combined Cidon’s management server with Herrmann’s gateway server to perform Cidon’s operations at a gateway. Petitioner contends that the gateway would encrypt cloud files as a searchable encrypted file by segmenting and encrypting file segments to form an encrypted file of the multiple encrypted file segments. Petitioner asserts that encrypted file segments would be searchable by a web service API for a document search and using metadata text/tags. Petitioner contends that Cidon taught or suggested searchable encrypted files because users could access a file or folder by browsing a web service account using an API to perform a document search. Petitioner asserts that Cidon’s management server extracted metadata from files uploaded to it, and the metadata could be used to help in file search operations using text or tags for searching. Pet. 29–32 (citing Ex. 1004 ¶¶ 91, 102, 166, 171, 222, 303–305, 309, 337, Figs. 13, 15; Ex. 1002 ¶¶ 84–91).

Petitioner contends that Cidon uses different encryption parameters to encrypt files for different users. Petitioner also asserts that a skilled artisan would have found it obvious that these encryption parameters would include “cryptographic key information” defined by the policy, and the encryption parameters would vary for specific users and groups. Petitioner asserts that Cidon also describes using encryption parameters to encrypt files, and an encryption key was a well-known encryption parameter. Pet. 33–34 (citing Ex. 1004 ¶¶ 108, 207, 208, 212, 324, 326; Ex. 1002 ¶¶ 89–91; Ex. 1001, 4:4–7, 10:1–3).

Patent Owner argues that the references do not disclose “encrypting . . . content of the file to produce a searchable encrypted file.” Patent Owner asserts that Cidon “contains no such disclosure” of encryption processes that produce a searchable encrypted file and searching the encrypted content of a file was highly unconventional. Prelim. Resp. 21. Patent Owner asserts that Cidon’s ability to access a file, search a document, and browse a file using metadata and text or tags does not teach or suggest the *contents* of encrypted documents are searchable. *Id.* at 22 (“As Dr. Black explains, a [skilled artisan] would have understood that the ability to search for and find files in a system is distinctly different from the ability to search the contents of the files themselves.”).

Element 1[b] of claim 1 recites “a searchable encrypted file.” It does not recite that the encrypted contents of the encrypted file are searchable as Patent Owner argues. *See* Prelim. Resp. 22.

This argument also ignores Petitioner’s reliance on Shikfa to teach the use of indexes of keywords of the encrypted content of documents to search the *contents of encrypted documents* as discussed at element 1[b][iii] below. Pet. 40–43. The ’678 patent system similarly uses indexes of encrypted keywords to search encrypted file content. Ex. 1001, 11:29–12:57, Figs. 3A, 3B. Obviousness is not determined on an element-by-element basis but on the claim as a whole based on the combined teachings of the references. *See In re Merck*, 800 F.2d 1091, (Fed. Cir. 1986) (“Non-obviousness cannot be established by attacking references individually where the rejection is based upon the teachings of a combination of references.”).

At this stage, Petitioner has made a sufficient showing that Cidon discloses element 1[b].

g. 1[b][i]: “dividing the file into a plurality of chunks”

Petitioner contends that Cidon segments a file into multiple segments, and Figure 13 of Cidon illustrates a segmentation that divides file 1410 into three segments 1430. Pet. 34–36 (citing Ex. 1004 ¶¶ 35, 305, 309, Figs. 13, 15). This contention, which Patent Owner does not contest at this stage, is supported by record evidence.

h. 1[b][ii]: “creating namespaces for one or more of the plurality of chunks; and”

Petitioner contends that Cidon describes calculating and creating a unique file segment identifier or signature for each file segment (chunk) based on the content of the file segment using a SHA2 signature. Petitioner asserts that a skilled artisan would have understood that a signature would identify the segments, and the segment identifiers are “namespaces” because they are “the set of names available for naming” file segments. Pet. 36–40 (citing Ex. 1004 ¶¶ 106, 305, 309, 383, Figs. 13, 15; Ex. 1002 ¶¶ 96, 98). These contentions, which Patent Owner does not contest at this stage, are supported by record evidence. File metadata may include the name, content type, and description of each file. Ex. 1004 ¶¶ 104–107, 113–121.

i. 1[b][iii]: “configuring the namespaces of the one or more chunks such that content of the file is encrypted in a manner that makes it searchable;”

Petitioner asserts that Cidon encrypts files and produces a searchable encrypted file with segment identifiers, but the identifiers (namespaces) do not make the encrypted *content* searchable. Petitioner contends that Shikfa uses pointers and identifiers to search and retrieve encrypted file segments by generating indexes of the keywords of the encrypted document content and using pointers to identify encrypted content of documents. Pet. 40–43.

Petitioner asserts that the indexes and pointers form namespaces that identify the encrypted documents and allow their encrypted contents to be searched. Pet. 40–43 (citing Ex. 1006 ¶¶ 29, 31, 36, Figs. 2, 3; Ex. 1002 ¶¶ 99–107; Ex. 1014). Petitioner contends that combining Shikfa’s search mechanism with Cidon, which already divided content into segments, would allow a chunk-by-chunk search of encrypted documents stored in cloud storage. Pet. 22, 43–45 (citing Ex. 1006 ¶¶ 39, 50; Ex. 1002 ¶¶ 103, 105–107; Ex. 1015, Ex. 1016).

j. Motivation to combine Shikfa with Cidon-Herrmann

Patent Owner argues that Petitioner relies on Shikfa for configuring identifiers (namespaces) of chunks to encrypt file content to be searchable, but “Petitioner fails to show any such motivation.” Prelim. Resp. 23–24. Patent Owner argues that Cidon’s management server is a complete system that encrypts cloud files and enforces secure access with comprehensive file encryption methods, and Petitioner fails to show why a skilled artisan would have modified Cidon’s “complete” system with Shikfa’s encryption of identifiers. *Id.* at 24. Patent Owner asserts that Cidon’s system provides “searchable encryption,” but Shikfa’s *client* encrypts documents so a broker server cannot access or discover the content of clients’ data. *Id.* at 25–26.

These arguments do not address Petitioner’s contentions that a skilled artisan would have combined Shikfa’s searchable encryption mechanism with Cidon’s encryption technique that divided content into segments with a segment identifier for each chunk to enable a search for encrypted chunks to “allow Cidon’s system to search and locate files on a segment-by-segment basis” as “implemented in Herrmann’s gateway server.” Pet. 43–44 (citing Ex. 1004, Fig. 13; Ex. 1006 ¶¶ 39, 50; Ex. 1002 ¶¶ 105–107).

Petitioner asserts that the modified system would have *searched encrypted file content* without requiring such capability at a storage provider to maintain privacy, to protect confidential information, and to allow storage on cloud storages that lack search capability. Pet. 44 (citing Ex. 1006 ¶ 50; Ex. 1002 ¶ 105).

