SYSTEM FOR DETECTING AND MANAGING FAKE WEBSITES IN A COMPUTING ENVIRONMENT

CROSS REFERENCE

This Application is based upon and derives the benefit of Indian Provisional Application Number 202341085624 filed on December 15, 2023, the contents of which are incorporated herein by reference.

FIELD OF INVENTION

[0001] Embodiments of the present disclosure relate to cyber security systems and more particularly relates to a system and method for detecting and managing fake websites, in a computing environment**.**

BACKGROUND

[0002] Security in an internet world has been a major challenge since many years. Internet provides a wide range of online platforms for exchanging information, and to provide a plurality of internet services. The exponential growth of such online platforms has led to an alarming surge in creation of duplicate websites. This may result in severe security threat to users, businesses, and challenge the overall integrity of the internet. Some of the existing mechanisms for identifying and mitigating these duplicate websites often fall short in ensuring online authenticity and security.

[0003] For example, some of the existing systems lack methods and systems for differentiating between original and duplicate websites. This may hamper the ability of users to make informed decisions about the legitimacy of such online platforms. The absence of robust tools to verify website authenticity makes the users vulnerable to various online threats, including phishing, scams, and identity theft.

[0004] Moreover, such an increase in duplicate websites risks the trust and confidence of users and further damages the efforts of original website owners who are at risk of reputational damage and loss of business. Some of the existing systems rely on visual cues or simple domain name checks and are no longer adequate to face sophisticated and deceptive duplicate websites.

[0005] One of the primary issues lies in the limitation of data points considered during the verification process. Existing methods often concentrate on singular aspects, such as domain name or SSL certificate status, leaving potential loopholes for fraudsters to exploit other unexamined elements. Therefore, such existing methods fail to scrutinize a broader spectrum of website properties.

[0006] Furthermore, website owners often lack efficient and immediate notification mechanisms when a duplicate website is detected. This delay in information dissemination undermines the ability of legitimate website owners to counteract fraudulent activities promptly.

[0007] In light of the above-mentioned challenges, there exists a need of system for detecting and managing fake websites in a computing environment**.**

SUMMARY

[0008] This summary is provided to introduce a selection of concepts, in a simple manner which is further described in the detailed description of the disclosure. This summary is neither intended to identify key or essential inventive concepts of the subject matter nor to determine the scope of the disclosure.

[0009] In accordance with an embodiment of the present disclosure, a computing system for detecting and managing fake websites in a computing environment is disclosed. The system includes one or more hardware processors and a memory coupled to the one or more hardware processors. The memory includes a plurality of modules in the form of programmable instructions executable by the one or more hardware processors. The plurality of modules includes a request handler module configured to receive a request for validating a website URL from a user via a communication network. The request includes at least one of URLs of a target website and user data. The plurality of modules includes the website validation module configured to determine a set of attributes corresponding to the website URL based on the received request. The set of attributes includes at least one of the static website attributes and the dynamic website attributes. The website validation module is configured to validate the website URL with an original website data based on the determined set of attributes using a machine learning-based validation model. The plurality of modules includes a report generation module configured to generate a validation report for the website URL based on results of validation. The plurality of modules includes an output module configured to output the validation report on a user

interface of a user device associated with the user and a device associated with an original website owner.

[00010] In accordance with another embodiment of the present disclosure, the method for detecting and managing fake websites in a computing environment is disclosed. The method includes receiving by a processor, a request for validating a website URL from a user via a communication network, the request includes at least one of URL of a target website and user data. Further, the method includes determining, by the processor, a set of attributes corresponding to the website URL based on the received request, the set of attributes include at least one of static website attributes and a dynamic website attributes. Further, the method includes validating, by the processor, the website URL with an original website data based on the determined set of attributes using a machine learning-based validation model. Further, the method includes generating, by the processor, a validation report for the website URL based on results of validation. Further, the method includes outputting, by the processor, the validation report on a user interface of a user device associated with the user and a device associated with an original website owner.

[00011] To further clarify the advantages and features of the present disclosure, a more particular description of the disclosure will follow by reference to specific embodiments thereof, which are illustrated in the appended figures. It is to be appreciated that these figures depict only typical embodiments of the disclosure and are therefore not to be considered limiting in scope. The disclosure will be described and explained with additional specificity and detail with the appended figures.

