(12) PATENT APPLICATION PUBLICATION
(19) INDIA
(22) Date of filing of Application :27/03/2022

(21) Application No.202211017653 A
(43) Publication Date : 08/04/2022

(54) Title of the invention : METHOD AND SYSTEM FOR SELECTIVELY OBFUSCATING SECTIONS WITHIN ELECTRONIC DOCUMENTS

(51) International classification	:G06Q0010100000, G06F0021140000, G06F0021620000, G06F0016930000, G06F0021100000
(86) International Application No Filing Date	:NA :NA
(87) International Publication No	: NA
(61) Patent of Addition to Application Number Filing Date	:NA :NA
(62) Divisional to Application Number Filing Date	:NA :NA

(71)**Name of Applicant :**
1)Coveidentity Tech Private Limited
Address of Applicant :Flat No. 501, Ruby Tower-01, Somdatt Landmark Sector 116, SAS NAGAR PUNJAB, Mohali, Punjab, 140307, INDIA ---------- ----------
Name of Applicant : NA
Address of Applicant : NA
(72)**Name of Inventor :**
1)Sarvpriye Soni
Address of Applicant :Flat No. 501, Ruby Tower-01, Somdatt Landmark Sector 116, SAS NAGAR, PUNJAB, Mohali, Punjab, India, 140307 ---------- ----------
2)Kunal Nandwani
Address of Applicant :2463, Sector 23C, Chandigarh ---------- ----------

(57) Abstract :
A method and system for selectively obfuscation sections of electronic document is disclosed. The method includes identifying one or more sections within the electronic document. The method further includes applying at least one of a plurality of obfuscating rules to each of the one or more sections. The method includes sharing, with a user, a copy of the electronic document and determining at least one attribute associated with the user. The method further includes selectively obfuscating at least one section from the one or more sections within the copy of the electronic document. The method includes providing the user access to the copy of the electronic document in response to selectively obfuscating the at least one section.

No. of Pages : 47 No. of Claims : 21

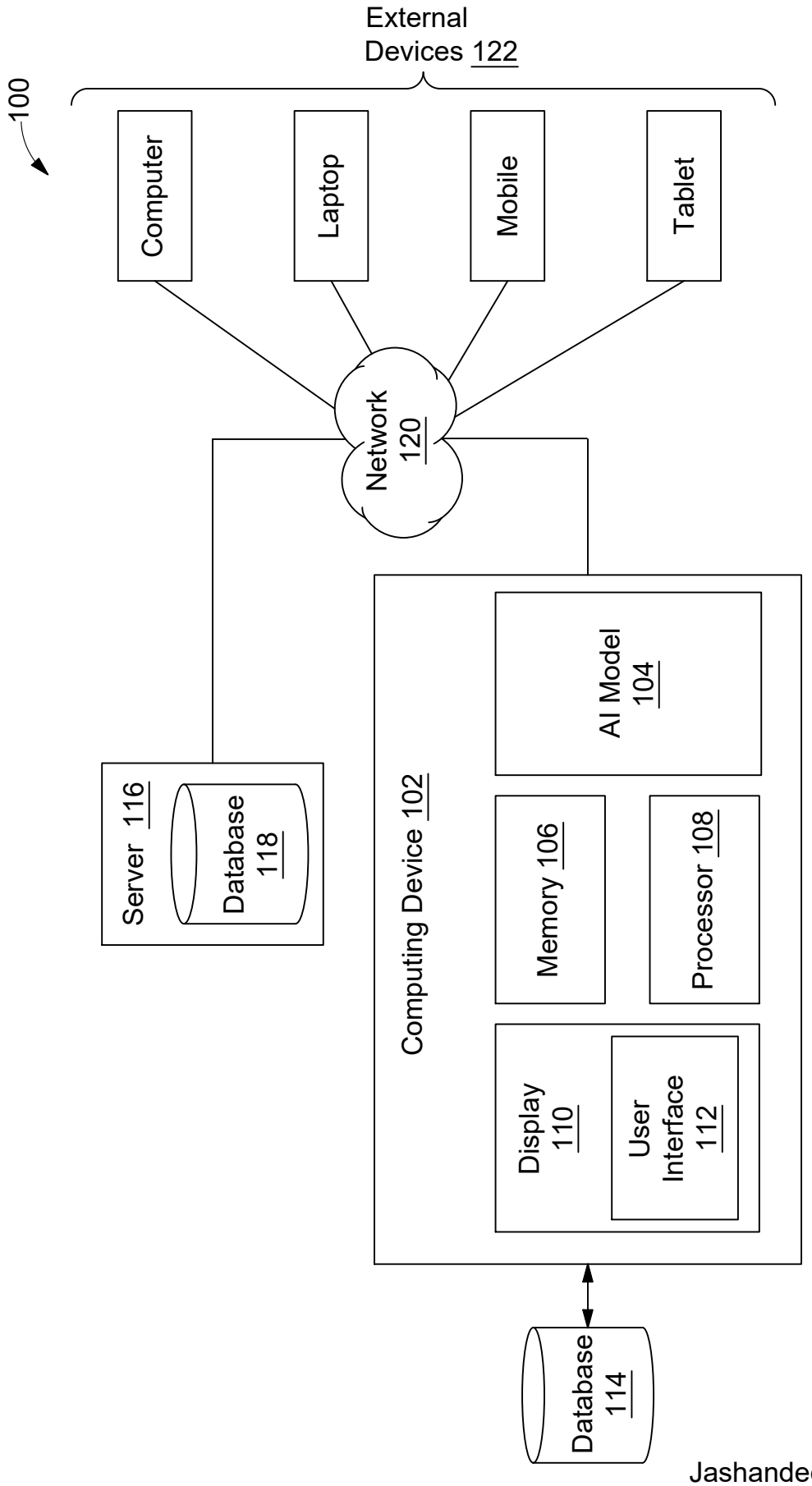

FIG. 1

Jashandeep Singh (INPA No: 2859)
Partner
InventIP Legal Services LLP
4thFloor, 91Springboard
D-107, Sector 2
Noida, Uttar Pradesh - 201301

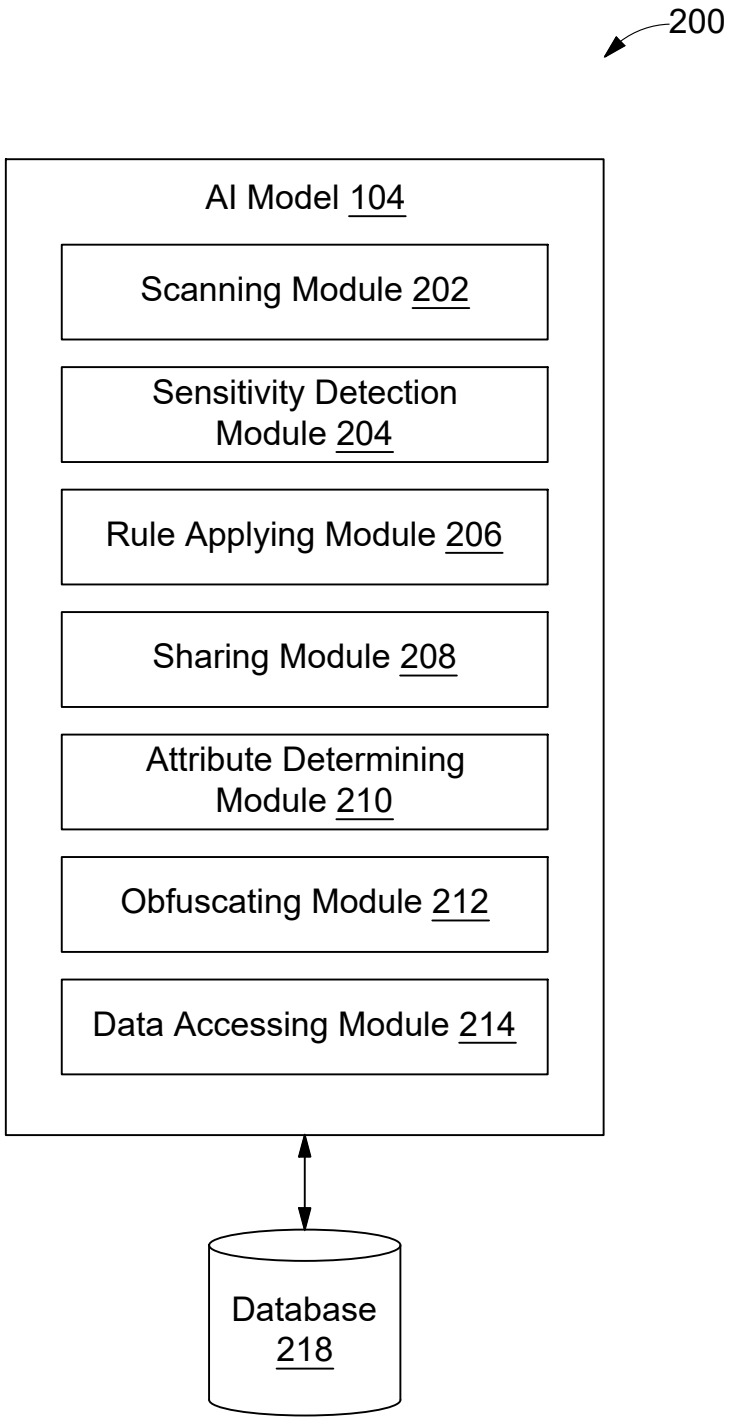

FIG. 2

Jashandeep Singh (INPA No: 2859)
Partner
InventIP Legal Services LLP
4thFloor, 91Springboard
D-107, Sector 2
Noida, Uttar Pradesh - 201301