Shikfa's searchable encryption would improve Cidon's ability to search the *content of encrypted document segments*. *KSR*, 550 U.S. at 417 (using a technique that improved one device to improve other devices in the same way is obvious unless its application is beyond the level of ordinary skill in the art). The improvement preserves the privacy of files, locates files by segments, and allows storage on cloud providers lacking search ability. Pet. 44; *see DyStar Textilfarben GmbH & Co. Deutschland KG v. C.H. Patrick Co.*, 464 F.3d 1356, 1368 (Fed. Cir. 2006) (holding that an implicit motivation exists when an "improvement" makes a product/process stronger, cheaper, faster, lighter, smaller, more durable, and/or more efficient).

Patent Owner's argument that "Cidon's system already provides for 'searchable encryption'" ignores Petitioner's rationale that Shikfa would enable Cidon to search encrypted files by the *content of segments*. Pet. 44.

Patent Owner's argument that Shikfa's encryption at a client would not be implemented on an intermediary gateway system or server of Cidon (and Herrmann) (Prelim. Resp. 26) attacks the references individually rather than as Petitioner proposes to modify Cidon-Herrmann's gateway server to search the encrypted *content of segments* as Shikfa teaches. Cidon and Herrmann already provide file search capability at a central server/gateway. Petitioner would enhance that capability rather than reconfigure the system of Cidon and Herrmann to move their search capability to a client. Pet. 44.

Patent Owner’s argument that searchable encryption is complex and unconventional (Prelim. Resp. 26–27) is contradicted by Shikfa’s high-level description of searchable encryption mechanisms (Ex. 1006 ¶¶ 29–37) and Cidon’s use of extracted metadata of encrypted files for text/tag searches of documents (Ex. 1004 ¶¶ 166–171) for expected results. Pet. 30–33, 43–45.

k. 1[c]: “storing, by the gateway device, the searchable encrypted file on the one or more cloud platforms based on the policy; and”

Petitioner contends that the gateway device of the combination would have functionality of Cidon’s management server and would store encrypted files on a cloud platform based on the policy via a connection to consumer-based file repositories through APIs or web access, e.g., by sending multiple encrypted file segments to the storage service. Petitioner also contends that Cidon’s policies include placement of files in specific directories or shares and violations of placement policies can result in moving files to reverse the violation. Pet. 46–49 (citing Ex. 1004 ¶¶ 10, 43, 208, 209, 214, 215, 229, 99, 100, 309, Abstract, claim 1, Figs. 2, 15; Ex. 1002 ¶ 110).

Patent Owner argues that Cidon does not disclose a policy that defines access rights in element 1[a][ii], encrypts file content in element 1[b], stores the searchable encrypted file in element 1[c], and manages access in element 1[d]. Prelim. Resp. 17. As discussed above for element 1[a][ii], Cidon does disclose a policy that can (1) provide access to file repositories, (2) store file repository information, (3) analyze and encrypt files, (4) store and retrieve encryption keys, (5) provide access policy configuration for secure file access, (6) enforce a secure file access policy, and (7) report file access use and devices used for access. Ex. 1004 ¶ 102. A single policy controls secure file access, encryption, storage, and management. *Id.* ¶¶ 102, 108.

Cidon also defines placement policies that control (1) file placement (storage) in specific directories, (2) file access and sharing permissions, (3) encrypting file content, and (4) managing user access. Ex. 1004 ¶¶ 206–217. A placement policy defines directories to store files, access and sharing permissions, copying, and file encryption. *Id.* ¶¶ 206–212.

At this stage, Petitioner has made a sufficient showing that Cidon teaches or suggests element 1[c].

- l. 1[d]: “managing access to the searchable encrypted file by the one or more users based on the policy.”*

Petitioner asserts that Cidon provides different access policies to users for cloud storage files by providing an access policy configuration for secure file access and enforcing an access policy for secure file access. Petitioner asserts that Cidon manages access via a management server and API access to cloud storage services such as Dropbox, and the IT Policy Enforcement Module 120 provides an admin interface to allow an administrator to define access policies by user or group. Petitioner further asserts that such access policies, once defined, are enforced through APIs. Petitioner also contends that a skilled artisan would have understood that Cidon’s management server controlled user access to searchable encrypted files based on the assigned access policy by “provid[ing] access policy configuration for secure file access” and by “enforc[ing] access policy for secure file access.” Pet. 49 (citing Ex. 1004 ¶¶ 67, 102, 108, 113; Ex. 1002 ¶ 112). These contentions, which Patent Owner does not contest at this stage, are supported sufficiently by record evidence.

m. Motivation to combine Cidon and Herrmann

Petitioner asserts that a skilled artisan would have added Herrmann’s gateway server and access policy assignment to Cidon’s management server to allow automatic policy assignment, improve system efficiency, offer real-time protection, and reduce human errors predictably. Pet. 22, 27–29.

Patent Owner argues that a skilled artisan would not include Cidon’s server in Herrmann’s gateway. Prelim. Resp. 28. This argument disregards that an obviousness inquiry considers the combined teachings of references. Whether Cidon is a “primary” or “secondary” reference (*see* Prelim. Resp. 28–29) “is merely a matter of presentation with no legal significance.” *In re Mouttet*, 686 F.3d 1322, 1333 (Fed. Cir. 2012).

Petitioner provides the access policy assignment functions of Cidon’s management server in Herrmann’s gateway server based on Herrmann’s teachings to perform access policy assignment in a gateway server to update access policies automatically for improved efficiency and reduced error. Pet. 25–28 (citing Ex. 1005 ¶¶ 60, 77, claim 21, Fig. 2; Ex. 1002 ¶¶ 80, 81; *see also In re Applied Materials, Inc.*, 692 F.3d 1289, 1298 (Fed. Cir. 2012) (“A reference must be considered for everything that it teaches.”)).

Herrmann’s teachings are reasonably pertinent to the problem solved by the inventors of providing secure cloud storage distribution/aggregation on cloud storage platforms by assigning file storage policies to users via a gateway device independent of cloud storage vendors. Ex. 1001, 1:16–20, 2:9–30; Ex. 1005 ¶¶ 60, 65–67; *see also In re Clay*, 966 F.2d 656, 659 (Fed. Cir. 1992) (“If a reference disclosure has the same purpose as the claimed invention, the reference relates to the same problem, and that fact supports use of that reference in an obviousness rejection.”); *cf.* Prelim. Resp. 30.

Herrmann's gateway server 350 operates with integrity server 370 to ensure compliance with anti-virus policies and verify client 310 can access protected data. Ex. 1005 ¶¶ 60, 65, 67, 77. Cidon's management server also would cooperate with Herrmann's gateway server to apply access policies to client devices. Pet. 24–29 (Herrmann's gateway server would accommodate Cidon's management server for predictable results); *Intelligent Bio-Systems, Inc. v. Illumina Cambridge Ltd.*, 821 F.3d 1359, 1367 (Fed. Cir. 2016) (“The reasonable expectation of success requirement refers to the likelihood of success in combining references to meet the *limitations of the claimed invention.*”) (emphasis added); *Pfizer, Inc. v. Apotex, Inc.*, 480 F.3d 1348, 1364 (Fed. Cir. 2007) (absolute predictability of success is not required).