BRIEF DESCRIPTION OF DRAWINGS

[00012] The disclosure will be described and explained with additional specificity and detail with the accompanying figures in which:

[00013] **FIG. 1** is a schematic diagram of an exemplary computing environment for detecting and managing fake websites in accordance with an embodiment of the present disclosure;

[00014] **FIG. 2** is a block diagram illustrating an exemplary computing system, such as those shown in **FIG. 1**, capable of detecting and managing fake websites, in accordance with an embodiment of the present disclosure;

[00015] **FIGs. 3A-B** are a schematic representations of an exemplary computing environment of capable of detecting and managing fake websites in accordance with an embodiment of the present disclosure;

[00016] FIG. 4 is a process flow diagram illustrating an exemplary method for detecting and managing fake websites in a computing environment, in accordance with an embodiment of the present disclosure;

[00017] FIGs. 5A-1, 5A-2 are graphical user interfaces depicting a process of receiving a request for detecting and managing fake websites in a computing environment, in accordance with an embodiment of the present disclosure;

[00018] FIGs. 5B-E are graphical user interface representations illustrating validation results of a target website, in accordance with an embodiment of the present disclosure; and

[00019] FIG. 6 is a process flow diagram illustrating an exemplary method for detecting and managing fake websites in a computing environment, in accordance with another embodiment of the present disclosure.

[00020] Further, those skilled in the art will appreciate that elements in the figures are illustrated for simplicity and may not have necessarily been drawn to scale. Furthermore, in terms of the construction of the device, one or more components of the device may have been represented in the figures by conventional symbols, and the figures may show only those specific details that are pertinent to understanding the embodiments of the present disclosure so as not to obscure the figures with details that will be readily apparent to those skilled in the art having the benefit of the description herein.

DETAILED DESCRIPTION OF THE DISCLOSURE

[00021] For the purpose of promoting an understanding of the principles of the disclosure, reference will now be made to the embodiment illustrated in the figures and specific language will be used to describe them. It will nevertheless be understood that no limitation of the scope of the disclosure is thereby intended. Such alterations and further modifications in the illustrated system, and such further applications of the principles of the disclosure as would normally occur to those skilled in the art are to be construed as being within the scope of the present disclosure. It will be understood by those skilled in the art that the foregoing general description and the following detailed description are exemplary and explanatory of the disclosure and are not intended to be restrictive thereof.

[00022] In the present document, the word “exemplary” is used herein to mean “serving as an example, instance, or illustration.” Any embodiment or implementation of the present subject matter described herein as “exemplary” is not necessarily to be construed as preferred or advantageous over other embodiments.

[00023] The terms “comprise”, “comprising”, or any other variations thereof, are intended to cover a non-exclusive inclusion, such that one or more devices or sub-systems or elements or structures or components preceded by “comprises…. a” does not, without more constraints, preclude the existence of other devices, sub-systems, additional sub-modules. Appearances of the phrase “in an embodiment”, “in another embodiment” and similar language throughout this specification may, but not necessarily do, all refer to the same embodiment.

[00024] Unless otherwise defined, all technical and scientific terms used herein have the same meaning as commonly understood by those skilled in the art to which this disclosure belongs. The system, methods, and examples provided herein are only illustrative and not intended to be limiting.

[00025] A computer system (standalone, client or server computer system) is configured by an application may constitute a “module” (or “subsystem”) that is configured and operated to perform certain operations. In one embodiment, the “module” or “subsystem” may be implemented mechanically or electronically, so a module includes dedicated circuitry or logic that is permanently configured (within a special-purpose processor) to perform certain operations. In another embodiment, a “module” or “subsystem” may also comprise programmable logic or circuitry (as encompassed within a general-purpose processor or other programmable processor) that is temporarily configured by software to perform certain operations.

[00026] Accordingly, the term “module” or “subsystem” should be understood to encompass a tangible entity, be that an entity that is physically constructed permanently configured (hardwired) or temporarily configured (programmed) to operate in a certain manner and/or to perform certain operations described herein.

[00027] The present system provides a mechanism for a user to verify whether a website is original or duplicate. Further, the present system provides a process to combine multiple information of the website to decide probability of the website to be fake. Furthermore, the present system provides notification to a website owner about existence of a duplicate website. Furthermore, the present system also provides the method for detecting and managing online platforms and channels such as, for example, but not limited to, fake websites, emails, contact numbers and social media handles. The present system interfaces with external entities and is adaptable to diverse platforms, overcoming the absence of method available to the user and offering a robust solution to combat online threats.

[00028] In accordance with another embodiment of the present disclosure, a method for detecting and managing fake websites in a computing environment is disclosed. The method includes

analysing a duplicate website, verifying the duplicate website based on predefined standards, and notifying original website owners about presence of potential duplicate websites.

[00029] Referring now to the drawings, and more particularly to **FIG. 1** through **FIG. 6**, where similar reference characters denote corresponding features consistently throughout the figures, there are shown preferred embodiments and these embodiments are described in the context of the following exemplary system and/or method.

[00030] **FIG. 1** is a schematic representation of an exemplary computing environment 100 for detecting and managing fake websites in a computing environment in accordance with an embodiment of the present disclosure.