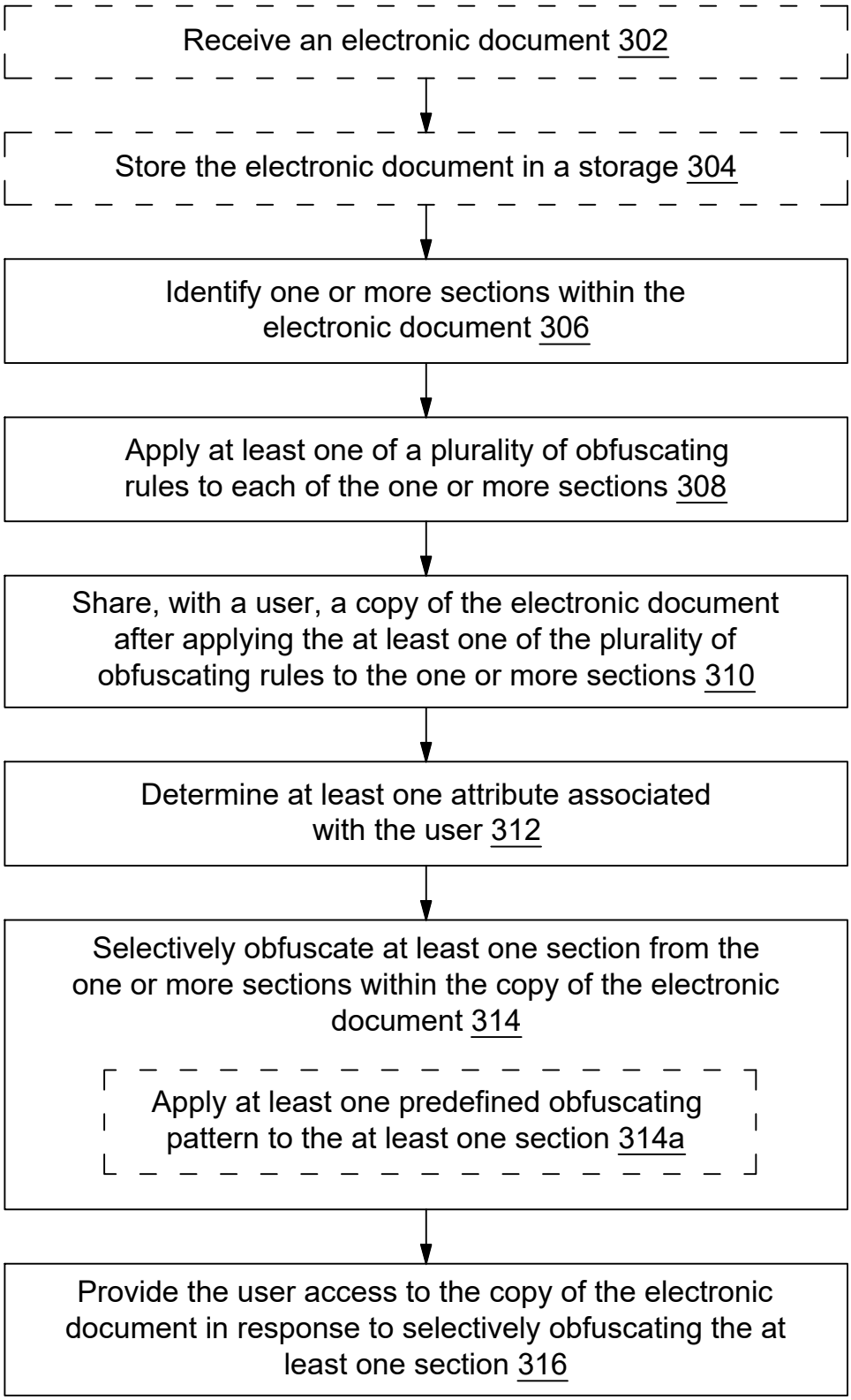

FIG. 3

Jashandeep Singh (INPA No: 2859)
Partner
InventIP Legal Services LLP
4thFloor, 91Springboard
D-107, Sector 2
Noida, Uttar Pradesh - 201301

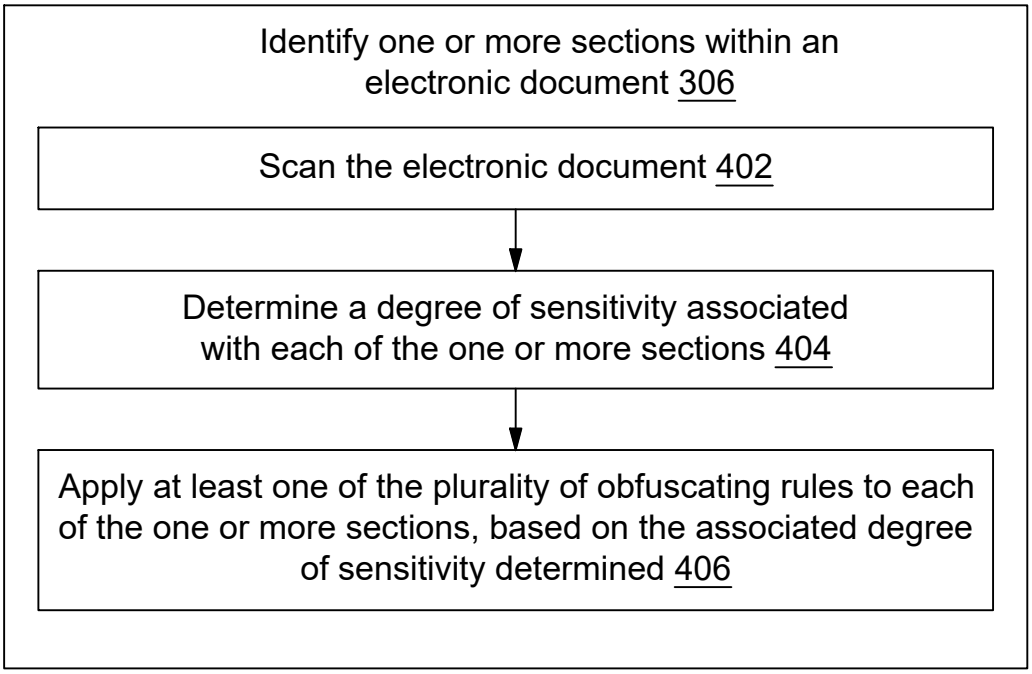

FIG. 4

Jashandeep Singh (INPA No: 2859)
Partner
InventIP Legal Services LLP
4thFloor, 91Springboard
D-107, Sector 2
Noida, Uttar Pradesh - 201301

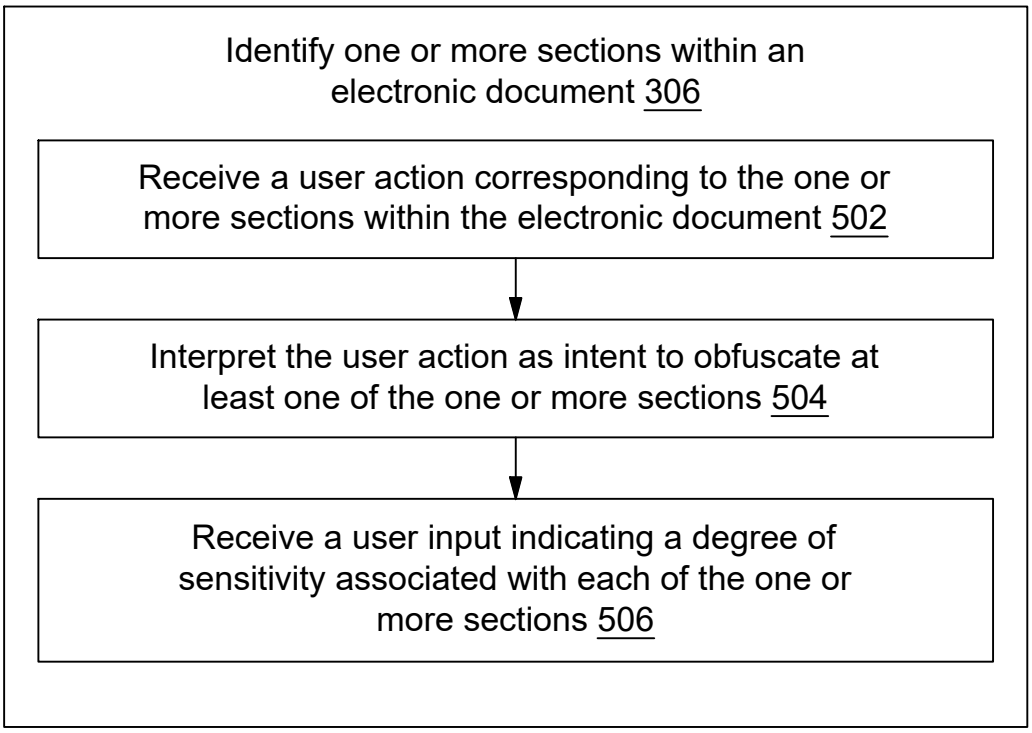

FIG. 5

Jashandeep Singh (INPA No: 2859)
Partner
InventIP Legal Services LLP
4thFloor, 91Springboard
D-107, Sector 2
Noida, Uttar Pradesh - 201301

