US005479512A

United States Patent [19]

Weiss

[11] **Patent Number: 5,479,512**

[45] **Date of Patent: Dec. 26, 1995**

[54] **METHOD AND APPARATUS FOR PERFORMING CONCRYPTION**

[75] Inventor: **Kenneth P. Weiss**, Newton, Mass.

[73] Assignee: **Security Dynamics Technologies, Inc.**, Cambridge, Mass.

[21] Appl. No.: **234,213**

[22] Filed: **Apr. 28, 1994**

Related U.S. Application Data

[63] Continuation-in-part of Ser. No. 213,951, Mar. 16, 1994, and Ser. No. 67,517, May 25, 1993, which is a continuation-in-part of Ser. No. 923,085, Jul. 31, 1992, Pat. No. 5,367,572, and Ser. No. 712,186, Jun. 7, 1991, Pat. No. 5,237,614.

[51] **Int. Cl.^{6}** **H04L 9/28**; H04L 9/00

[52] **U.S. Cl.** **380/28**; 380/9; 380/23; 380/25; 380/49; 235/380

[58] **Field of Search** 380/4, 9, 21, 28, 380/43, 44, 46, 49, 50, 59, 30, 23, 25, 54; 235/380

[56] **References Cited**

U.S. PATENT DOCUMENTS

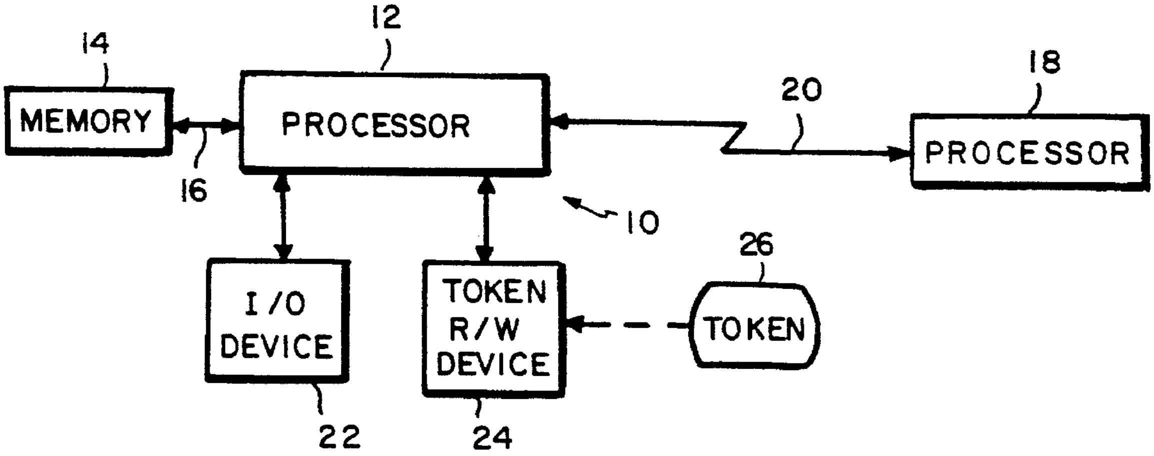
4,386,416	5/1983	Giltner et al.	380/49 X
4,454,575	6/1984	Bushan et al.	380/49 X
4,788,543	11/1988	Rubin	380/50 X
4,893,339	1/1990	Bright et al.	380/28
5,150,410	9/1992	Bertrand	380/28
5,153,918	10/1992	Tuai	380/25
5,285,497	2/1994	Thatcher, Jr.	380/49
5,315,655	5/1994	Chaplin	380/4
5,321,749	6/1994	Virga	380/54 X

Primary Examiner—Bernarr E. Gregory
Attorney, Agent, or Firm—Wolf, Greenfield & Sacks

[57] **ABSTRACT**

A method and apparatus for the integrated compression and encryption (concryption) of clear data and for the deconcryption of concrypted data to obtain the clear data for utilization. For concryption, the clear data and an encryption key are obtained, at least one compression step is performed and at least one encryption step is performed utilizing the encryption key. The encryption step is preferably performed on the final or intermediate results of a compression step, with compression being a multistep operation. For deconcryption, decompression and deencryption steps are performed on concrypted data in essentially the reverse order for the performance of corresponding compression and encryption steps during the concryption operation.