[00031] According to **FIG. 1**, the computing environment 100 may include one or more user devices 108 associated with one or more users communicatively coupled to a computing system 102 via a network 104. In an exemplary embodiment of the present disclosure, the one or more users may be website users, individuals, organizations or entities, and the like. The one or more user devices 108 are used by the one or more users to access the one or more websites 106 via the network 104. In an exemplary embodiment of the present disclosure, the one or more user devices 108 may include a laptop computer, desktop computer, tablet computer, smartphone, wearable device, smart watch, a digital camera and the like. Further, the network 104 may be internet, Wireless Fidelity (WI-FI), cloud connectivity, satellite communication and the like. The computing system 102 may be hosted on a central server, such as cloud server or a remote server.

[00032] In an exemplary embodiment, the one or more websites 106 may include one or more duplicate websites 106A-N. The duplicate websites 106A-N may be similar to duplicate website 106 not shown in **FIG. 1**. The duplicate websites 106A-N may be a website hosted by unauthorized individuals or entities, replicating some or all information from the original website 112A-M without consent, often with malicious intent to deceive website users.

[00033] The original website 112A-M (also referred herein individually as original website 112) (not shown in **FIG. 1)**. The original website 112A-M may be a website hosted by the owner of the website, encompassing essential attributes such as, for example, but not limited to, a domain name, a sub-domain name, a Secure Sockets Layer (SSL) certificate, and associated properties including address, hosting country, a validity date, hosting server details, content, links, mapping to Internet Protocol (IP) address, date of hosting, website validity, and other identifying attributes with public, derived, and private information.

[00034] Further, the computing environment 100 includes the computing system 102 capable of detecting duplicate websites 106A-N and notifying the owner of the original website 112, and the duplicate website detection system provider (not shown in **FIG. 1**). Although, FIG. 1 illustrates the computing system 102 communicatively coupled to the websites 106A-N and original websites 112A-M and the user device 108, one skilled in the art can envision that the computing system 102 may be connected to other websites and original websites112A-M and user devices 108, at multiple geographical locations via the network 104.

[00035] In an embodiment of the present disclosure, the computing environment 100 includes an external database (not shown) communicatively coupled to the computing system 102 via the network 104. The external database may store website properties, rules, and the like.

[00036] Further, the one or more user devices 108 may include a local browser, a mobile application or a combination thereof. Furthermore, the one or more users may use a web application via the local browser, the mobile application or a combination thereof to communicate with the computing system 102. In an embodiment of the present disclosure, the computing system 102 includes a plurality of modules 110. Details on the plurality of modules 110 have been elaborated in subsequent paragraphs of the present description with reference to FIG.2.

[00037] Those of ordinary skilled in the art will appreciate that the hardware depicted in FIG. 1 may vary for particular implementations. For example, other peripheral devices such as an optical disk drive and the like, Local Area Network (LAN), Wide Area Network (WAN), Wireless (e.g., Wi-Fi) adapter, graphics adapter, disk controller, input/output (I/O) adapter also may be used in addition or in place of the hardware depicted. The depicted example is provided for the purpose of explanation only and is not meant to imply architectural limitations with respect to the present disclosure.

[00038] In an embodiment of the present disclosure, the computing system 102 is configured to extract properties such as, for example, but not limited to static website attributes and dynamic website attributes of the duplicate websites 106A-N when a user device 108 is accessing the duplicate websites 106A-N, and validate the extracted properties using one or more pre-defined rules or an artificial intelligence or machine learning models or any other method known in the art. Further, the computing system 102 is configured to determine a ranking score for each of the duplicate websites 106A-N based on results of validation, where the ranking score indicates the probability of the duplicate websites 106A-N to be duplicate. Furthermore, the computing system 102 is configured to predict whether the duplicate websites 106A-N are duplicate based on the determined ranking

score. For example, if the ranking score range between a value tagged to indicate as duplicate, then the computing system 102 may generate a result stating that the duplicate websites 106A-N may be duplicate and generate corresponding notification messages. Further, the computing system 102 is configured to notify the user devices 108 whether the intended website is original and duplicate. Further, the computing system 102 is configured to notify to the original website owner 112A-M as well to inform there is possibility of user suspecting website as duplicate, and existence of possible duplicate website as notification.

[00039] **FIG. 2** is a block diagram illustrating an exemplary computing system 102, such as those shown in **FIG. 1**, capable of detecting and managing fake websites in a computing environment, in accordance with an embodiment of the present disclosure. Further, the computing system 102 includes one or more hardware processors 202, a memory 204 and a storage unit 206. The one or more hardware processors 202, the memory 204 and the storage unit 206 are communicatively coupled through a system bus 208 or any similar mechanism. The memory 204 includes the plurality of modules 110 in the form of programmable instructions executable by the one or more hardware processors 202. Further, the plurality of modules 110 include a request handler module 210, a website validation module 212, a report generation module 214, an output module 216, an alert generation module 218, and a blockchain validation module 220.