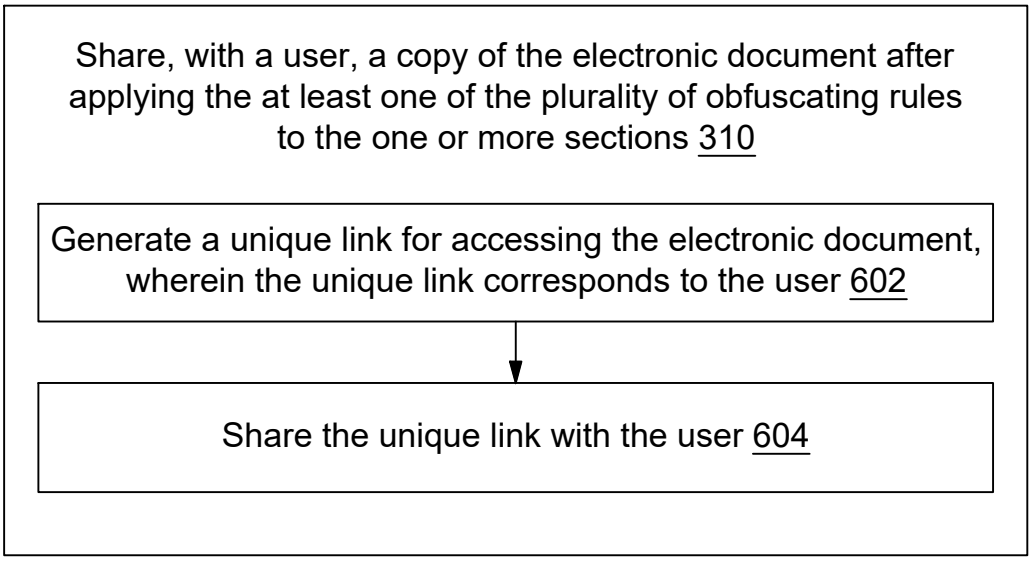

FIG. 6

Jashandeep Singh (INPA No: 2859)
Partner
InventIP Legal Services LLP
4thFloor, 91Springboard
D-107, Sector 2
Noida, Uttar Pradesh - 201301

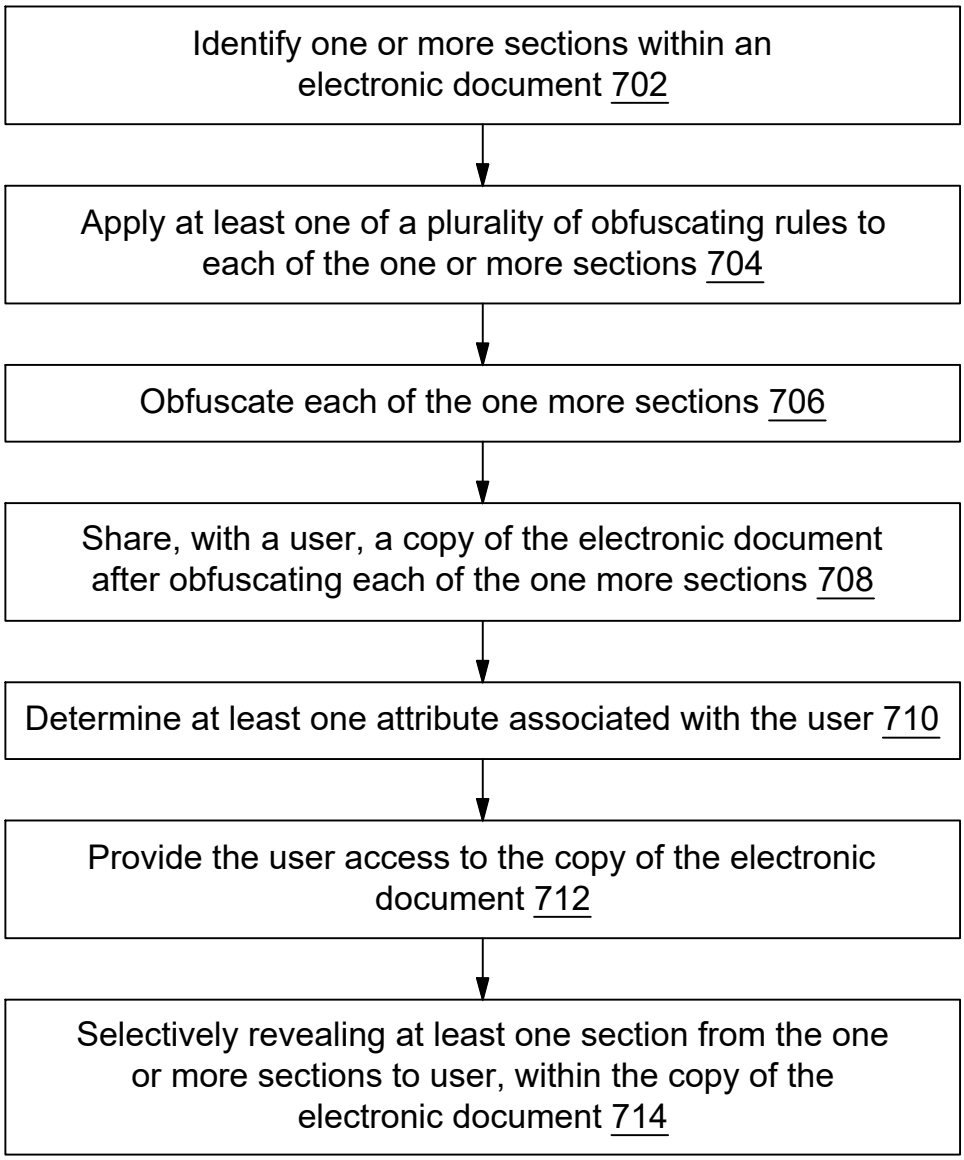

FIG. 7

Jashandeep Singh (INPA No: 2859)
Partner
InventIP Legal Services LLP
4thFloor, 91Springboard
D-107, Sector 2
Noida, Uttar Pradesh - 201301

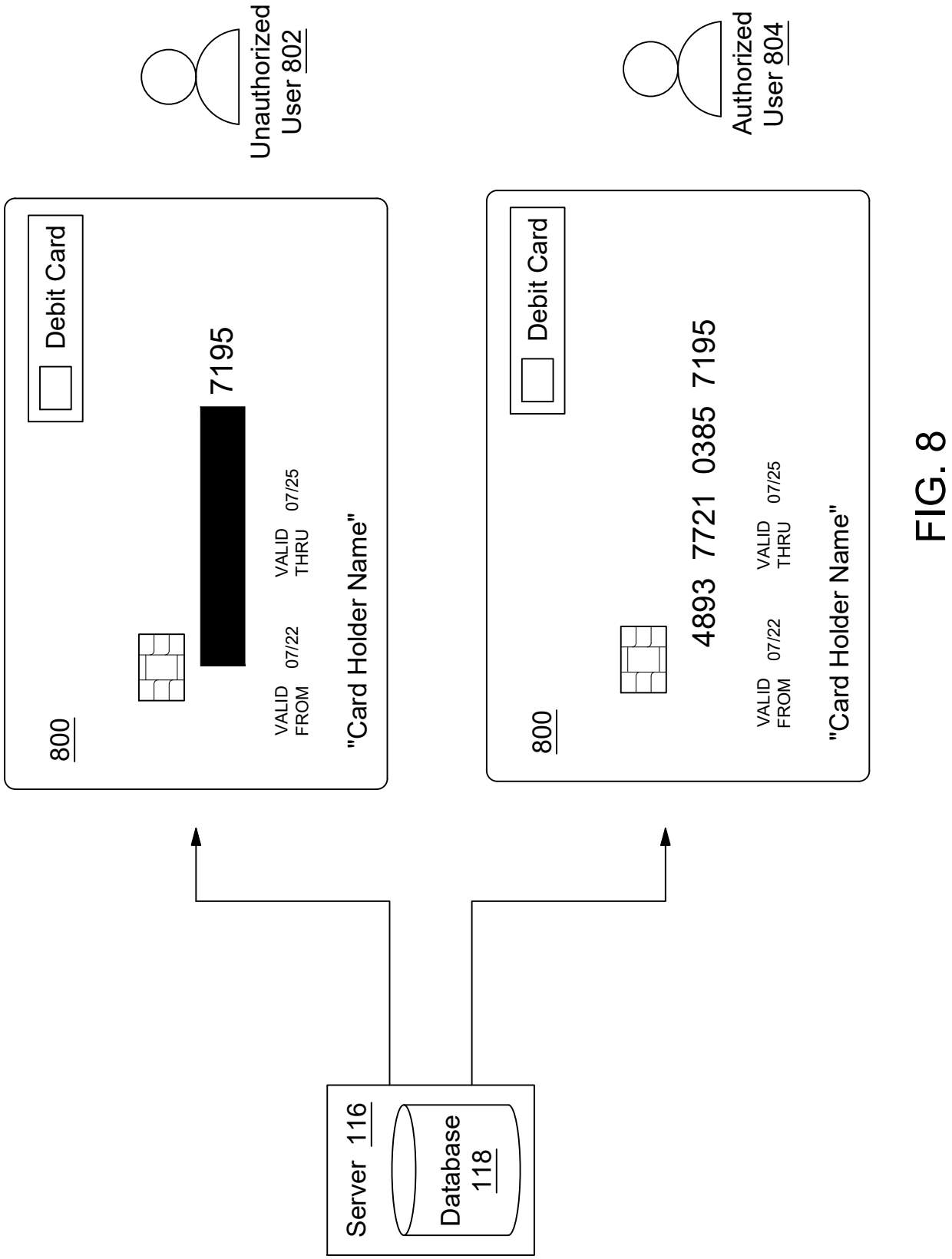

FIG. 8

Jashandeep Singh (INPA No: 2859)
Partner
InventIP Legal Services LLP
4thFloor, 91Springboard
D-107, Sector 2
Noida, Uttar Pradesh - 201301