29 Claims, 3 Drawing Sheets



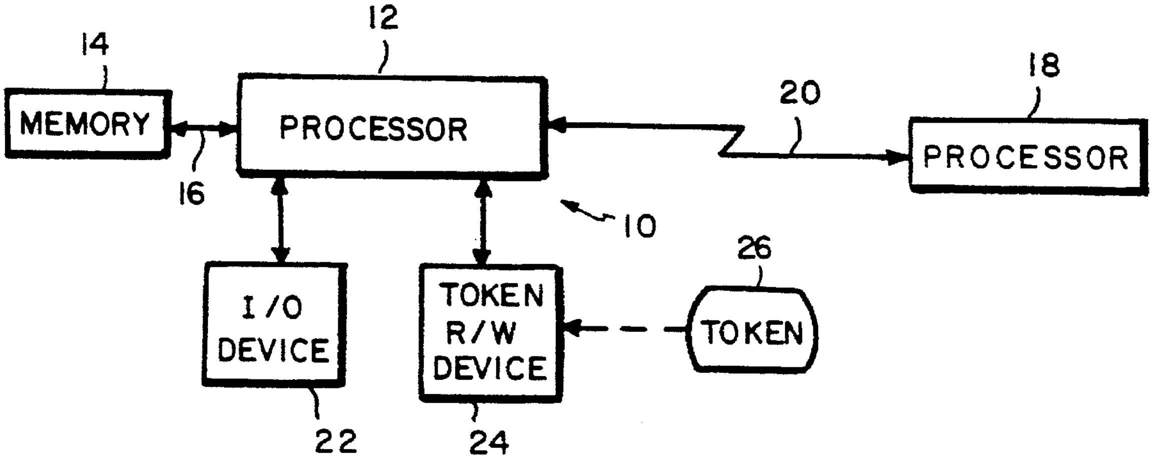


FIG. 1

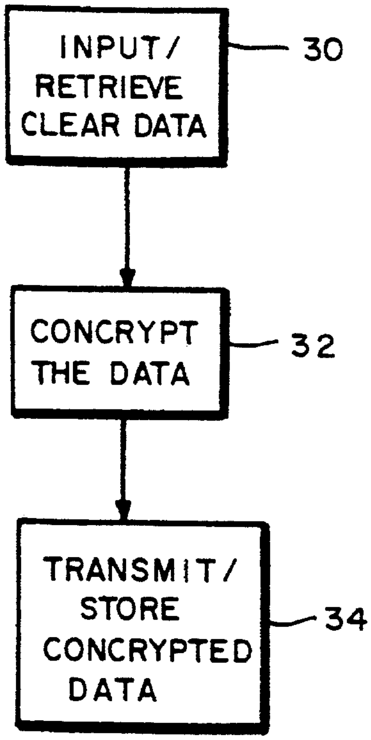


FIG. 2A

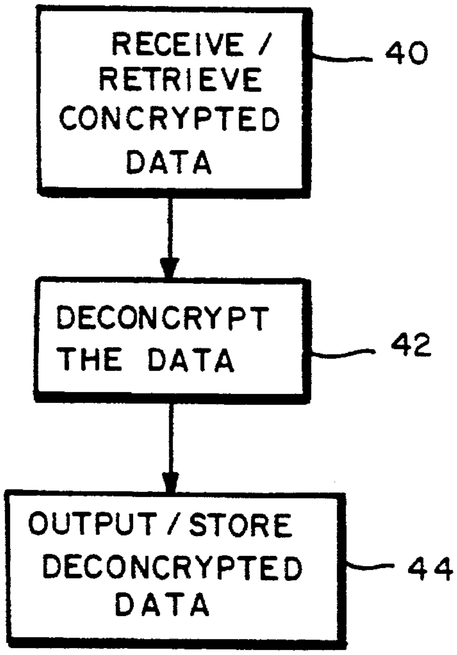

RECEIVE / RETRIEVE CONCRYPTED DATA
40
DECONCRYPT THE DATA
42
OUTPUT / STORE DECONCRYPTED DATA
44

FIG. 2B

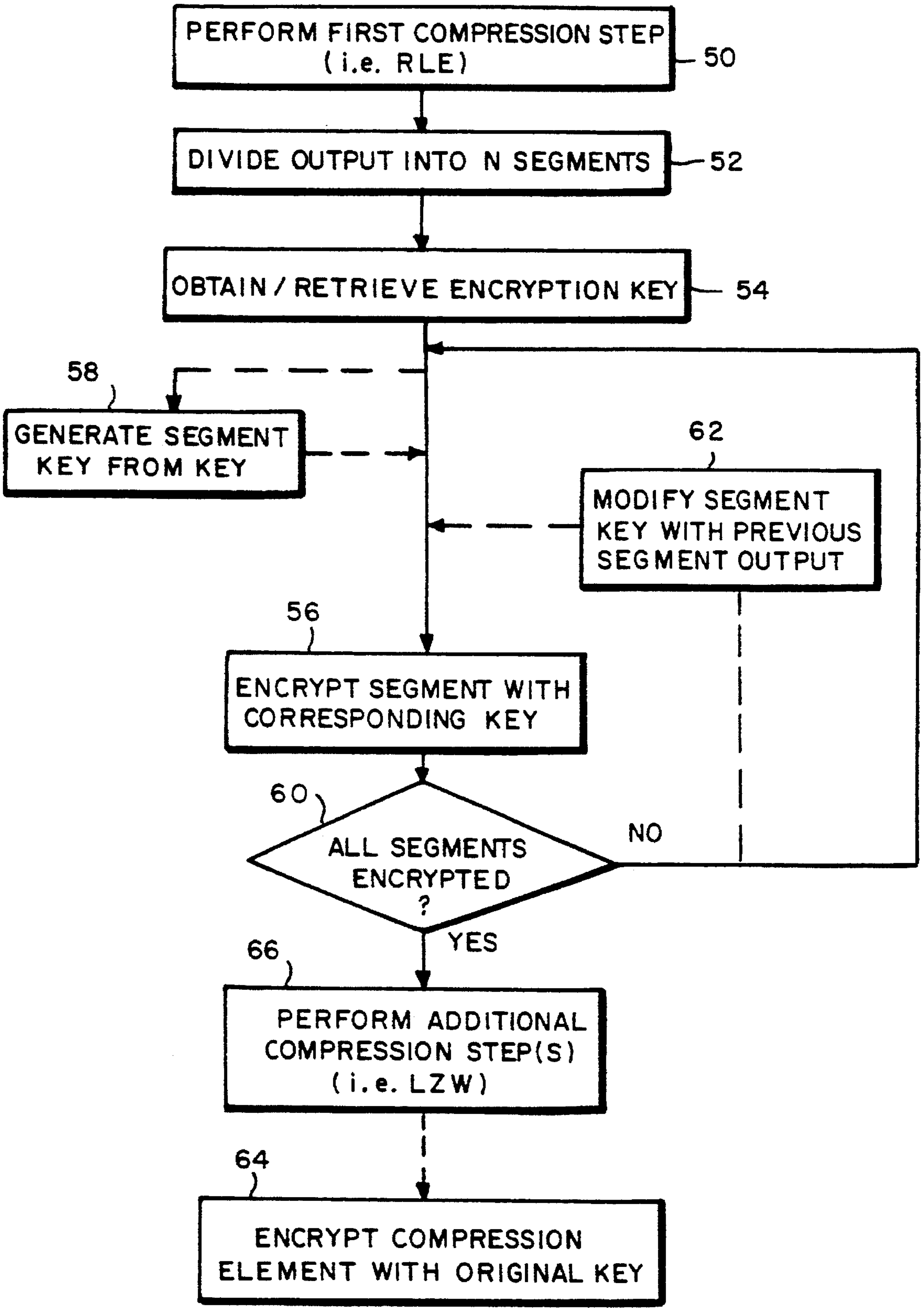

PERFORM FIRST COMPRESSION STEP (i.e. RLE)
50
DIVIDE OUTPUT INTO N SEGMENTS
52
OBTAIN / RETRIEVE ENCRYPTION KEY
54
58
GENERATE SEGMENT KEY FROM KEY
62
MODIFY SEGMENT KEY WITH PREVIOUS SEGMENT OUTPUT
56
ENCRYPT SEGMENT WITH CORRESPONDING KEY
60
ALL SEGMENTS ENCRYPTED ?
NO
YES
66
PERFORM ADDITIONAL COMPRESSION STEP(S) (i.e. LZW)
64
ENCRYPT COMPRESSION ELEMENT WITH ORIGINAL KEY