[00040] The one or more hardware processors 202, as used herein, means any type of computational circuit, such as, but not limited to, a microprocessor unit, microcontroller, complex instruction set computing microprocessor unit, reduced instruction set computing microprocessor unit, very long instruction word microprocessor unit, explicitly parallel instruction computing microprocessor unit, graphics processing unit, digital signal processing unit, or any other type of processing circuit. The one or more hardware processors 202 may also include embedded controllers, such as generic or programmable logic devices or arrays, application specific integrated circuits, single-chip computers, and the like.

[00041] The memory 204 may be non-transitory volatile memory and non-volatile memory. The memory 204 may be coupled for communication with the one or more hardware processors 202, such as being a computer-readable storage medium. The one or more hardware processors 202 may execute machine-readable instructions and/or source code stored in the memory 204. A variety of machine-readable instructions may be stored in and accessed from the memory 204. The memory 204 may include any suitable elements for storing data and machine-readable instructions, such as read only memory, random access memory, erasable programmable read only memory, electrically erasable programmable read only

memory, a hard drive, a removable media drive for handling compact disks, digital video disks, diskettes, magnetic tape cartridges, memory cards, and the like. In the present embodiment, the memory 204 includes the plurality of modules 110 stored in the form of machine-readable instructions on any of the above-mentioned storage media and may be in communication with and executed by the one or more hardware processors 202.

[00042] The storage unit 206 may be a cloud storage. The storage unit 206 may store the website data, properties, rules, and the like.

[00043] The request handler module 210 is configured to receive a request for validating a website URL from a user via a communication network 104. The request includes at least one of URL of a target website 106A-N (also referred herein as duplicate website 106A-N) and user data. The target website 106A-N is a website which is to be validated for duplication. The user data may include name, mobile number email and URL of the target website 106. The URL refers to Uniform Resource Locator.

[00044] The website validation module 212 is configured to determine a set of attributes corresponding to the website URL based on the received request. The set of attributes includes at least one of the static website attributes and dynamic website attributes. The static website attributes include at least one of, for example, but not limited to, a domain name, a sub-domain name, a geo location Sub domain name, a geo location of Domain and sub domain registration, a geo location of hosted IP address for domain / subdomain URL, a SSL certificate validity date dates, a SSL certificate process type, a Domain / sub-domain SSL status, a Serial number of SSL certificate, a SSL certificate public key, Domain provider details. The dynamic website attributes include at least one of a page content and check sum of the URL, a Logo and signed logo if applicable, a Domain, sub-domain and URL from black-list and white listed table lookup, a Purpose of the URL received by end user – financial, privacy, KYC, education, sales, marketing, Government, a domain / subdomain and URL look-up from 3rd party risk register, a Domain / subdomain and URL lookup from Government risk register, a Mechanism of URL redirection applied, a Response time of the URL, a Route to access the URL, a Number of hops to reach URL, a Regulatory status and response to access the URL, an Information type the URL is accessing, a Lookup from system created black list and white listed domain / sub domain and URLs, a Configurable business rules provided by original website owner.

[00045] The website validation module 212 is configured to validate the website URL with an original website 112A-M data based on the determined set of attributes using a machine learning-based validation model. In validating the website URL with the original website 112A-M data based on the determined set of attributes using the machine learning-based

validation model, the website validation module 212 is configured to generate dynamic website attributes for the website URL using the static website attributes and the received request. Further, the website validation module 212 is configured to map each of the static website attributes and the generated dynamic website attributes with a reference set of attributes corresponding to the original website 112A-M. Further, the website validation module 212 is configured to rank each of the static website attributes and the generated dynamic website attributes based on the mapping using a machine learning based ranking model. Further, the website validation module 212 is configured to compute a probability value of website accuracy for the target website106A-N based on a list of ranking. Further, the website validation module 212 is configured to compare the computed probability value with a threshold accuracy level allowed for the original website 112A-M. Further, the website validation module 212 is configured to determine if the target website 106A-N is a fake website based on the comparison.

[00046] In an exemplary embodiment, the website validation module 212 is configured to determine the ranking by creating dynamic information base for original website 112A-M. When the original website 112A-M owner subscribes or accesses service of the computing system 102, then using his inputs of owned website, the website validation module 212 is configured to create URL, domain/subdomain the information base of original website 112A-M. Further, the website validation module 212 is configured to create a dynamic information base for target website 106A-N provided by end user 108. Further, the website validation module 212 is configured to calculate a rank from dynamic information of original website 112A-M and target website 106A-N, by applying for example, but not limited to, deterministic ranking process for static information and probabilistic ranking process for dynamic information. Further, the website validation module 212 is configured to apply ranking by similar mechanism for dynamic information for overall ranking. A person skilled in the art may envision that the ranking process or technique may include any other techniques known in the art.