On this record, we find that Petitioner has established a reasonable likelihood that claim 1 is unpatentable over Cidon, Shikfa, and Herrmann.

5. *Independent Claim 16*

a. *16[pre]: “A secure cloud storage system comprising:”*

Petitioner contends that Cidon discloses a management server of a secure cloud storage system for “encrypting a file” including “segmenting the file into multiple file segments” that are sent to the cloud storage device. Pet. 50 (citing Ex. 1004 ¶¶ 57, 99, 100, Fig. 2; contentions for 1[pre]). These contentions, which Patent Owner does not contest at this stage, are supported by record evidence.

b. *16[a]: “one or more processors;”*

Petitioner asserts that Cidon's management server 100 is a computer that includes a “processing unit.” Pet. 51 (citing Ex. 1004 ¶¶ 307, 407, 416). These contentions, which Patent Owner does not contest at this stage, are supported by record evidence.

c. 16[b]: “a communication interface mechanism”

Petitioner contends that Cidon discloses that its management server communicates with user devices 60, 70 to receive requests for decrypting files or send encryption keys to user devices and connects to file repositories through API 101, 103 and interfaces such as file transfer protocol (FTP) and secure FTP (SFTP). Petitioner also contends that a skilled artisan would understand that the management server includes a communication interface mechanism. Pet. 51–52 (citing Ex. 1004 ¶¶ 100, 101, 309, 340, 342; Ex. 1002 ¶ 118). These contentions, which Patent Owner does not contest at this stage, are supported by record evidence.

d. 16[c]: “one or more internal data storage devices operatively coupled to the one or more processors and storing:”

Petitioner contends that Cidon’s management server 100 includes internal data storage such as memory operatively coupled to a processing unit that stored software instructions or a computer program to execute the described methods when executed by a processing unit and various modules. Pet. 52 (citing Ex. 1004 ¶¶ 50, 101, 102, 307, 407, 412, 416; Ex. 1002 ¶ 119). These contentions, which Patent Owner does not contest at this stage, are supported by record evidence.

e. 16[c][i]: “a policy assignment module, which, when executed by the one or more processors, implements a policy selected from a group of policies for a user,”

Petitioner contends that Cidon’s management server includes an IT policy enforcement module and interface that allow an administrator to define and implement different access policies for different users/groups. Pet. 53 (citing Ex. 1004 ¶¶ 50, 101, 108; Ex. 1002 ¶ 121).

Patent Owner argues that Cidon does not assign a policy selected from a group of policies because an administrator defines the access policies for users through a web browser interface. Prelim. Resp. 33. Patent Owner asserts that a skilled artisan would understand that defining a policy differs from selecting a policy from a group of policies. *Id.* (citing Ex. 2001 ¶ 91).

Cidon allows companies to organize users into groups and assign different access policies to each group. Ex. 1004 ¶ 108. Administrators can define access policies for each group, and the policies are enforced by APIs that implement a policy for a particular user/group selected from the group of policies defined by a company for its enterprise users and groups. *Id.*

Petitioner asserts that skilled artisans would understand such teachings to mean IT policy enforcement module 120 implements access policies that an administrator defines for users and groups. Petitioner contends that IT policy enforcement module checks users' credentials to determine if access should be granted based on a policy defined by an IT administrator for that user from a group of policies. Pet. 53. Dr. Lee testifies that a skilled artisan would have found it obvious that module 120 "would select a policy for the appropriate user or user group to be implemented." Ex. 1002 ¶ 121.

An administrator defines access policies for different users or groups. IT Policy Enforcement Module 120 checks the credentials of the requesting application user and the file to determine if access is to be granted. Ex. 1004 ¶ 108. Module 120 enforces access policies that IT administrators define and store in the module by applying the applicable policy of the group of defined policies to each user "to determine if access is to be granted." *Id.*

Petitioner has provided sufficient evidence to establish that Cidon discloses element 16[c][i].

- f. 16[c][i][A]/16[c][i][B]: “wherein the policy defines and manages access to and processing of a file to be uploaded on a cloud,” “wherein the policy defines access rights of the user;”*

Petitioner contends that Cidon’s policy defines and manages access to and processing of a file to be uploaded on a cloud and defines access rights of the user. Pet. 53 (citing contentions for elements 1[a][i] and 1[a][ii]). These contentions, which Patent Owner does not contest at this stage, are supported by record evidence.

- g. 16[c][ii]: “an encryption module, which, when executed by the one or more processors:”*

Petitioner asserts that a skilled artisan would understand that Cidon’s encryption would be performed by an encryption module using instructions executable by the processor. Pet. 54 (citing Ex. 1004 ¶¶ 50, 102; Ex. 1002 ¶ 124). This contention, which Patent Owner does not contest at this stage, is supported by record evidence.

- h. 16[c][ii][A]: “using cryptographic key information defined by the policy, produc[ing] a searchable encrypted file by encrypting content of the file to be stored across one or more cloud platforms;”*

Petitioner contends that Cidon uses cryptographic key information defined by the policy to produce a searchable encrypted file by encrypting the content of the file and storing the encrypted content across multiple cloud platforms. Pet. 54 (citing Ex. 1004 ¶ 174; Ex. 1002 ¶ 125; contentions for element 1[d]). These contentions, which Patent Owner does not contest at this stage, are supported by record evidence.

- i. *16[c][ii][B]/16[c][ii][C]/16[c][ii][D]: “divid[ing] the file into a plurality of chunks;” “creat[ing] namespaces for one or more of the plurality of chunks; and” “configure[ing] the namespaces of the one or more chunks such that content of the file is encrypted in a manner that makes it searchable;”*

Petitioner contends that Cidon alone, or with Shikfa, discloses or renders obvious these limitations. Pet. 55 (citing contentions for similar elements 1[b][i], 1[b][ii], and 1[b][iii]). These contentions, which Patent Owner does not contest at this stage, are supported by record evidence.

- j. *16[c][iii]: “a storage module, which, when executed by the one or more processors, stores the searchable encrypted file on the one or more cloud platforms based on the policy; and”*

Petitioner asserts that Cidon’s management server sends a searchable encrypted file to cloud storage, which would have been obvious to do based on the policy. Pet. 55 (citing Ex. 1004 ¶ 50, 102; Ex. 1002 ¶ 130; contentions for elements 16[a] and 16[c]). These contentions, which Patent Owner does not contest at this stage, are supported by record evidence.