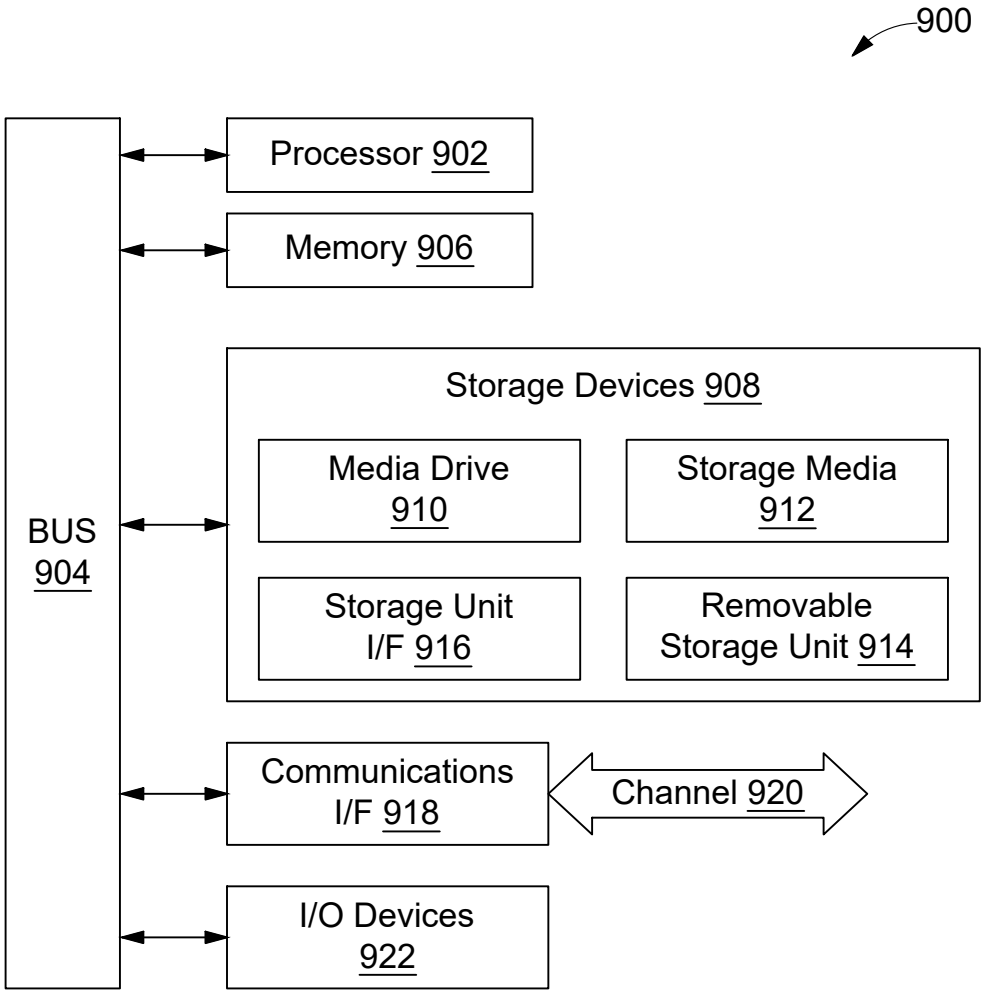

FIG. 9

Jashandeep Singh (INPA No: 2859)
Partner
InventIP Legal Services LLP
4thFloor, 91Springboard
D-107, Sector 2
Noida, Uttar Pradesh - 201301

FORM 2

THE PATENTS ACT, 1970
(39 of 1970)
&
THE PATENTS RULES, 2003

COMPLETE SPECIFICATION
(See section 10, rule 13)

1. TITLE OF THE INVENTION:

METHOD AND SYSTEM FOR SELECTIVELY OBFUSCATING SECTIONS WITHIN ELECTRONIC DOCUMENTS

2. APPLICANT(S)

Name	Nationality	Address of the Applicant
Coveidentity Tech Private Limited	**Indian**	**Flat No. 501, Ruby Tower-01, Somdatt Landmark Sector 116, SAS NAGAR PUNJAB, Mohali, Punjab, 140307, India**

3. PREAMBLE TO THE DESCRIPTION

COMPLETE SPECIFICATION
The following specification particularly describes the invention and the manner in which it is to be performed.

DESCRIPTION

Technical Field

[001] Generally, the invention relates to securing sensitive information present in documents. More specifically, the invention relates to method and system for selectively obfuscating sections within electronic documents.

Background

[002] As a result of advancement in technology, use of online digital services has seen an exponential increase. People have been increasingly using digital services to store and/or share copy of sensitive documents with friends/family and various service providers. However, the increase in use of such digital services has also led to a steep increase in cybercrime, where unauthorized users capture sensitive information from such documents without prior permission. There is therefore a need of tools to ensure that individuals can experience the convenience of digital services without compromising on data privacy.

SUMMARY OF INVENTION

[003] In one embodiment, a method for selectively obfuscation sections of electronic document is disclosed. The method may include receiving an electronic document. The method may further include storing the electronic document in a storage. The method may further include identifying one or more sections within the electronic document. Each of the at least one section may include sensitive information. The method may further include applying at least one of a plurality of obfuscating rules to each of the one or more sections. The method may further include

sharing, with a user, a copy of the electronic document after applying the at least one of the plurality of obfuscating rules to the one or more sections. The method may further include determining at least one attribute associated with the user. The method may further include selectively obfuscating at least one section from the one or more sections within the copy of the electronic document, based on the determined at least one attribute associated with the user and the applied at least one of the plurality of obfuscating rules. The method may further include providing the user access to the copy of the electronic document in response to selectively obfuscating the at least one section.

[004] In another embodiment, a method for selectively obfuscation sections of electronic document is disclosed. The method may include identifying one or more sections within an electronic document. Each of the at least one section includes sensitive information. The method may further include applying at least one of a plurality of obfuscating rules to each of the one or more sections. The method may further include obfuscating each of the one more sections. The method may further include sharing, with a user, a copy of the electronic document after obfuscating each of the one more sections. The method may further include determining at least one attribute associated with the user. The method may further include providing the user access to the copy of the electronic document. The method may further include selectively revealing at least one section from the one or more sections to user, within the copy of the electronic document, based on the determined at least one attribute associated with the user and the applied at least one of the plurality of obfuscating rules.

[005] In another embodiment, a system for selectively obfuscation sections of electronic document is disclosed. The system may include a computing device

comprising a processor and a memory communicatively coupled to the processor. The memory may store processor-executable instructions, which, on execution, may causes the processor to receive an electronic document and further store the electronic document in a storage. The processor-executable instructions, on execution, may further cause the processor to identify one or more sections within an electronic document. Each of the at least one section includes sensitive information. The processor-executable instructions, on execution, may further cause the processor to apply at least one of a plurality of obfuscating rules to each of the one or more sections. The processor-executable instructions, on execution, may further cause the processor to share, with a user, a copy of the electronic document after applying the at least one of the plurality of obfuscating rules to the one or more sections. The processor-executable instructions, on execution, may further cause the processor to determine at least one attribute associated with the user. The processor-executable instructions, on execution, may further cause the processor to selectively obfuscate at least one section from the one or more sections within the copy of the electronic document, based on the determined at least one attribute associated with the user and the applied at least one of the plurality of obfuscating rules. The processor-executable instructions, on execution, may further cause the processor to provide the user access to the copy of the electronic document in response to selectively obfuscating the at least one section.

[006] In another embodiment, a computer program product for selectively obfuscation sections of electronic document is disclosed. In one example, the computer program product is embodied in a non-transitory computer readable storage medium of a computing device and includes computer instructions receiving an electronic document. The computer instructions may further include storing the

electronic document in a storage. The computer instructions may further include identifying one or more sections within the electronic document. Each of the at least one section may include sensitive information. The computer instructions may further include applying at least one of a plurality of obfuscating rules to each of the one or more sections. The computer instructions may further include sharing, with a user, a copy of the electronic document after applying the at least one of the plurality of obfuscating rules to the one or more sections. The computer instructions may further include determining at least one attribute associated with the user. The computer instructions may further include selectively obfuscating at least one section from the one or more sections within the copy of the electronic document, based on the determined at least one attribute associated with the user and the applied at least one of the plurality of obfuscating rules. The computer instructions may further include providing the user access to the copy of the electronic document in response to selectively obfuscating the at least one section.

[007] It is to be understood that both the foregoing general description and the following detailed description are exemplary and explanatory only and are not restrictive of the invention, as claimed.

BRIEF DESCRIPTION OF THE DRAWINGS

[008] The present application can be best understood by reference to the following description taken in conjunction with the accompanying drawing figures, in which like parts may be referred to by like numerals.

[009] **FIG. 1** is a block diagram illustrating a system for selectively obfuscation sections of electronic documents, in accordance with an embodiment.

[010] **FIG. 2** is a block diagram illustrating various modules within an Artificial Intelligence (AI) model of a computing device configured to selectively obfuscate sections of electronic documents, in accordance with an embodiment.

[011] **FIG. 3** illustrates a flowchart of a method for selectively obfuscation sections of electronic document, in accordance with an embodiment.

[012] **FIG. 4** illustrates a flowchart of a method for identifying, via an AI model, one or more sections within electronic document that need to be obfuscated, in accordance with an embodiment.

[013] **FIG. 5** illustrates a flowchart of a method for identifying, by a user, one or more sections within electronic document that need to be obfuscated, in accordance with an embodiment.

[014] **FIG. 6** illustrates a flowchart of a method for sharing a copy of electronic document with user after applying obfuscating rules, in accordance with an embodiment.

[015] **FIG. 7** illustrates a flowchart of a method for selectively revealing obfuscated sections within a copy of an electronic document shared with the user, in accordance with an embodiment.

[016] **FIG. 8** illustrates selective obfuscation of a debit card number within a digital copy of a debit card, in accordance with an exemplary embodiment.