[00047] In an exemplary embodiment, if there is a mismatch in any row of the static attributes, then a probability rank is determined as; RANK_STATIC = 1, the value 1 indicates that the target website 106A-N is 100% fake website.

[00048] In an exemplary embodiment, if there is a match in any row of the static attributes, then a probability rank is determined as; RANK_STATIC = 0, wherein the value 0 indicates that the target website 106A-N is 100% match website.

[00049] In an exemplary embodiment, if there is a match in row i of the dynamic attributes, then a probability rank is determined as; RANK_DYNAMIC(i) = i/N, where N is total number of dynamic information checked.

[00050] In an exemplary embodiment, if there is mismatch in row then a probability rank is determined as; RANK_DYNAMIC(i) = 0

[00051] In an exemplary embodiment, the website validation module 212 is configured to compute the probability of detecting accurate website is described as below.

$$Probability = [f1\,(RANK_STATIC\ for\ all\ the\ static\ rows = 0)\ and\ f2\,(RANK_DYNAMIC(i)\ of\ all\ the\ dynamic\ rows = sum\ of\ all\ the\ ranks)\,] \ldots\ldots Equation\ (1)$$

[00052] In an exemplary embodiment, if the computed probability of detecting target website 106A-N is less than 95% (< 95%) then, the target website 106A-N is possibly a fake or a duplicate website 106A-N.

[00053] In an exemplary embodiment, if computed probability of detecting target website 110 is more than or equal to 95% (>= 95%) then, the target website 106A-N is not fake or not duplicate.

[00054] The report generation module 214 is configured to generate a validation report for the website URL based on results of validation. In generating the validation report for the website URL based on results of validation, the report generation module is configured to generate one or more AI-driven insights for the target website based on the results of validation. The one or more AI-driven insights include such as, for example, but not limited to, domain name mismatch with additional alphabet in the reference website name, SSL certificate date mismatch between reference and target website, host country of the reference website is different than host country of the target website. . The report generation module 214 is configured to generate the validation report for the website URL. The validation report includes the generated one or more AI-driven insights, one or more issues associated with the target website, root causes for the one or more issues and recommendations for resolving the one or more issues. The root causes may include such as, for example, but not limited to, dynamic website URL, host country mismatch, IP address mismatch, dynamic keyword information, broken or empty links in the URL, invalid social media links in the website.

[00055] The output module 216 is configured to output the validation report on a user interface of a user device 108 associated with the user and a device associated with an original website owner.

[00056] The blockchain validation module 218 is configured to verify the results of validation using a blockchain network system. The blockchain validation module 218 includes, for example, one or more authorized expert block nodes. Further, the blockchain validation module 218 is configured to determine whether the target website 106A-N belongs to critical cyber-attacks such as, for example, but not limited to phishing attack, ransomware, Denial-of-Service (DoS), Man-in-the-Middle (MitM), SQL injection, Cross -Site Scripting (XSS), Zero-Day Exploits, DNS Spoofing based on the verification. Further, the blockchain validation module 218 is configured to generate emergency messages such as, for example, but not limited to high priority messages, SOS alerts, mass notification system comprising information associated with the target website 106A-N and the type of critical cyber-attack determined. Further, the blockchain validation module 218 is configured to broadcast the generated emergency messages to one or more authorities such as, for example, but not limited to regulatory authorities of government, cyber-crime branch, Cyber Regulations Appellate Tribunal using a communication network 104.

[00057] The alert generation module 220 is configured to generate an alert message to the original website owner if the results of validation indicate that the website URL corresponds to a fake website 106A-N (also referred herein as duplicate website 106A-N OR target website 106 A-N). Further, the alert generation module 220 is configured to send the generated alert message to the original website owner using a communication network 104.

[00058] In an exemplary embodiment, the computing system 102 may be configured for gathering a set of information, including for example, but not limited to, static and dynamic attributes from the duplicate websites 106A-N which the user device 108 is trying to access. The computing system 102 may employ various methods, including for example, but not limited to, direct data submission by the website owner, automated tools, software agents, or scripts to acquire the website data. The acquired website data may include essential attributes such as domain name, subdomain name, SSL certificate details, content, links, mapping to IP address, date of hosting, and other identifying attributes containing public, derived, and private information. The computing system 102 ensures a comprehensive dataset for subsequent analysis by the validation module 212.

[00059] The computing system 102 is configured for performing validation checks and processes to verify the acquired website data. The computing system 102 confirms the authenticity of the acquired website data, eliminating potential errors or discrepancies that could

compromise the duplicate detection process. The computing system 102 validates the acquired website data using one or more pre-defined rules or an artificial intelligence or machine learning models or any other method known in the art.