FIG. 3A

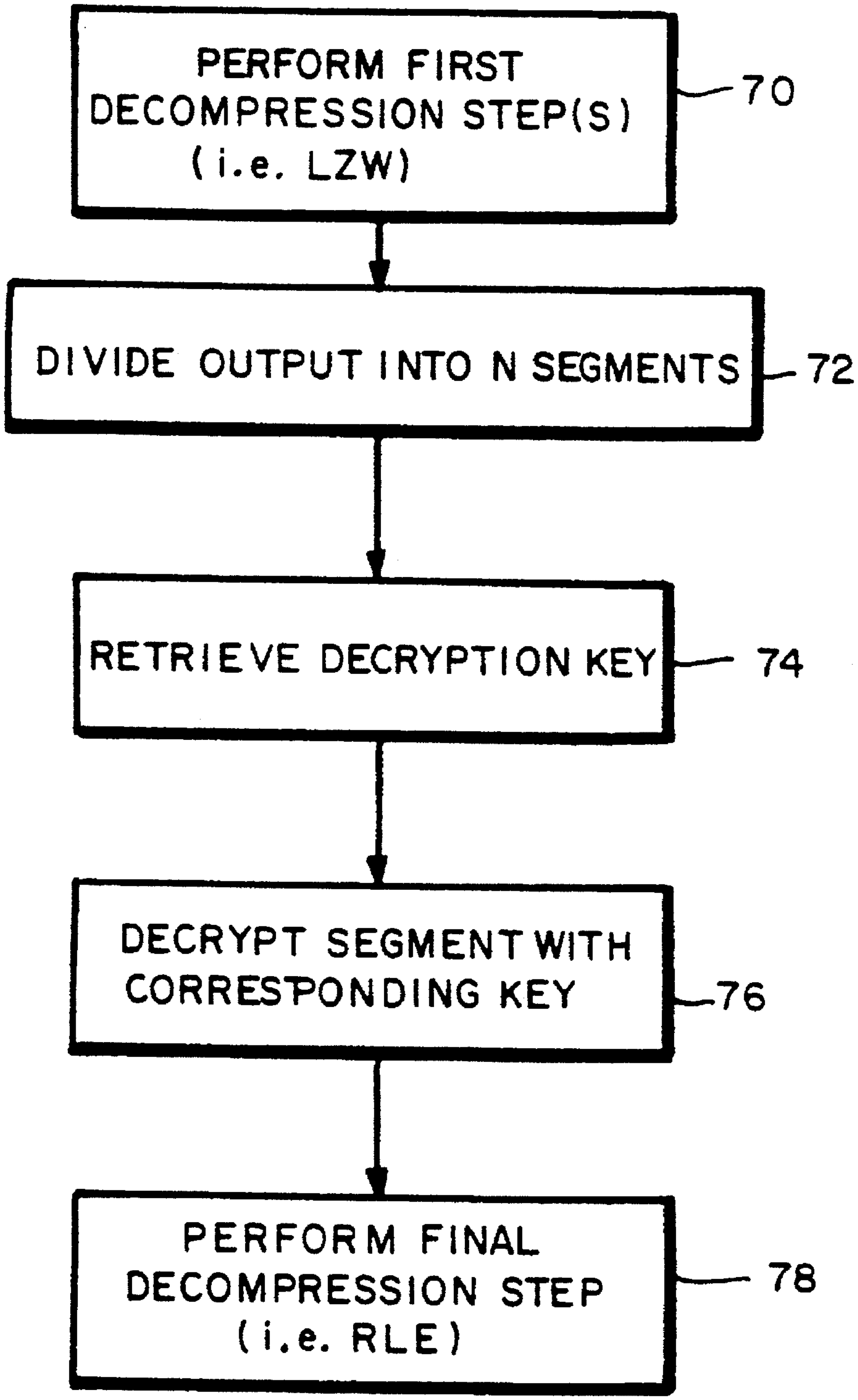

PERFORM FIRST DECOMPRESSION STEP(S) (i.e. LZW)
70
DIVIDE OUTPUT INTO N SEGMENTS
72
RETRIEVE DECRYPTION KEY
74
DECRYPT SEGMENT WITH CORRESPONDING KEY
76
PERFORM FINAL DECOMPRESSION STEP (i.e. RLE)
78

FIG.3B

METHOD AND APPARATUS FOR PERFORMING CONCRYPTION

RELATED APPLICATIONS

This application is a continuation-in-part of U.S. patent application Ser. No. 08/067,517, filed May 25, 1993 for ENHANCED SECURITY FOR A SECURE TOKEN CODE (the '517 application), now pending and of U.S. patent application Ser. No. 08/213,951, filed Mar. 16, 1994 for METHOD AND APPARATUS FOR UTILIZING A TOKEN FOR RESOURCE ACCESS (the '951 application). The '517 application is a continuation-in-part of U.S. patent application Ser. No. 07/923,085, filed Jul. 31, 1992 for METHOD AND APPARATUS FOR PERSONAL IDENTIFICATION, now U.S. Pat. No. 5,367,572, and of U.S. patent application Ser. No. 07/712,186, filed Jun. 7, 1991 for INTEGRATED NETWORK SECURITY SYSTEM, now U.S. Pat. No. 5,237,614. The disclosures of these applications are incorporated by reference herein.