- k. *16[c][iv]: “a management module, which, when executed by the one or more processors manages and controls access to the searchable encrypted file by the user based on the policy.”*

Petitioner contends that Cidon’s management server manages access to the searchable encrypted file by the users based on the policy. Pet. 55–56 (citing Ex. 1004 ¶ 50, 102; Ex. 1002 131; contentions for elements 16[a] and 16[c]). These contentions, which Patent Owner does not contest at this stage, are supported by record evidence.

On this record, we find that Petitioner has established a reasonable likelihood that claim 16 is unpatentable over Cidon, Shikfa, and Herrmann.

6. *Dependent Claims 2, 3, 8–14, 17, and 21–27*

Petitioner provides detailed contentions showing Cidon, Herrmann, and/or Shikfa teach or suggest the limitations of dependent claims 2, 3, 8–14, 17, and 21–27 with Dr. Lee’s supporting testimony. Pet. 56–69. These contentions, which Patent Owner does not contest at this stage, are supported by evidence of record. On this record, we find that Petitioner has shown a reasonable likelihood that claims 2, 3, 8–14, 17, and 21–27 are unpatentable over Cidon, Herrmann, and Shikfa.

E. Ground 2: Alleged Obviousness Over Cidon, Shikfa, Herrmann, Fellenstein

Petitioner asserts that claim 6 is unpatentable under 35 U.S.C. § 103 over Cidon, Shikfa, Herrmann, and Fellenstein. Pet. 7, 69–70.

1. *Fellenstein (Ex. 1007)*

Fellenstein adds keywords for retrieving a file to the file name so that each file name with keywords that match an inputted retrieval word can be regarded as a result of the retrieval. Ex. 1007 ¶ 8.

2. *Claim 6: “wherein the step of configuring the namespaces comprises storing content of the file as filenames.”*

Petitioner relies on teachings of Fellenstein (Ex. 1007) that key words from a file’s content can be used in the filename, and the keyword filenames can be used to retrieve the file. Pet. 70 (citing Ex. 1007 ¶ 8).

3. *Motivation to Combine*

Petitioner asserts that a skilled artisan would have been motivated to add this well-known functionality to Cidon, Herrmann, and Shikfa to provide an additional search option. Pet. 70 (citing Ex. 1002 ¶¶ 167, 168). These contentions, which Patent Owner does not contest at this stage, are supported by evidence of record.

Petitioner has established a reasonable likelihood that claim 6 is unpatentable over Cidon, Herrmann, Shikfa, and Fellenstein.

F. Ground 3: Alleged Obviousness Over Cidon, Shikfa, Herrmann, Hirai

Petitioner asserts claim 15 is unpatentable under 35 U.S.C. § 103 over Cidon, Shikfa, Herrmann, and Hirai. Pet. 7, 71–72.

1. *Hirai (Ex. 1008)*

Hirai discloses a file retrieval system that encodes a file name and key words related to file data using a cryptographic key. Ex. 1008, 5:64–6:13.

2. *Claim 15: “. . . wherein said encrypting further comprises encrypting one or more of filename and search indices.”*

Petitioner relies on Hirai (Ex. 1008) for a file retrieving system that generates and encrypts file names and key words for file data and Shikfa for encrypting indexes of keywords to search encrypted documents. Pet. 71–72 (citing Ex. 1006 ¶ 29, Fig. 2; Ex. 1008, 5:64–6:13; Ex. 1002 ¶ 170).

Petitioner asserts that Shikfa’s and Hirai’s functions would protect file names and indexes. Pet. 72 (citing Ex. 1006 ¶ 50; Ex. 1002 ¶ 172). These contentions, which Patent Owner does not contest at this stage, are supported by evidence of record. Petitioner has established a reasonable likelihood claim 15 is unpatentable over Cidon, Herrmann, Shikfa, and Hirai.

G. Ground 4: Alleged Obviousness Over Auradkar, Chiueh, Chambers

Petitioner asserts claims 1–3, 8–17, and 21–27 are unpatentable under 35 U.S.C. § 103 over Auradkar, Chiueh, and Chambers.¹⁴ Pet. 7, 72–135.

¹⁴ Petitioner asserts that claims 1–3, 8–19, and 21–27 are unpatentable over Auradkar, Chiueh, and Chambers (Pet. 7, 72), but Petitioner presents no substantive arguments for claims 18 and 19 (*id.* at 72–135).

1. *Auradkar (Ex. 1009)*

Auradkar controls access to cloud data 512 in cloud container 500 by providing an enterprise access policy 530 that determines how data 512 stored in data container 510 of cloud container 500 can be accessed, manipulated, retrieved, and searched as shown in Figure 5, which is reproduced below. Ex. 1009 ¶ 117.

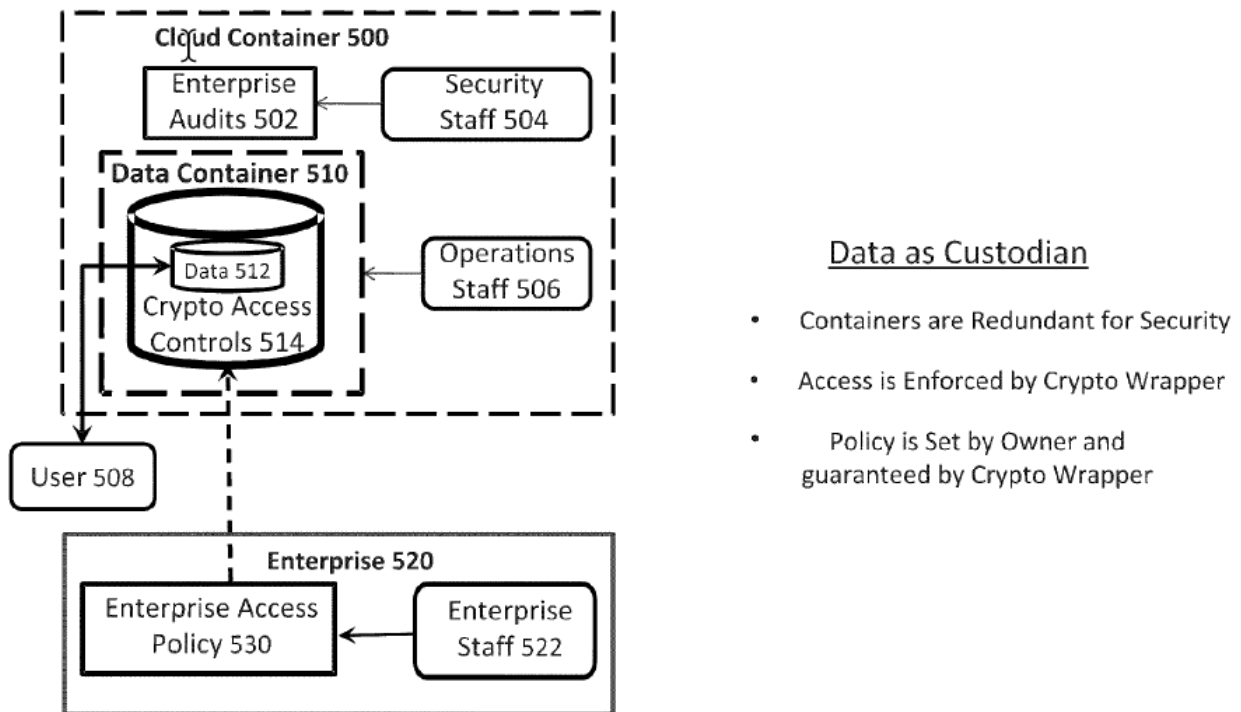


Figure 5 depicts enterprise access policy 530 that controls how data in cloud container 500 is accessed, retrieved, and searched. Ex. 1009 ¶ 117.