[00060] The computing system 102 is configured to employ advanced process and comparison techniques to analyze the acquired and validated website data. The computing system 102 systematically evaluates multiple properties, such as domain name, SSL certificate details, content, and other identifying attributes, to determine the probability of a website being a duplicate. By comparing these attributes between the original and potential duplicate websites, the computing system 102 provides a conclusive assessment of the website's authenticity. The computing system 102 forms the essence of the detection logic, contributing to the overall effectiveness of the system.

[00061] The computing system 102 serves as the concluding phase in the detection process. Upon completion of the duplication detection analysis, the computing system 102 generates and transmits notifications to relevant stakeholders such as, for example, but not limited to website user 108, owner 316 of original website 112. These notifications include results such as whether the website is identified as an original or a potential duplicate. In the event of a potential duplicate, notifications are sent to both the end user and the owner of the original website 001. The computing system 102 ensures timely communication of detection outcomes, facilitating informed decision-making and proactive responses to mitigate potential risks associated with duplicate websites.

[00062] **FIGs. 3A-B** are a schematic representations of an exemplary computing environment of capable of detecting and managing fake websites in accordance with an embodiment of the present disclosure; According to **FIG. 3A**, the computing environment 100 may include an owner 316 of original website. In an exemplary embodiment, the owner 316 of the original website may be an individual or a corporate entity hosting a website. Further, the computing environment 100 may include an original website 112 associated with the owner 316 of the original website 112. Each of the original website 112 may be a website hosted by the owner of the website 316, comprising essential attributes such as for example, but not limited to, a domain name, a sub-domain name, a Secure Sockets Layer (SSL) certificate, and associated properties including, but not limited to, an address, a hosting country, a validity date, a hosting server details, a content, links, mapping to internet protocol (IP) address, a date of hosting, a website validity, and other identifying attributes with a public, a derived, and a private information. Each of the original website 112 may be hosted on an internet 104. The internet 104 may be a network connectivity infrastructure facilitating domain name utility, IP address allocation, routing, and application-specific

processing. Further, the computing environment 100 may include a website user 108 willing to use the websites using the internet 107. The website user 108 may be an individual or entity accessing a website on the internet 104 through a computing system such as PC, laptop, mobile, handheld device, or tablet computer, or computing device which has provision to access website.

[0001] Further, the computing environment 100 may include a duplicate website 106 also hosted on the internet 104. The duplicate website 106 may be a website hosted by unauthorized individuals or entities, replicating some or all information from the original website 112 without consent, or without replicating information from the original website 112 but claiming duplicate website is genuine in whole or part of original website 112, is the often with malicious intent to deceive website users 108.

[0002] Further, the computing environment 100 may include a duplicate detection interface 314. The duplicate detection interface 314 may be a system interface provided by a duplicate website detection system 304 to external entities (such as for e.g., entities hosted on websites of government, governing bodies, industry forums, individual websites, original website 112 and the like through various interfaces such as for example, but not limited to, widgets, web portal links, web portal forms, redirection pages, application programming interface (API) or any other system where end user can choose to verify website identity whether the website is original or duplicate. The duplicate website detection system 304 is similar to the computing system 102 such as those shown in **FIG. 2.**

[0003] Furthermore, the computing environment 100 may include a duplicate website detection server provider 318 connected to the duplicate website detection system 304. In an exemplary embodiment, the duplicate website detection system 304 may be an individual, or organization, or entity offering services or facilities related to duplicate website 106 detection to one or multiple owners 316 of original websites 112. The duplicate website detection server provider 318 may be the same as the owner of original website 316 or a different entity.

[0004] Furthermore, the computing environment 100 may include the duplicate website detection system 304 further connected to the duplicate website detection server provider 318, and the duplicate detection interface 314. Further, the duplicate website detection system 304 may also be connected to the website user 108 via the internet 104. The duplicate website detection system 304 may also be connected to the duplicate website 106 via the internet 104. In an exemplary embodiment, the duplicate website detection system 304 may be a comprehensive system comprising software, hardware, computing resources either alone or in a combination thereof designed to detect duplicate websites, notifying the original

website owner 316 and/or the duplicate website detection service provider 318. The duplicate website detection system 304 may detect duplication of one or more websites. Further, the duplicate website detection system 304 may include components such as a management interface agent 306, a detection application agent 308, a detection data 310 and a notification agent 312. The components depicted within the duplicate website detection system 304 are in addition to the plurality of modules 110.

[0005] In an embodiment, the management interface agent 306 may be a user interface using graphical, command-line, API, or other mechanisms. Further, the management interface agent 306 is responsible to configure, control, and administer the duplicate website detection system 304.

[0006] In an embodiment, the detection application agent 308 may be an application, software, or hardware implemented through programming languages or scripting, running on a computing device with logic for duplicate website detection. The detection logic may use various process and criteria to identify potential duplicate websites.