[017] **FIG. 9** is a block diagram of an exemplary computer system for implementing embodiments consistent with the present disclosure.

DETAILED DESCRIPTION OF THE DRAWINGS

[018] The following description is presented to enable a person of ordinary skill in the art to make and use the invention and is provided in the context of particular applications and their requirements. Various modifications to the embodiments will be readily apparent to those skilled in the art, and the generic principles defined herein may be applied to other embodiments and applications without departing from the spirit and scope of the invention. Moreover, in the following description, numerous details are set forth for the purpose of explanation. However, one of ordinary skill in the art will realize that the invention might be practiced without the use of these specific details. In other instances, well-known structures and devices are shown in block diagram form in order not to obscure the description of the invention with unnecessary detail. Thus, the invention is not intended to be limited to the embodiments shown but is to be accorded the widest scope consistent with the principles and features disclosed herein.

[019] While the invention is described in terms of particular examples and illustrative figures, those of ordinary skill in the art will recognize that the invention is not limited to the examples or figures described. Those skilled in the art will recognize that the operations of the various embodiments may be implemented using hardware, software, firmware, or combinations thereof, as appropriate. For example, some processes can be carried out using processors or other digital circuitry under the control of software, firmware, or hard-wired logic. (The term “logic” herein refers to fixed hardware, programmable logic and/or an appropriate combination thereof, as would be recognized by one skilled in the art to carry out the recited functions.) Software and firmware can be stored on computer-readable storage media. Some other processes can be implemented using analog circuitry, as is well known to one of

ordinary skill in the art. Additionally, memory or other storage, as well as communication components, may be employed in embodiments of the invention.

[020] Referring now to FIG. 1, a block diagram of a system 100 for selectively obfuscation sections of electronic documents is illustrated, in accordance with an embodiment. The system 100 may include a computing device 102 that may be responsible for selectively obfuscation sections of electronic documents. Examples of the computing device 102 may include, but are not limited to, a server, a desktop, a laptop, a notebook, a tablet, a smartphone, a mobile phone, an application server, or the like. Obfuscating, for example, may include, but is not limited to blurring, overlaying predefined image, overlaying predefined characters or alphabets, or colored redactions. In an embodiment, the electronic documents may be physical documents that are available in digital form. Examples of the electronic documents may include, but are not limited to digital copy of passports, national Identity (ID) cards, driving licence, academic records, credit cards, or debit cards.

[021] The computing device 102 may include an Artificial Intelligence (AI) model 104, which may further include various modules that enable the computing device 102 to selectively obfuscate sections of the electronic document. These modules are explained in detail in conjunction with FIG. 2. In order to selectively obfuscate sections of an electronic document, the computing device 102 may be configured to receive the electronic document. Once the electronic document is received, the computing device 102 may store the electronic document in a storage. The storage may be at least one of an online storage (for example, a server 116) or a device storage (for example, a memory 106). Upon storing the electronic document in the storage, the computing device 102 may identify one or more sections within the electronic document, such that, each of the one or more sections include sensitive

information. Methods of identifying one or more sections within the electronic document has been explained in greater detail in conjunction with FIG. 4 and FIG. 5.

[022] Once the one or more sections within the electronic document are identified, the computing device 102 may apply at least one of a plurality of obfuscating rules to each of the one or more sections. Thereafter, a copy of the electronic document may be shared with a user. Further, the computing device 102 may determine at least one attribute associated with the user. Based on the determined at least one attribute associated with the user and the applied at least one of the plurality of obfuscating rules, the computing device 102 may selectively obfuscate at least one section from the one or more sections within the copy of the electronic document.

[023] The computing device 102 may then provide the user access to the copy of the electronic document, in response to selectively obfuscating the at least one section. In some embodiments, each section of the copy of the electronic document is obfuscated when shared with a user. In this case, when the user accesses the copy of the electronic document, the at least one section from the one or more sections may be selectively revealed to user, based on the determined at least one attribute associated with the user and the applied at least one of the plurality of obfuscating rules. The complete process followed by the system 100 is further explained in detail in conjunction with FIG. 2 to FIG. 7.

[024] The computing device 102 may further include the memory 106, a processor 108, and a display 110. The display 110 may include a user interface 112. The end-user may interact with the computing device 102 and vice versa through the display 110 and the user interface 112. By way of an example, the display 110 may be used to display results (i.e., partial obfuscated section from the one or more sections within the copy of electronic documents, complete obfuscated section from

the one or more sections within the copy of electronic documents, the at least one predefined obfuscating pattern within the copy of electronic documents, etc.,) based on actions performed by the computing device 102, to an end-user (i.e., bank agents, students, office staffs, employees, telecom executives, etc.,). In a similar manner, the display 110 may be used to display the at least one revealed section from the one or more sections to user, within the copy of the electronic document. The user access to at least one revealed section may change based on the determined at least one attribute associated with the user and the applied at least one of the plurality of obfuscating rules.

[025] By way of another example, the user interface 112 may be used by the user to provide inputs to the computing device 102. Thus, for example, in some embodiments, the user may ingest an input via the user interface 112 of the computing device 102. The input may include a user action linked to one or more sections within the electronic document. The computing device 102 may interpret the user action as intent to obfuscate the one or more sections, apply at least one predefined obfuscating pattern to the at least one section, and share the copy of the electronic document with the end-user via the user interface 112.

[026] The memory 106 may store instructions that, when executed by the processor 108, may cause the processor 108 to selectively obfuscate or reveal sections of the electronic document. As will be described in greater detail in conjunction with FIG. 2 to FIG. 7, in order to selectively obfuscate or reveal sections of the electronic document, the processor 108 in conjunction with the memory 106 may perform various functions including identification of one or more sections within an electronic document, applying at least one of the plurality of obfuscating rules to at least one of the one or more sections, sharing a copy of the electronic document with

a user, determining of at least one attribute associated with the user, selectively obfuscating the at least one section, and providing the user access to the copy of the electronic document.

[027] The memory 106 may also store various data (e.g., the electronic document, sensitive information associated with the electronic document, data related to a degree of sensitivity associated with each of the one or more sections, the at least one attribute associated with the user, etc.) that may be captured, processed, and/or required by the computing device 102. The memory 106 may be a non-volatile memory (e.g., flash memory, Read Only Memory (ROM), Programmable ROM (PROM), Erasable PROM (EPROM), Electrically EPROM (EEPROM) memory, etc.) or a volatile memory (e.g., Dynamic Random-Access Memory (DRAM), Static Random-Access memory (SRAM), etc.).

[028] Further, a database 114 may be connected to the computing device 102 and may be used to store the electronic document, the sensitive information associated with the electronic document, data related to the degree of sensitivity associated with each of the one or more sections, and/or the at least one attribute associated with the user. Additionally, the database 114 may be periodically updated based on the at least one attribute associated with the user and the at least one of the plurality of obfuscating rules.

[029] The computing device 102 may also interact with the server 116 or external devices 122 over a network 120 for sending and receiving data. The external devices 122 may be used by the plurality of end users to access the copy of the electronic document received from the computing device 102. Examples of the external devices 122 may include, but are not limited to, computer, tablet, smartphone, and laptop. The network 120, for example, may be any wired or wireless

communication network and the examples may include, but may be not limited to, the Internet, Wireless Local Area Network (WLAN), Wi-Fi, Long Term Evolution (LTE), Worldwide Interoperability for Microwave Access (WiMAX), and General Packet Radio Service (GPRS).

[030] In some embodiment, the computing device 102 may fetch one or more set of data associated with the electronic document from the server 116. In addition, the server 116 may provide user access to the copy of the electronic document. The server 116 may further include a database 118. The database 118 may store information associated with the electronic document and the at least one attribute associated with the user. By way of an example, the database 118 may store the sensitive information associated with each of the at least one section of the electronic document and the at least one attribute associated with the user in order to selectively obfuscate at least one section from the one or more sections. The database 118 may be periodically updated with new information available for selectively obfuscating the at least one section.

[031] Referring now to FIG. 2, a block diagram 200 of various modules within the AI model 104 of the computing device 102 that is configured to selectively obfuscate sections of electronic documents is illustrated, in accordance with an embodiment. Once the electronic document is received by the computing device 102, the AI model 104 may identify one or more sections within the received electronic document. The at least one section may include sensitive information. In order to identify one or more sections, the AI model 104 may include a scanning module 204 and a sensitivity detection module 206. The scanning module 204 may scan the electronic document to identify one or more sections that include sensitive information.

It may be noted that the AI model 104 may be trained to identify the sensitive information in a plurality of types of electronic documents.

[032] Further, the sensitivity detection module 206 may be configured to determine a degree of sensitivity associated with each of the one or more sections. In some embodiments, to identify one or more sections within the received electronic document, a user action corresponding to the one or more sections within the electronic document may be received. The user action may include a user input indicating a degree of sensitivity associated with each of the one or more sections. Based on the received user action, it may be interpreted that the user action is an intent to obfuscate at least one of the one or more sections.

[033] The AI model 104 may further include a rule applying module 206. Once the one or more sections within an electronic document are identified, the rule applying module 206 may apply at least one of a plurality of obfuscating rules to each of the one or more sections based on the associated degree of sensitivity. In one embodiment, the plurality of obfuscating rules may include partial obfuscation of a section from the one or more sections. In another embodiment, the plurality of obfuscating rules may include complete obfuscation of a section from the one or more sections.

[034] The AI model 104 may further include a sharing module 208 that may be configured to share a copy of the electronic document with a user, after applying the at least one of the plurality of obfuscating rules to the one or more sections. In an embodiment, for sharing the copy of the electronic document with the user, the sharing module 208 may generate a unique link for accessing the electronic document. It may be noted that the unique link may be unique to the user. Once the unique link is generated, the sharing module 208 may further share the unique link with the user.