Payloads and tags are encrypted. The encrypted records, tags, and indexes are uploaded to the cloud as searchable, encrypted data records and encrypted indexes so that the content and records are identified by searching indexes. We reproduce Figure 15 of Auradkar below to illustrate this arrangement for searching the encrypted contents of encrypted files. *See* Ex. 1009 ¶¶ 125, 127, 130, 131.

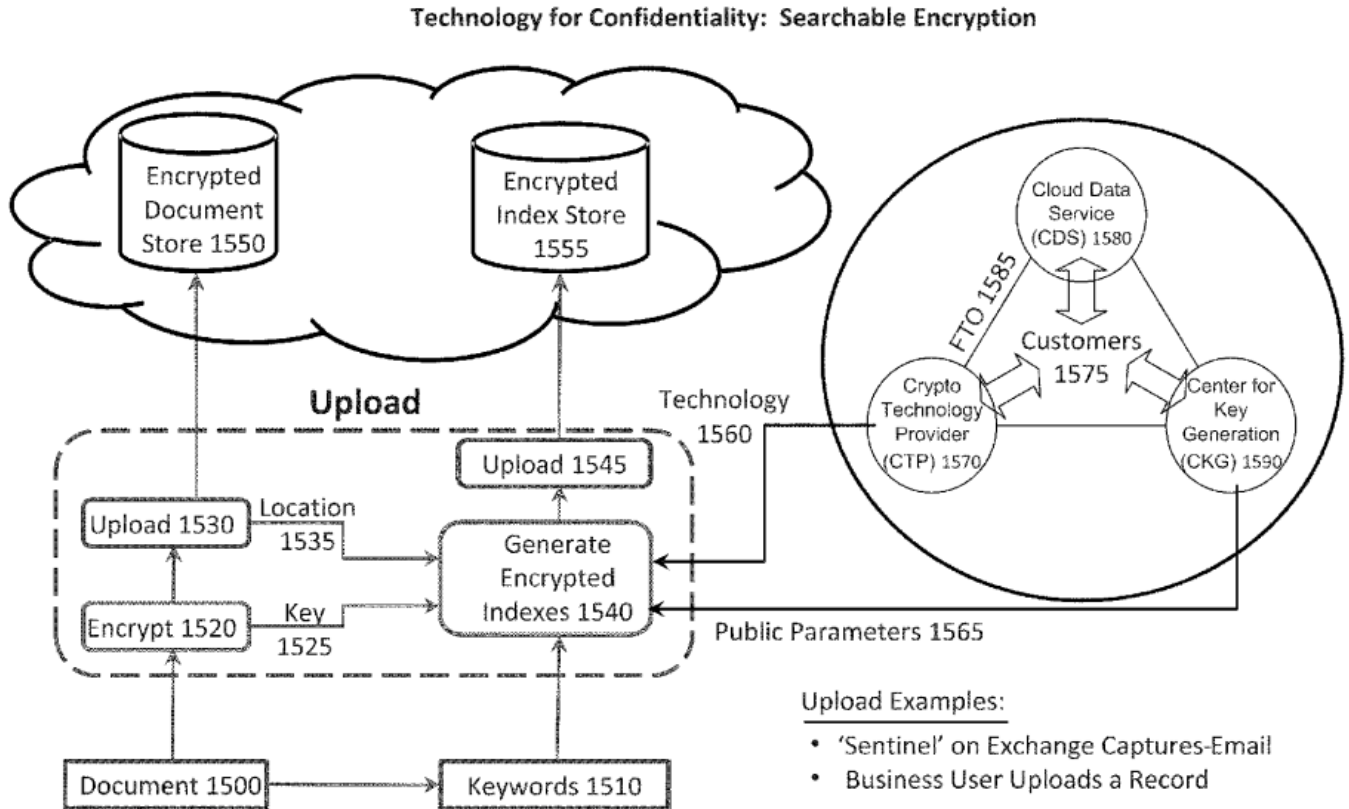


FIG. 15

Figure 15 illustrates documents 1500 and keywords 1510 that are encrypted and uploaded to the cloud into stores 1550, 1555. Ex. 1009 ¶ 130.

2. Chiueh (Ex. 1011)

Chiueh's system stores encrypted document pages and encrypts words in an index (Global Search Index (GSI) of a Significant Word Set (SWS)). Encrypted keyword searches can obtain a first index that identifies encrypted pages with the encrypted keywords. Ex. 1011 ¶¶ 8, 20, 25, 40, Fig. 3.

Each encrypted word in the GSI maps to a document ID that identifies an encrypted page where the word is found, and the document ID is a combination of a file name and a page offset in the document. *Id.* ¶ 40.

3. Chambers (Ex. 1010)

Chambers discloses a network access device 102 that may operate as a gateway device that applies access control policies 117 to client devices 108 to control their access to LAN 105 as shown in Figure 1, reproduced below.