[0007] In an embodiment, the detection data 310 may include one or more properties of a website to provide a set of information crucial for the identification of potential duplicate websites 106A-N. These properties may include for but are not limited to a domain name, a sub domain name, a SSL certificate and its associated properties such as, an address, a country of hosting, a validity date, a hosting server, a content, links, mapping to IP address with date of hosting, a validity of website and other attribute to identify website with public, derived and private information.

[0008] This data is collected directly or indirectly from the owner of original website 316 through software, tools, or scripts or the like. The comprehensive set of information facilitates a thorough analysis of websites, enabling the detection logic to discern potential duplicates.

[0009] In an embodiment, the notification agent 312 may be a component responsible for notifying the owner of original website owner 316 and/or the duplicate website detection server provider 318 upon the detection of a potential duplicate website 106. Further, the notification agent 312 is responsible for generating notifications related to the detected duplicate websites 106A-N and notifying them to the original website owner 316, website user 108 and/or the duplicate website detection server provider 318. The notification may include for example, but not limited to, detailed analysis reports.

[00010] The notification agent 312 serves as a final phase in the detection logic, communicating the result outcome to the end user i.e. website user 108. Upon completion of the detection logic check, the notification agent 312 generates notifications indicating whether the

intended website is deemed original or a potential duplicate. The notifications are disseminated to multiple recipients:

[00011] **Website user 108 Notification**: The website user 108 is promptly notified about the authenticity of the website, providing assurance or alerting them to exercise caution if the website is flagged as a potential duplicate. This proactive approach enhances user awareness and security.

[00012] **Original website owner 316 notification**: Simultaneously, the original website owner 316 and/or duplicate website detection service provider 318 is informed of the detection outcome. This notification serves to alert the original website owner 316 about the possibility of users suspecting the website as a duplicate and notifies them of the existence of a potential duplicate website 106. Such timely notifications empower the original website owner 316 and/or duplicate website detection service provider 318 to take necessary /corrective actions, preserving the integrity and trustworthiness of their online presence.

[00013] **Exemplary Scenario 1: Real-time Duplicate Website Detection**

[00014] In this scenario, the computing system 102 operates in real-time to detect and validate properties of duplicate websites when a user device 108 is accessing them. The system 102 continuously monitors user interactions and extracts relevant properties of the duplicate websites 106A-N in real-time. The extracted properties are then validated using pre-defined rules, artificial intelligence, or machine learning models. In an example embodiment, AI models below may be implemented for validating the target website 106. For example, a Support Vector Machines (SVM) may be used for classifying data points into categories (real or fake website). The SVM models may find hyperplanes that best separate the data points in high dimensional space. The SVM models may be traiedn an SVM on features extracted from known real and fake websites (e.g., URL length, presence of specific keywords, website age). Further, a random forest model may be used which combine multiple decision trees, leading to more robust and accurate predictions. By training a Random Forest model on features extracted from websites, a classification of real or fake is obtained based on the combined knowledge of all the decision trees. Furthermore, deep learning models such as Convolutional Neural Networks (CNNs) may be used for analyzing website visuals. By training a CNN on images of legitimate and fake website layouts, text fonts, and security certificates, the model may identify patterns that indicate a fake website. Additionally, models such as the isolation Forest , Local Outlier Factor (LOF): LOF may be used. Additionally, Graph Neural Networks (GNNs) for Multi-source Validation may be used. Traditional website validation analyses data in isolation (text, images). However, the present system 100 uses GNNs at processing data

with inherent relationships. Consider a website as a network of nodes (webpages, images, user reviews) connected by edges (links). The GNN models analyze these connections to identify inconsistencies. Further, models such as Few-Shot Learning may be used for adapting to new data with minimal training examples. For example, a few-shot learning model may be trained on a small set of new scam website examples. The model may then identify similar patterns in other websites, even if they have not been explicitly added to the training data. Moreover, a Generative Adversarial Networks (GANs) may be used which consist of two models: a generator which creates a synthetic data and a discriminator that tries to distinguish real data from the generated data. This training process may be leveraged for both data augmentation and anomaly detection. For example, for tasks requiring a large amount of training data (e.g., training image recognition models for identifying fake website layouts), a GAN may generate additional realistic website mockups to supplement the real data. Also, the GAN may be trained on legitimate website data. The discriminator, which learns to distinguish real from generated data, may then be used to detect anomalies in original websites that deviate from the patterns it learned.

[00015] Additionally, explainable AI models may be used to further explain why a website validation model flagged a target website 106 as suspicious. This transparency may build trust in the validation system and help identify areas for improvement.

[00016] For instance, the computing system 102 may observe a user accessing a website that looks similar to a well-known e-commerce platform. The system 102 extract features such as webpage structure, content, and metadata. It then validates these properties against a set of rules or a machine learning model trained to identify genuine websites 112A-M. If the properties match those of a known duplicate website 106A-N, the system 102 assigns a ranking score indicating the probability of it being a duplicate.