[035] The AI model 104 may further include an attribute determining module 210. The attribute determining module 210 may determine at least one attribute associated with the user. In an embodiment, the at least one attribute associated with the user may include, but is not limited to at least one of: a current location of the user, a role associated with the user, access rights granted to the user, relation of the user with an entity sharing the copy of the electronic document, current day and time, device being used by the user to access the copy of the electronic document, a network ID associated with the internet connection being used by the user, or other bibliographic data associated with the user. The determined attribute associated with the user may be stored in a database 218.

[036] The AI model 104 may further include an obfuscating module 212. Based on the determined at least one attribute associated with the user and the applied at least one of the plurality of obfuscating rules, the obfuscating module 212 may selectively obfuscate at least one section from the one or more sections within the copy of the electronic document. In some embodiments, for selectively obfuscating the at least one section, the obfuscating module 212 may apply at least one predefined obfuscating pattern to the at least one section. The at least one predefined obfuscating pattern may include at least one of, but is not limited to blurring, predefined image, predefined characters or alphabets, or colored redactions. In some embodiments, when all the sections within the copy of the electronic document are obfuscated, the obfuscating module 212 may selectively reveal at least one section from the one or more sections to the user, based on the determined at least one attribute associated with the user.

[037] The AI model 104 may further include a data accessing module 214 that is configured to provide the user access to the copy of the electronic document in

response to selectively obfuscating the at least one section. In some embodiments, the user access to the copy of the electronic document may be provided based on the determined at least one attribute associated with the user and the applied at least one of the plurality of obfuscating rules. This is further explained in conjunction with FIG. 7.

[038] It should be noted that all such aforementioned modules 202 – 214 may be represented as a single module or a combination of different modules. Further, as will be appreciated by those skilled in the art, each of the modules 202 – 214 may reside, in whole or in parts, on one device or multiple devices in communication with each other. In some embodiments, each of the modules 202 – 214 may be implemented as dedicated hardware circuit comprising custom application-specific integrated circuit (ASIC) or gate arrays, off-the-shelf semiconductors such as logic chips, transistors, or other discrete components. Each of the modules 202 – 214 may also be implemented in a programmable hardware device such as a field programmable gate array (FPGA), programmable array logic, programmable logic device, and so forth. Alternatively, each of the modules 202 – 214 may be implemented in software for execution by various types of processors (e.g., processor 108). An identified module of executable code may, for instance, include one or more physical or logical blocks of computer instructions, which may, for instance, be organized as an object, procedure, function, or other construct. Nevertheless, the executables of an identified module or component need not be physically located together but may include disparate instructions stored in different locations which, when joined logically together, include the module, and achieve the stated purpose of the module. Indeed, a module of executable code could be a single instruction, or many instructions, and

may even be distributed over several different code segments, among different applications, and across several memory devices.

[039] As will be appreciated by one skilled in the art, a variety of processes may be employed for selectively obfuscation sections of electronic document. For example, the system 100 and the associated computing device 102 may selectively obfuscate sections of electronic document by the processes discussed herein. In particular, as will be appreciated by those of ordinary skill in the art, control logic and/or automated routines for performing the techniques and steps described herein may be implemented by the system 100 and the associated computing device 102 either by hardware, software, or combinations of hardware and software. For example, suitable code may be accessed and executed by the one or more processors on the system 100 to perform some or all of the techniques described herein. Similarly, application specific integrated circuits (ASICs) configured to perform some, or all of the processes described herein may be included in the one or more processors on the system 100.

[040] Referring now to FIG. 3, a flowchart of a method for selectively obfuscation sections of electronic documents is illustrated, in accordance with an embodiment. At step 302, an electronic document may be received. In an embodiment, the electronic document may be received by uploading the electronic document digitally to the computing device 104. Once the electronic document is received, at step 304, the electronic document may be stored in a storage. The storage may be at least one of an online storage (for example, the server 116) or a device storage (for example, the memory 106). In an alternate configuration, the computing device 102 may have an application that may be configured to selectively obfuscate one or more sections within electronic documents being shared by a user. At an initial step, an application may be opened, and a document of user’s choice may be uploaded. The

document may be uploaded from the online storage, the device storage, or through a scanner (which may be an in-built camera or an external scanner that is communicatively coupled). In case the document is already scanned by the application or already uploaded in the application, the document may be simply clicked on to select for sharing.

[041] At step 306, one or more sections may be identified within the electronic document. In an embodiment, each of the one or more sections may include sensitive information. The method of identifying one or more sections within an electronic document is explained in detail in conjunction with FIG. 5.

[042] Once the one or more sections within an electronic document are identified, at step 308, at least one of a plurality of obfuscating rules may be applied to each of the one or more sections. The plurality of obfuscating rules may include one or more of partial obfuscation of a section from the one or more sections, or complete obfuscation of a section from the one or more sections.

[043] At step 310, a copy of the electronic document may be shared with a user after applying at least one of the plurality of obfuscating rules to the one or more sections. The method of sharing the copy of the electronic document with the user is explained in conjunction with FIG. 6. Once the copy of the electronic document is shared with the user, at step 312, at least one attribute associated with the user may be determined. The at least one attribute associated with the user may include, but are not limited to at least one of a current location of the user, a role associated with the user, access rights granted to the user, relation of the user with an entity sharing the copy of the electronic document, current day and time, device being used by the user to access the copy of the electronic document, a network ID associated with the

internet connection being used by the user, or other bibliographic data associated with the user.

[044] Based on the determined at least one attribute associated with the user and the applied at least one of the plurality of obfuscating rules, at step 314, at least one section from the one or more sections may be selectively obfuscated within the copy of electronic document. The step 314 further includes a step 314a, where in order to selectively obfuscate the at least one section, at least one predefined obfuscating pattern may be applied to each of the at least one section. In an embodiment, the at least one predefined obfuscating pattern may include, but are not limited to at least one of blurring, predefined image, predefined characters or alphabets, colored redactions. In an embodiment, a different obfuscating pattern may be applied on each of the at least one section. In other words, it's not required to apply the same obfuscating patterns on each section. Moreover, the obfuscating patterns may also vary based on degree of sensitivity associated with a given section.

[045] In an alternate embodiment, a user may open the document on the computing device 102 and may subsequently select sections that are required to blurred. To this end, the user may drag a cursor over the section that is required be blurred and the section may accordingly get blurred. The user may repeat this till all the sections that are intended to be blurred have been covered. After selectively obfuscating the at least one section, at step 316, the user may be provided access to the copy of the electronic document. This is further explained in detail in conjunction with FIG. 6.

[046] The computing device 102 may enable individuals and entities to automatically (or manually in some embodiments) select sections of a document that should be revealed to a third party and other sections of the document that should be

blurred (or obfuscated/hidden) from the third party. Thus, the disclosed system and method is beneficial for both parties since they get the required inputs, and at the same time unnecessary details within the document are not shared with the third party. Moreover, since the original document is not altered, different such iterations with multiple users may be executed without any hassle. Additionally, after the document has been shared with the third party, the document owner at a later point in time may decide to blur certain unblurred sections or unblur some blurred sections. The computing device 102 and the system 100 may enable the document owner to remotely control such actions.

[047] Therefore, the document owner remains in absolute control of what is revealed to a third-party recipient at any point in time. By way of an example, when the document owner later decides to unblur one or more blurred sections, the document owner may access an admin portal to view who all have access to the document. From the admin portal, the document owner may have the option to unblur or revoke access for each individual receiver. It may be noted that in case any information on the electronic document needs to be blurred or unblurred after sending, the owner of the electronic document has controls to do so. The method and system also provide a holistic solution for access management in organizations, so that different sets of employees in the organization hierarchy may get different levels of control over data.

[048] Moreover, the obfuscating rules applied on the document before sharing it make sure that certain sections of the document are automatically blurred or unblurred based on change in attributes associate with the third party at any given point in time. By way of an example, certain sections within a document may be unblurred or blurred for a specific time of day. Moreover, geo-fencing may also be

used such that sensitive information is unblurred only in particular locations and that too for specific people only. For example, employees may only see company sensitive information within documents when they are inside the office premises. However, the company sensitive information may be blurred when these documents are opened elsewhere.

[049] Referring now to FIG. 4, a flowchart of a method for identifying, via the AI model 104, one or more sections that need to be obfuscated within an electronic document is illustrated, in accordance with an embodiment. With reference to step 306 in FIG. 3, in order to identify one or more sections within the electronic document, the electronic document may be scanned at step 402. In some embodiments, the electronic document may be scanned through the AI model 104. The AI model 104 may be trained to identify sensitive information in a plurality of types of electronic documents. Examples of various types of electronic documents may include, but are not limited to passports, driving license, Aadhar card, Credit/Debit cards, contracts, licensing agreements, invoices, renumeration letters, or other similar documents. Thus, the AI model 104 is trained to identify what specific sections within a particular type of document may include sensitive information and the type of sensitive information. By way of an example, credit cards issued by a specific bank and of a specific type would have credit card number, Card Verification Value (CVV) number, and expiry date at specific locations. The AI model 104 model may thus be trained to identify these locations in specific documents. Additionally, or alternatively, the AI model 104 may be trained to identify specific type of data as sensitive information. For example, numerals, names of people, address, or any other location related information.