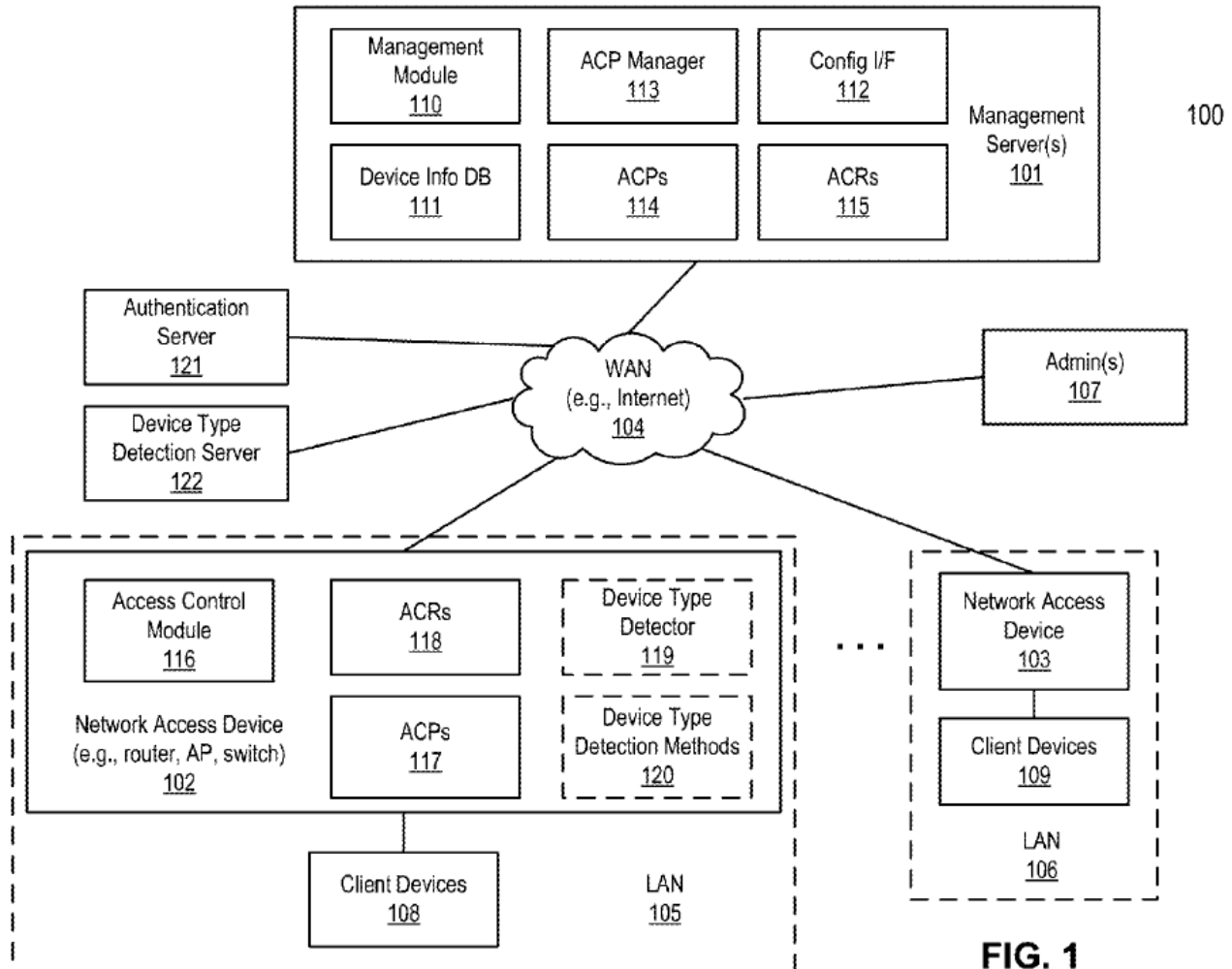


FIG. 1

Figure 1 illustrates management server 101 and access control policy manager 113 that transmits access control policies (ACPs) 117 and access control rules (ACRs) 118 to network access devices 102 such as gateways and access points to control access of client devices 108 by enforcing ACPs 117 and ACRs 118. Ex. 1010 ¶¶ 24, 27, 28.

4. *Independent Claim 1*

a. *1[pre]*

Petitioner contends that Auradkar discloses a method for encrypting and storing files. Pet. 79–80 (citing Ex. 1009, Fig. 15; Ex. 1002 ¶ 190). This contention, which Patent Owner does not contest at this stage, is supported by evidence of record.

b. *1[a][i] assigning a policy to manage access*

Petitioner asserts that Auradkar assigns to enterprise staff a policy to manage access to a file stored on cloud container 500, and different policies are assigned to different accessing entities and tasks. Petitioner also asserts that Chambers’ network access device 102 is a gateway device with access control module 116 that selects and applies an access control policy to a user automatically and to different user groups (e.g., “staff,” “iPad group”). Pet. 80–85 (citing Ex. 1009 ¶¶ 112, 113, 116, 117, 119, Figs. 1, 2, 5, 6; Ex. 1010 ¶¶ 21, 24, 46, Figs. 1, 4A; Ex. 1002 ¶¶ 195–198; Ex. 1001 9:11–19).

Petitioner contends that a skilled artisan would have used Chambers’ gateway to implement Auradkar’s “assigning” and other claimed functions and automatically assign the pertinent security policies because an enterprise has different users who use multiple devices to access cloud data. Petitioner contends that the combined system would assign a policy automatically based on a user’s role in an organization or users’ devices to apply a policy consistently, avoid repeated policy configuration for the same user, improve system efficiency, and reduce human errors. Pet. 85–87 (citing Ex. 1009, Fig. 11; Ex. 1010 ¶¶ 5, 6, 21, 29, 66, 82; Ex. 1005 ¶¶ 18, 77; Ex. 1002 ¶¶ 200–202). These contentions, which Patent Owner does not contest at this stage, are supported by evidence of record.

c. 1[a][ii]: the policy defines user access rights

Petitioner contends that Auradkar discloses a policy that defines user access rights with the policy and enforcement within the control of users and associated logs are accessible only with the specific capabilities granted to a user. Stored cloud data are accessed, manipulated, retrieved, and searched according to the access policy. Pet. 87–88 (citing Ex. 1009 ¶¶ 112, 117).

Patent Owner argues that Petitioner fails to show that Auradkar uses a single policy that meets elements 1[a][ii], 1[b], 1[c], and 1[d], but instead relies on disparate policies in Auradkar “as if they were one and the same.” Prelim. Resp. 34–35. Patent Owner argues that Petitioner cites Auradkar’s “access policies” that control users’ access to data to disclose a policy that defines user access rights but relies on a separate disclosure of data storage policies that control how data could be stored as a searchable encrypted file based on the policy. *Id.* at 35. These arguments are unavailing.

Auradkar allows users to create and enforce policies of the enterprise to include encryption and data accessibility only for users with specific capabilities. Ex. 1009 ¶ 112. Auradkar discloses that enterprises can set an access policy to control how data is stored, accessed, manipulated, retrieved, and searched to include crypto access controls, and different access policies and crypto controls can be applied to different entities or tasks performed by enterprise staff. *Id.* ¶ 117, Fig. 5 (cited in Pet. 80–83 for “a policy”).

Auradkar illustrates enterprise access *policy* 530 in Figure 5, which we reproduced above. Enterprise access policy 530 governs the access of enterprise 520 and enterprise staff 522 to data in cloud container 500 and data storage, access, manipulation, retrieval, and search. Ex. 1009 ¶ 117.