FIELD OF THE INVENTION

This invention relates to the processing of data from clear form to a compressed and encrypted form and to the restoring of the data to clear form for utilization.

BACKGROUND OF THE INVENTION

One byproduct of the "information age" is the huge amounts of data which are stored in various storage media and which are transmitted over various transmission media. In order to reduce the amount of storage media required, to reduce the time required to retrieve data and to reduce required transmission times and/or bandwidths, it has been a common practice for some years to use some form of compression on the raw or clear data before it is stored or transmitted. Depending on the nature of the data, the acceptable computation penalty and other factors, compression ratios in excess of two to one can be achieved for relatively simple systems, with far higher compression ratios being available for more sophisticated compression techniques, such as where two or more compression techniques are chained. For example, when text data is to be transmitted, a run-length encoding (RLE) technique may be utilized to eliminate, or reduce the transmission bandwidth for all of the white spaces around the actual text and the actual text may then be further compressed by using a compression algorithm such as Huffman encoding, Lemple-Ziv (LZ) encoding, one of the many variations on LZ encoding such as Lemple-Ziv-Walsh (LZW) or a combination of two or more such compression techniques. When the data is retrieved from memory, or at the receiving end of a transmission, the data may be decompressed for utilization.

Another problem with the huge quantity of data currently available, particularly where the computer systems storing/utilizing the data are networked, is that data may be and frequently is surreptitiously observed or obtained by unauthorized people or organizations. Where the data is stored or transmitted in compressed form, the information obtained by unauthorized accessing of memory or transmission media cannot be utilized in the form obtained; however, compression algorithms which are usually publicly available or specified in advance, do not therefore provide security for the data. Even if compression algorithms were not known, they are not secure since they work on redundancy and the basis used for cryptographic code breaking is the detection and analyzing of redundant information. Therefore, compression alone, regardless of the degree of sophistication, is not much of a challenge to decipher for experienced cryptanalysts.

Therefore, it is desirable that valuable or sensitive information which is to be stored or transmitted be stored or transmitted in encrypted form. However, both encryption and compression are time and computer cycle intensive. Therefore, the independent, sequential performance of compression and encryption as separate operations on clear data before storage or transmission, and the reversing of these processes to permit utilization of the data, places an added burden on the data processing system performing these functions which may significantly increase the response time of the system to service requests and/or require the use of more powerful and therefore more expensive processing equipment. It would therefore be desirable if encryption and compression could be integrated so as to be automatically performed together as a single concryption operation, the term "concryption" being sometimes used hereinafter to refer to the integrated performance of compression and encryption on data, with a performance penalty for the combined operation which is reduced so as to be more comparable to either technology being performed separately than to that involved in performing the two technologies as separate functions.

SUMMARY OF THE INVENTION

In accordance with the teachings of this invention, concryption is performed on clear data by a data processing device as part of a single operation rather than as two separate operations. More specifically, once the data is loaded into the data processing system, the operations of compression and encryption are performed in an integrated fashion as part of a single operation with reduced memory and/or storage access. Since loading data from memory into a computer and restoring the data to storage are time-consuming operations, performing concryption with a reduced memory and/or storage access results in a significant reduction in the performance penalty for performing the two operations without regard to savings which may also be effected as a result of the algorithmic integration of these operations.

More particularly, clear data is received at the processor, for example as the result of being generated by the processor, of a memory readout or of receipt over a transmission line, and a concryption operation is performed on the clear data, which operation includes at least one compression step and air least one encryption step, which steps are automatically performed in a selected sequence. For preferred embodiments, the compression operation is a multistep operation with the encryption being performed on the results of a compression step and/or on an element utilized in performing at least one compression step. The concrypted data may be outputted either by storing this data in a memory/storage media, by transmitting the concrypted data or by utilizing this data in another suitable manner. When the concrypted data is to be deconcrypted to permit use thereof in clear form, deconcrypting is performed utilizing at least one decompression step and at least one deencryption step, which steps are performed automatically in a sequence which is substantially the reverse of the selected sequence in which compression and encryption, respectively, are performed during the concryption operation.

For preferred embodiments, the encryption key is a code derived from a card or other token carried by an authorized user. Techniques for providing enhanced security for a static code or key stored in such token are discussed in some of the parent applications. While enhanced security may be obtained, particularly for transmitted data, if such encryption

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you’re on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm’s cloud-native docket research platform finds what other services can’t. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS

Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS

Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS

Sync your system to PACER to automate legal marketing.

WHAT WILL YOU BUILD? | sales@docketalarm.com | 1-866-77-FASTCASE

fastcase®
Smarter legal research.