[050] Once the electronic document is scanned, a degree of sensitivity associated with each of the one or more sections may be determined by the AI model 104 at step 404. Thereafter, at step 406, at least one of the plurality of obfuscating rules may be applied to each of the one or more sections, based on the associated degree of sensitivity determined by the AI model 104. In some embodiment, a higher degree of sensitivity determined for a section may ensure that a stricter obfuscating rule is applied to that section. By way of an example, the highest degree of sensitivity assigned to a section may necessitate that complete blurring of the section may be applied universally for all users. In contrast, the lowest degree of sensitivity assigned to a section may lead to only partial blurring of the section.

[051] Referring now to FIG. 5, a flowchart of a method for identifying, by a user, one or more sections that need to be obfuscated within an electronic document is illustrated, in accordance with an embodiment. With reference to step 306 in FIG. 3, in order to identify one or more sections within the electronic document, a user action corresponding to one or more sections within the electronic document may be received at step 502. Examples of the user action may include, but are not limited to drawing a bounding box around a section in the electronic document, selecting a pre-marked section within the electronic document, or making a specific geometric pattern on the electronic document. At step 504, the user action may be interpreted as intent to obfuscate the one or more sections. Further, at step 506, a user input may be received indicating a degree of sensitivity associated with each of the one or more sections. Thereafter, the one or more sections may be obfuscated based on the associated degree of sensitivity.

[052] Referring now to FIG. 6, a flowchart of a method for sharing a copy of electronic document with a user after applying obfuscating rules is illustrated, in

accordance with an embodiment. With reference to the step 310 in FIG. 3, in order to identify one or more sections within the electronic document, a unique link may be generated for accessing the electronic document at step 602. The unique link may be unique to the user and may enable the user to access the copy of the electronic document. In other words, anyone else accessing the unique link may not be able to access the copy of the electronic document. The unique link, for example, may have an address pointed to the server database 118.

[053] Once the unique link is generated, the unique link may be shared with the user at step 604. The user may extract the copy of the electronic document by clicking on the unique link. As discussed before, a unique link is generated for each user. Thus, the type of obfuscating rules applied on the copy of the electronic document available at the unique link may also be different.

[054] Referring now to FIG. 7, a flowchart of a method for selectively revealing obfuscation sections within a copy of an electronic document shared with a user is illustrated, in accordance with an embodiment. In this embodiment, when the copy of the electronic document is shared with the user, all sections within the copy of the electronic document are obfuscated. One or more of these sections are selectively revealed to the user. Thus, the method explained in FIG. 7 is different from the method explained in FIG. 3, where one or more sections are selectively obfuscated once the copy of the electronic document is shared with the user. In the current embodiment, at step 702, one or more sections within the electronic document that include sensitive information may be identified. At step 704, at least one of a plurality of obfuscating rules may be applied to each of the one or more sections. This has already been explained in detail in conjunction with FIG. 3.

[055] At step 706, each of the one or more sections may be obfuscated. Thereafter, at step 708, a copy of the electronic document may be shared with the user. Further, at step 710, at least one attribute associated with the user may be identified. This has already been explained in detail in conjunction with FIG. 3.

[056] At step 712, the user may be provided access to the copy of the electronic document. Based on the determined at least one attribute associated with the user and the applied at least one of the plurality of obfuscating rules, at least one section from the one or more sections may be selectively revealed to the user, at step 714.

[057] Referring now to FIG. 8, selective obfuscation of a debit card number within a digital copy 800 of a debit card is illustrated, in accordance with an exemplary embodiment. In this exemplary embodiment, the digital copy 800 of the debit card may be shared with two users, i.e., an unauthorized user 802 and an authorized user 804. Before the digital copy is shared, firstly, one or more sections that include debit card number, expiry date, and the CVV number within the digital copy of the debit card 800 are identified as having sensitive information. Thereafter, obfuscation rules are applied to each of these sections. In the current exemplary embodiment, obfuscation rules may be that only the debit card number needs to be concealed from unauthorized users (for example, the unauthorized user 802). The unauthorized user 802 and the authorized user 804 may be identified based on attributes associated with them. For example, the authorized user 804 may be a family member, while the unauthorized user 802 may just be an acquaintance. Additionally, the obfuscation rule may be to reveal the debit card number only to a family member.

[058] The digital copy 800 may be shared as a file with each of the unauthorized user 802 and the authorized user 804. Alternatively, a unique link may be shared with each of the unauthorized user 802 and the authorized user 804.The unique link may point to the server 116 that stores the digital copy 800.

[059] Irrespective of the means of accessing the digital copy 800, as depicted in FIG.8, when the unauthorized user 802 accesses the digital copy 800, the debit card number is partially redacted. However, when the authorized user 804 accesses the digital copy 800, the debit card number is completely revealed.

[060] Various embodiments provide method and system for selectively obfuscation sections within an electronic document. One or more sections within the electronic document may be selectively obfuscated for different users by firstly applying at least one of a plurality of obfuscating rules and secondly by using attributes associated with various users accessing the electronic document. Based on combination of an obfuscation rule and a user attribute, the user accessing the electronic document may be granted or denied access to a particular section within the electronic document.

[061] The method and system enable individuals and entities to automatically (or manually) select sections of a document that should be revealed to a third party and other sections of the document that should be blurred (or obfuscated/hidden) from the third party. Thus, the disclosed system and method is beneficial for both parties since they get the required inputs, and at the same time unnecessary details within the document are not shared with the third party. Moreover, since the original document is not altered, different such iterations with multiple users may be executed without any hassle. Additionally, after the document has been shared with the third party, the document owner at a later point in time may decide to blur certain unblurred

sections or unblur some blurred sections. Thus, the document owner may remotely control such actions and remains in absolute control of what is revealed to a third-party recipient at any point in time. It may be noted that in case any information on the electronic document needs to be blurred or unblurred after sending, the owner of the electronic document has controls to do so. The method and system also provide a holistic solution for access management in organisations, so that different sets of employees in the organizational hierarchy may get different levels of control over data.

[062] Moreover, the obfuscating rules applied on the document before sharing it make sure that certain sections of the document are automatically blurred or unblurred based on change in attributes associate with the third party at any given point in time. By way of an example, certain sections within a document may be unblurred or blurred for a specific time or day. Moreover, geo-fencing may also be used such that sensitive information is unblurred only in particular locations and that too for specific people only. For example, employees may only see company sensitive information within documents when they are inside the office premises. However, the company sensitive information may be blurred when these documents are opened elsewhere.

[063] As will be appreciated by those skilled in the art, the techniques described in the various embodiments discussed above are not routine, or conventional, or well understood in the art. The techniques discussed above provide for selectively obfuscation sections of electronic documents. The techniques may allow individuals to blur, unblur, and revoke access to specific sections within the electronic document as and when required. Since no edits are made to the original file, different recipients can be given different versions of the same electronic document. Further, through the above-mentioned techniques the original document

is not altered so different iterations can be sent to different people without any hassle. The techniques are privacy-centric, and the system provides a secure document vault since it is protected by end to end 256-bit encryption. Hence, all documents uploaded and edited are kept safe.

[064] As will be also appreciated, the above-described techniques may take the form of computer or controller implemented processes and apparatuses for practicing those processes. The disclosure can also be embodied in the form of computer program code containing instructions embodied in tangible media, such as floppy diskettes, solid state drives, CD-ROMs, hard drives, or any other computer-readable storage medium, wherein, when the computer program code is loaded into and executed by a computer or controller, the computer becomes an apparatus for practicing the invention. The disclosure may also be embodied in the form of computer program code or signal, for example, whether stored in a storage medium, loaded into and/or executed by a computer or controller, or transmitted over some transmission medium, such as over electrical wiring or cabling, through fiber optics, or via electromagnetic radiation, wherein, when the computer program code is loaded into and executed by a computer, the computer becomes an apparatus for practicing the invention. When implemented on a general-purpose microprocessor, the computer program code segments configure the microprocessor to create specific logic circuits.

[065] The disclosed methods and systems may be implemented on a conventional or a general-purpose computer system, such as a personal computer (PC) or server computer. Referring now to FIG. 9, an exemplary computing system 900 that may be employed to implement processing functionality for various embodiments (e.g., as a SIMD device, client device, server device, one or more processors, or the like) is illustrated. Those skilled in the relevant art will also recognize

how to implement the invention using other computer systems or architectures. The computing system 900 may represent, for example, a user device such as a desktop, a laptop, a mobile phone, personal entertainment device, DVR, and so on, or any other type of special or general-purpose computing device as may be desirable or appropriate for a given application or environment. The computing system 900 may include one or more processors, such as a processor 902 that may be implemented using a general or special purpose processing engine such as, for example, a microprocessor, microcontroller, or other control logic. In this example, the processor 902 is connected to a bus 904 or other communication medium. In some embodiments, the processor 902 may be an Artificial Intelligence (AI) processor, which may be implemented as a Tensor Processing Unit (TPU), or a graphical processor unit, or a custom programmable solution Field-Programmable Gate Array (FPGA).

[066] The computing system 900 may also include a memory 906 (main memory), for example, Random Access Memory (RAM) or other dynamic memory, for storing information and instructions to be executed by the processor 902. The memory 906 also may be used for storing temporary variables or other intermediate information during execution of instructions to be executed by the processor 902. The computing system 900 may likewise include a read only memory (“ROM”) or other static storage device coupled to bus 904 for storing static information and instructions for the processor 902.

[067] The computing system 900 may also include a storage device 908, which may include, for example, a media drive 910 and a removable storage interface. The media drive 910 may include a drive or other mechanism to support fixed or removable storage media, such as a hard disk drive, a floppy disk drive, a magnetic tape drive, an SD card port, a USB port, a micro-USB, an optical disk drive, a CD or

DVD drive (R or RW), or other removable or fixed media drive. A storage media 912 may include, for example, a hard disk, magnetic tape, flash drive, or other fixed or removable medium that is read by and written to by the media drive 910. As these examples illustrate, the storage media 912 may include a computer-readable storage medium having stored therein particular computer software or data.