A different enterprise access policy can be applied to each different accessing entity or task, and each such policy 530 “can be reflected by the crypto access controls 514 of data container 510.” *Id.* We disagree that Petitioner conflates policies. Prelim. Resp. 35–36. Auradkar describes an *enterprise access policy 530* that defines access rights, encryption, storage, and managing access. Ex. 1009 ¶ 117. That Auradkar describes details of the policy in other paragraphs does not negate this description of a policy. As discussed in Ground 1, a policy can be one or more policies, and the ’678 patent also describes a policy comprising multiple aspects or sub-policies. Ex. 1001, 2:15–30, 3:23–67, 4:1–19, 9:11–10:16.

d. 1[b]: encrypting using a key defined by the policy

Petitioner contends that Auradkar encrypts a record, metadata, and/or tags and encrypts document 1500 with associated keywords. Petitioner asserts that Auradkar uploads encrypted document to the cloud so customers can search the indexes to identify content and/or records matching an index. Petitioner asserts that Auradkar allows users to access matching content “based on privileges or not.” Petitioner contends that Auradkar teaches a policy that defines encryption keys. Pet. 88–93 (citing Ex. 1009 ¶¶ 96, 124, 125, 127, 130, 133, Figs. 11, 12, 15, 16; Ex. 1002 ¶¶ 210, 211; Ex. 1001, 4:4–7, 12:44–47, Fig. 3B).

Patent Owner argues generally that Auradkar does not disclose a single policy that satisfies elements 1[a][ii], 1[b], 1[c], and 1[d]. Prelim. Resp. 34–37. As discussed above for element 1[a][ii], Auradkar teaches an *enterprise access policy 530* that defines access rights, encryption, storage, and managing access. Ex. 1009 ¶ 117. At this stage, we find that Petitioner has established sufficiently that Auradkar discloses element 1[b].

e. 1[b][i]–1[b][iii]: namespaces for chunks

Petitioner contends that Auradkar discloses breaking a document into XML fragments (chunks) with different protection levels and applying labels to each fragment to control access thereto using tags as namespaces with filenames to search files or segments. Petitioner asserts that Chiueh creates and configures namespaces for chunks to allow search, identification, and retrieval of segments of encrypted documents. Pet. 93–106 (citing Ex. 1009 ¶¶ 92, 95, 98, 125, 150, Figs. 11, 12, 19; Ex. 1011 ¶¶ 20–25, 28, 40, Figs. 2, 3; Ex. 1002 ¶¶ 212–214, 217–221, 232, 233; Ex. 1014; Ex. 1001, 12:14–18, 12:42–55; element 1[b][ii] contentions). These contentions, which Patent Owner does not contest at this stage, are supported by record evidence.

f. 1[c]: storing searchable encrypted file

Petitioner contends that Auradkar discloses uploading and storing a searchable, encrypted file on cloud platforms based on a policy. Petitioner contends that Auradkar’s policy controls how and where data can be stored, how long it can be stored, and how to upload document 1500 by encrypting it and uploading it to encrypted document store 1550 provided by a cloud service provider(s). Petitioner asserts that it would have been obvious to use Chambers’ gateway device to do so. Pet. 106–108 (citing Ex. 1009 ¶¶ 96, 189, Figs. 15, 28; Ex. 1002 ¶ 236; contentions for element 1[a][i]).

Patent Owner argues that Auradkar does not disclose a single policy that satisfies elements 1[a][ii], 1[b], 1[c], and 1[d]. Prelim. Resp. 34–37. As discussed above for element 1[a][ii], Auradkar teaches an *enterprise access policy* 530 that defines access rights, encryption, storage, and managing access. Ex. 1009 ¶ 117. At this stage, we find that Petitioner has established sufficiently that Auradkar discloses element 1[c].

g. 1[d]: managing access to searchable encrypted file

Petitioner contends that Auradkar manages access to the searchable, encrypted file by users based on a policy within the control of users or an enterprise so data and logs are encrypted and accessible within the specific capabilities granted to a user and within various crypto access controls that are guided by enterprise access policy 530 to protect the data from unwanted access. Pet. 108–109 (citing Ex. 1009 ¶¶ 112, 113, 117, Fig. 5).

Patent Owner argues that Auradkar does not disclose a single policy that satisfies elements 1[a][ii], 1[b], 1[c], and 1[d]. Prelim. Resp. 34–37. As discussed above, Auradkar’s *enterprise access policy 530* defines access rights, encryption, storage, and managing access. Ex. 1009 ¶ 117. At this stage, we find that Petitioner has established sufficiently that Auradkar discloses element 1[d].

h. Motivation to combine the references

Petitioner contends that a skilled artisan would have been motivated to combine Auradkar’s computer security system that could search encrypted data with Chiueh’s mechanism that searched individual document pages to enable a more efficient search and retrieval of individual pages (chunks) instead of the entire document. Pet. 79. Petitioner contends that Chiueh’s system assigned a document identification (namespace) to each encrypted page to indicate an encrypted page where a given word could be found and adding this capability to Auradkar’s whole-document search would allow searching of encrypted files to retrieve encrypted *portions* stored in the cloud and use bandwidth resources efficiently. *Id.* at 96–97. Petitioner asserts that Chiueh’s functions would improve Auradkar by allowing the retrieval of individual pages rather than an entire document. *Id.* at 105–106.

Patent Owner argues that Chiueh teaches against using Chambers' gateway as an interface between a client and protected data sources to carry out the claimed operations of the gateway because Chiueh encrypts pages and word sets at a client rather than an intermediary gateway. Prelim. Resp. 38–39. Patent Owner argues that Auradkar's comprehensive system already allows for search and retrieval of encrypted document portions stored in the cloud for “searchable encryption” of documents. *Id.* at 39.

Patent Owner's individual attack on the references is unavailing. Petitioner proposes to improve “Auradkar's existing whole-document search” so “the modified system would have allowed retrieval of encrypted document portions stored in the cloud” to conserve network bandwidth as Chiueh teaches. Pet. 97; *KSR*, 550 U.S. at 417; *DyStar*, 464 F.3d at 1368.

Petitioner contends that Auradkar tags payloads for searching XML fragments (Pet. 94–96), as Patent Owner recognizes (Prelim. Resp. 39), but wants to improve this capability with Chiueh's namespace document ID for each encrypted page so encrypted words are mapped to a document ID and a given word can be found (Pet. 96–97) even in document chunks (*id.* at 97).

Petitioner also contends that a skilled artisan would have considered Auradkar's XML tags to be namespaces for payloads. Pet. 96. Modifying Auradkar with Chiueh's document IDs would improve Auradkar's ability to retrieve all encrypted document portions, not just XML documents or XML fragments. *See* Pet. 97. The capability of Auradkar's system is enhanced beyond searching XML fragments with XML tags by using namespace IDs to search *encrypted portions of any document* stored in the cloud. *Id.* at 96–97. Enhancing Auradkar to assign namespace IDs to all document portions obviates the need to perform this operation at a client. *Cf.* Prelim. Resp. 38.

Petitioner is not modifying Chiueh's client. Petitioner has enhanced Auradkar's system by using namespace document IDs to search all of the encrypted document portions (not just XML fragments). Pet. 96–97. Even if Chiueh's document ID is limited to clients, as Patent Owner and Dr. Black assert (Prelim. Resp. 38; Ex. 2001 ¶ 105), the modification is to Auradkar, not Chiueh, *and*, a skilled artisan could weigh pros and cons and determine that the enhancement to Auradkar's system would outweigh any perceived problems with using Chiueh's document ID outside a client when Auradkar already uses similar XML tags to search XML fragments. *See Mouttet*, 686 F.3d at 1331 (“A reference may be read for all that it teaches, including uses beyond its primary purpose.”), 1334 (explaining that an inferior combination is not inapt for obviousness purposes unless it would be unlikely to work).