[068] In alternative embodiments, the storage devices 908 may include other similar instrumentalities for allowing computer programs or other instructions or data to be loaded into the computing system 900. Such instrumentalities may include, for example, a removable storage unit 914 and a storage unit interface 916, such as a program cartridge and cartridge interface, a removable memory (for example, a flash memory or other removable memory module) and memory slot, and other removable storage units and interfaces that allow software and data to be transferred from the removable storage unit 914 to the computing system 900.

[069] The computing system 900 may also include a communications interface 918. The communications interface 918 may be used to allow software and data to be transferred between the computing system 900 and external devices. Examples of the communications interface 918 may include a network interface (such as an Ethernet or other NIC card), a communications port (such as for example, a USB port, a micro-USB port), Near field Communication (NFC), etc. Software and data transferred via the communications interface 918 are in the form of signals which may be electronic, electromagnetic, optical, or other signals capable of being received by the communications interface 918. These signals are provided to the communications interface 918 via a channel 920. The channel 920 may carry signals and may be implemented using a wireless medium, wire or cable, fiber optics, or other communications medium. Some examples of the channel 920 may include a phone

line, a cellular phone link, an RF link, a Bluetooth link, a network interface, a local or wide area network, and other communications channels.

[070] The computing system 900 may further include Input/Output (I/O) devices 922. Examples may include, but are not limited to a display, keypad, microphone, audio speakers, vibrating motor, LED lights, etc. The I/O devices 922 may receive input from a user and also display an output of the computation performed by the processor 902. In this document, the terms “computer program product” and “computer-readable medium” may be used generally to refer to media such as, for example, the memory 906, the storage devices 908, the removable storage unit 914, or signal(s) on the channel 920. These and other forms of computer-readable media may be involved in providing one or more sequences of one or more instructions to the processor 902 for execution. Such instructions, generally referred to as “computer program code” (which may be grouped in the form of computer programs or other groupings), when executed, enable the computing system 900 to perform features or functions of embodiments of the present invention.

[071] In an embodiment where the elements are implemented using software, the software may be stored in a computer-readable medium and loaded into the computing system 900 using, for example, the removable storage unit 914, the media drive 910 or the communications interface 918. The control logic (in this example, software instructions or computer program code), when executed by the processor 902, causes the processor 902 to perform the functions of the invention as described herein.

[072] It will be appreciated that, for clarity purposes, the above description has described embodiments of the invention with reference to different functional units and processors. However, it will be apparent that any suitable distribution of functionality

between different functional units, processors or domains may be used without detracting from the invention. For example, functionality illustrated to be performed by separate processors or controllers may be performed by the same processor or controller. Hence, references to specific functional units are only to be seen as references to suitable means for providing the described functionality, rather than indicative of a strict logical or physical structure or organization.

[073] Although the present invention has been described in connection with some embodiments, it is not intended to be limited to the specific form set forth herein. Rather, the scope of the present invention is limited only by the claims. Additionally, although a feature may appear to be described in connection with particular embodiments, one skilled in the art would recognize that various features of the described embodiments may be combined in accordance with the invention.

[074] Furthermore, although individually listed, a plurality of means, elements or process steps may be implemented by, for example, a single unit or processor. Additionally, although individual features may be included in different claims, these may possibly be advantageously combined, and the inclusion in different claims does not imply that a combination of features is not feasible and/or advantageous. Also, the inclusion of a feature in one category of claims does not imply a limitation to this category, but rather the feature may be equally applicable to other claim categories, as appropriate.

CLAIMS

WHAT IS CLAIMED IS:

1. A method for selectively obfuscation sections of electronic document, wherein the method comprising:

identifying one or more sections within an electronic document, wherein each of the at least one section comprises sensitive information;

applying at least one of a plurality of obfuscating rules to each of the one or more sections;

sharing, with a user, a copy of the electronic document after applying the at least one of the plurality of obfuscating rules to the one or more sections;

determining at least one attribute associated with the user;

selectively obfuscating at least one section from the one or more sections within the copy of the electronic document, based on the determined at least one attribute associated with the user and the applied at least one of the plurality of obfuscating rules; and

providing the user access to the copy of the electronic document in response to selectively obfuscating the at least one section.

2. The method of claim 1, further comprising:

receiving the electronic document; and

storing the electronic document in a storage, wherein the storage may be at least one of an online storage or a device storage.

3. The method of claim 1, wherein identifying comprises:

scanning the electronic document, by an Artificial Intelligence (AI) model, wherein the AI model is trained to identify sensitive information in a plurality of types of electronic documents; and

determining, by the AI model, a degree of sensitivity associated with each of the one or more sections.

4. The method of claim 3, wherein the at least one of the plurality of obfuscating rules are applied to each of the one or more sections based on the associated degree of sensitivity.

5. The method of claim 1, wherein identifying comprises:

receiving a user action corresponding to the one or more sections within the electronic document;

interpreting the user action as intent to obfuscate at least one of the one or more sections.

6. The method of claim 5, further comprising receiving a user input indicating a degree of sensitivity associated with each of the one or more sections.

7. The method of claim 1, wherein the plurality of obfuscating rules comprises at least one of:

partial obfuscation of a section from the one or more sections; or

complete obfuscation of a section from the one or more sections.

8. The method of claim 1, wherein selectively obfuscating the at least one section comprises applying at least one predefined obfuscating pattern to the at least one section.

9. The method of claim 8, wherein the at least one predefined obfuscating pattern comprises at least one of blurring, predefined image, predefined characters or alphabets, or coloured redactions

10. The method of claim 1, wherein the at least one attribute associated with the user comprises at least one of: a current location of the user, a role associated with the user, access rights granted to the user, relation of the user with an entity sharing the copy of the electronic document, current day and time, device being used by the user to access the copy of the electronic document, a network ID associated with the internet connection being used by the user, or other bibliographic data associated with the user.

11. The method of claim 1, wherein sharing the copy of the electronic document comprises:

generating a unique link for accessing the electronic document, wherein the unique link corresponds to the user; and

sharing the unique link with the user.

12. A method for selectively obfuscation sections of electronic document, wherein the method comprising:

identifying one or more sections within an electronic document, wherein each of the at least one section comprises sensitive information;

applying at least one of a plurality of obfuscating rules to each of the one or more sections;

obfuscating each of the one or more sections;

sharing, with a user, a copy of the electronic document after obfuscating each of the one or more sections;

determining at least one attribute associated with the user;

providing the user access to the copy of the electronic document; and

selectively revealing at least one section from the one or more sections to user, within the copy of the electronic document, based on the determined at least one attribute associated with the user and the applied at least one of the plurality of obfuscating rules.

13. A system for selectively obfuscation sections of electronic document, the system comprising:

a processor; and

a memory communicatively coupled to the processor, wherein the memory stores processor-executable instructions, which, on execution, causes the processor to:

identify one or more sections within an electronic document, wherein each of the at least one section comprises sensitive information;

apply at least one of a plurality of obfuscating rules to each of the one or more sections;

share, with a user, a copy of the electronic document after applying the at least one of the plurality of obfuscating rules to the one or more sections;

determine at least one attribute associated with the user;

selectively obfuscate at least one section from the one or more sections within the copy of the electronic document, based on the determined at least one attribute associated with the user and the applied at least one of the plurality of obfuscating rules; and

provide the user access to the copy of the electronic document in response to selectively obfuscating the at least one section.

14. The system of claim 13, wherein the processor is further configured to:

receive the electronic document; and

store the electronic document in a storage, wherein the storage may be at least one of an online storage or a device storage.

15. The system of claim 13, wherein to identify one or more sections, the processor is further configured to:

scan the electronic document, by an Artificial Intelligence (AI) model, wherein the AI model is trained to identify sensitive information in a plurality of types of electronic documents; and

determine, by the AI model, a degree of sensitivity associated with each of the one or more sections.

16. The system of claim 15, wherein the at least one of the plurality of obfuscating rules are applied to each of the one or more sections based on the associated degree of sensitivity.

17. The system of claim 16, wherein to identify one or more sections, the processor is further configured to:

receive a user action corresponding to the one or more sections within the electronic document; and

interpret the user action as intent to obfuscate at least one of the one or more sections.

18. The system of claim 17, wherein the processor is further configured to receive a user input indicating a degree of sensitivity associated with each of the one or more sections.

19. The system of claim 13, wherein for selectively obfuscate the at least one section the processor is further configured to apply at least one predefined obfuscating pattern to the at least one section, and wherein the at least one predefined obfuscating pattern comprises at least one of blurring, predefined image, predefined characters, or alphabets, coloured redactions.

20. The system of claim 13, wherein wherein the at least one attribute associated with the user comprises at least one of: a current location of the user, a role associated with the user, access rights granted to the user, relation of the user with an entity sharing the copy of the electronic document, current day and time, device being used

by the user to access the copy of the electronic document, a network ID associated with the internet connection being used by the user, or other bibliographic data associated with the user.

21. The system of claim 13, wherein to share the copy of the electronic document, the processor is further configured to:

generate a unique link for accessing the electronic document, wherein the unique link corresponds to the user; and

share the unique link with the user.

ABSTRACT

A method and system for selectively obfuscation sections of electronic document is disclosed. The method includes identifying one or more sections within the electronic document. The method further includes applying at least one of a plurality of obfuscating rules to each of the one or more sections. The method includes sharing, with a user, a copy of the electronic document and determining at least one attribute associated with the user. The method further includes selectively obfuscating at least one section from the one or more sections within the copy of the electronic document. The method includes providing the user access to the copy of the electronic document in response to selectively obfuscating the at least one section.

To be published with FIG. 8.