Patent Owner and Dr. Black assert that a skilled artisan would not use Chiueh's encryption techniques on an intermediary gateway or on remote systems in Chambers and Auradkar because Chiueh uses a *client* to encrypt document pages and word sets. Patent Owner asserts that *remote servers* do not have keys and cannot decrypt document pages and word sets. Prelim. Resp. 38–39 (citing Ex. Ex. 2001 ¶ 105 (citing Ex. 1011 ¶¶ 8–10)). This argument is unavailing because Chiueh does not counsel against encrypting document pages and word sets at an enterprise system of Auradkar or at an intermediate gateway of the Auradkar-Chambers combination. Pet. 80–87. Chiueh encrypts document pages and word sets at the client rather than at a *remote server* where the document pages and word sets are *stored*. Ex. 1011 ¶ 10 (“the client respectively encrypts the document pages and the significant word set by using different keys, and then transmits the encrypted pages and the significant word set to the remote server for storage.”).

Patent Owner argues that a skilled artisan would not have a reasonable expectation of success in modifying Auradkar with Chiueh's page-based "significant-word-set" technique. Prelim. Resp. 40–41. Dr. Black testifies that a skilled artisan would not expect success because the references are incompatible. Ex. 2001 ¶¶ 108, 109. However, Petitioner proposes to add Chiueh's functions to Auradkar's system to enhance its capabilities where Auradkar already uses XML tags on documents and segments. Pet. 96–97, 101–106. Chiueh's encrypted keyword index retrieves document pages to complement Auradkar's XML tags. *Id.* Chiueh uses encryption at a client, rather than a remote server, for bandwidth and security reasons that do not impact on encrypting at Auradkar's system. *See* Ex. 1011 ¶¶ 4–8, 20–40.

Petitioner asserts that a skilled artisan would have applied Auradkar's functions at an intermediary gateway of Chambers so the system could select and apply appropriate access control policies to client devices automatically without intervention by an administrator or management server. Petitioner contends that the modified system automatically assigns, configures, applies, and updates policies based on a user's role in an organization or a user's device for more consistent application of the policy, avoidance of repeated policy configurations for the same user, improved efficiency of the system, reduced human errors, and real-time protection. Pet. 84–87 (citing Ex. 1010 ¶¶ 5, 6, 21, 24, 46, Fig. 1; Ex. 1002 ¶ 200).

Patent Owner's arguments do not address sufficiently Petitioner's asserted reasons to combine the teachings of Auradkar and Chambers to improve Auradkar's system by implementing access policy assignment and other functions at Chambers' intermediary gateway as automated functions for the benefits described above. Pet. 85–87; *see* Prelim. Resp. 43–47.

On this record, we find that Petitioner has established a reasonable likelihood that claim 1 is unpatentable over Auradkar, Chiueh, and Chambers.

5. *Claim 16*

Petitioner contends that Auradkar, Chambers, and Chiueh render obvious a secure cloud storage system for encrypting and storing files in the cloud by using a processor, network interface, and memory to perform the claimed functions. Pet. 109–118. These contentions, which Patent Owner does not contest at this stage, are supported by record evidence. On this record, we find that Petitioner has established a reasonable likelihood that claim 16 is unpatentable over Auradkar, Chiueh, and Chambers.

6. *Dependent Claims 2, 3, 8–15, 17, and 21–27*

Petitioner provides detailed contentions for claims 2, 3, 8–15, 17, and 21–27. Pet. 118–135. These contentions, which Patent Owner does not contest at this stage, are supported by record evidence. On this record, we find Petitioner has established a reasonable likelihood that claims 2, 3, 8–15, 17, and 21–27 are unpatentable over Auradkar, Chiueh, and Chambers.

H. Ground 5: Alleged Obviousness Over Auradkar, Chiueh, Chambers, Inoue

Petitioner asserts that claim 6 is unpatentable under 35 U.S.C. § 103 over Auradkar, Chiueh, Chambers, and Inoue. Pet. 7, 135–138.

1. *Inoue (Ex. 1012)*

Inoue correlates one or more extracted keywords with image data as keywords for image data searches. Inoue also uses the keywords as the title of the image data. Ex. 1012 ¶ 104, Fig. 4.

2. *Claim 6*

Petitioner asserts that a skilled artisan would have included Inoue's functionality of storing content of a file as a filename into the Auradkar-Chiueh-Chambers system to produce filenames that include a keyword with a reasonable expectation of success because the practice of assigning keywords to filenames was well-known and compatible with the Auradkar-Chiueh-Chambers system. Pet. 135–138 (citing Ex. 1009 ¶ 130, Fig. 15; Ex. 1012 ¶ 104, Fig. 4; Ex. 1002 ¶¶ 299–306; Ex. 1001, 12:7–9).

3. *Motivation to combine*

Petitioner asserts that it would have been obvious to use Inoue's functions in the Auradkar-Chiueh-Chambers system to allow searching of files via their file names as a faster, more efficient way of searching and for expanded search options. Pet 137–138. These contentions, which Patent Owner does not contest at this stage, are supported by record evidence.

On this record, we find that Petitioner has established a reasonable likelihood that claim 6 is unpatentable over Auradkar, Chiueh, Chambers, and Inoue.

III. CONCLUSION

For the reasons discussed above, we are persuaded that Petitioner has demonstrated a reasonable likelihood of prevailing in establishing that at least one of claims 1–3, 6, 8–17, and 21–27 of the '678 patent is unpatentable.

IV. ORDER

In consideration of the foregoing, it is hereby:

ORDERED that *inter partes* review of the '678 patent is hereby instituted as to claims 1–3, 6, 8–17, and 21–27 on all grounds set forth in the Petition; and

FURTHER ORDERED that pursuant to 35 U.S.C. § 314(c) and 37 C.F.R. § 42.4, notice is hereby given of the institution of a trial on the grounds of unpatentability authorized above; the trial commences on the entry date of this decision.

IPR2023-00458
Patent 9,280,678 B2

For PETITIONER:

Thomas Millikan
Babak Tehranchi
Kristen Schunter
PERKINS COIE LLP
millikan-ptab@perkinscoie.com
tehranchi-ptab@perkinscoie.com
schunter-ptab@perkinscoie.com

For PATENT OWNER:

James Glass
John McKee
Quincy Lu
Andrew Holmes
Ognjen Zivojnovic
QUINN EMANUEL URQUHART & SULLIVAN LLP
jimglass@quinnemanuel.com
johnmckee@quinnemanuel.com
quincylu@quinnemanuel.com
drewholmes@quinnemanuel.com
ogizivojnovic@quinnemanuel.com