[00017] Based on the determined ranking score, the computing system 102 predicts whether the accessed website is a duplicate. If the score falls within a predefined range indicating a high probability of duplication, the system 102 generates a notification message to the user device 108, informing them about the potential duplicate website and recommending caution.

[00018] Additionally, the computing system 102 may notify the original website owner 316, alerting them to the possibility that users may be suspecting their website 106 as a duplicate. This allows the owner 316 to investigate and take necessary actions to protect their brand and users.

Exemplary Scenario 2: Batch Analysis for Website Owners

[00019] In this scenario, the computing system 102 performs batch analysis periodically to identify potential duplicate websites across a range of user interactions. The system 102 collects data on multiple duplicate websites 106A-N accessed by various user devices 108 over a specified time period.

[00020] The extracted properties are then validated using pre-defined rules or machine learning models. The computing system 102 determines ranking scores for each duplicate website 106A-N, indicating the probability of duplication. For example, the system 102 may identify a cluster of websites with similar features and validate them collectively.

[00021] Once the ranking scores are determined, the computing system 102 generates a report for the original website owner 316. This report includes a list of potential duplicate websites, their ranking scores, and other relevant information. The owner 316 is then notified of the possibility of users suspecting their website 106 as a duplicate, allowing them to take appropriate actions to safeguard their brand and reputation.

Exemplary Scenario 3: Collaborative Detection

[00022] In this scenario, the computing system 102 fosters collaboration among multiple user devices 108 to enhance duplicate website detection. The system 102 collects data from a network of users accessing websites and shares information about potential duplicates among them.

[00023] When a user device 108 accesses a website, the computing system 102 extracts and validates properties, determining a ranking score. This score is then shared anonymously with the central system. If multiple users access similar websites and the properties match, the system 102 aggregates the ranking scores to enhance the accuracy of duplicate detection.

[00024] Based on the aggregated scores, the computing system 102 generates notifications to the respective user devices 108, informing them of potential duplicate websites 106A-N. Simultaneously, the original website owner 316 is notified about the collaborative suspicion of duplication, allowing them to investigate and take corrective measures.

[00025] FIG. 4 is a process flow diagram illustrating an exemplary method for detecting and managing fake websites in a computing environment, in accordance with an embodiment of the present disclosure. At step 402, property-I logic is initiated. At step 404, property-I of original website W1 is selected. At step 406, property-I of reference website W2 is selected. At step 408, perform a comparison logic of step 404 and 406. At step 410, duplicate probability of website X is ranked. At step 412, next property logic for next property of same website W1 is initiated and the steps from 402 are repeated until all

properties of the website W1 are covered. At step 414, once all the properties are covered, a result=f (Rank duplicate probability X) of all properties is generated. At step 416, the result is notified to website owners and/or duplicate system detection service provider 318.

[00026] The method 400 may be implemented in any suitable hardware, software, firmware, or combination thereof.

[00027] FIGs. 5A-1, 5A-2 aregraphical user interfaces for receiving a request for detecting and managing fake websites in a computing environment, in accordance with an embodiment of the present disclosure. According to **FIG. 5A-1,** the original website 112 is provided with an input check feature 500, allowing the website user 108 to check authenticity of the original website 112 within the website itself. Hence, the user need not use any third party websites for authenticating the target websites. Further, the **FIG.5A-2** depicts**,** a website user 108 may have to enter name, mobile number, email and URL of the suspected website, which may be detected as authentic or duplicate based on the machine learning process of the computing system 102.

[00028] FIGs. 5B-E are graphical user interface representations illustrating validation results of a target website, in accordance with an embodiment of the present disclosure. **FIG. 5B** depicts a negative result of the validating the targeted website 106A-N, when the website is detected as duplicate website 106A-N. Further, the **FIG 5C** depicts a positive result of validating the targeted website 106A-N, when the website is detected as original website 112A-M. Further, the **FIG. 5D** depicts a message sent to the owner 316 of the original website 112A-M on detecting the duplicate website 106A-N of same name. Further, the **FIG. 5E** depicts an alert sent to the website user 108 on detecting the duplicate website 106A-N.

[00029] FIG. 6 is a process flow diagram illustrating an exemplary method for detecting and managing fake websites in a computing environment 100, in accordance with another embodiment of the present disclosure. At step 602, the method 600 includes receiving, by a processor 202, a request for validating a website URL from a user via a communication network 104. The request includes at least one of URL of a target website and user data. At step 604, the method 600 includes determining, by the processor 202, a set of attributes corresponding to the website URL based on the received request. The set of attributes include at least one of the static website attributes and dynamic website attributes. At step 606, the method 600 includes validating, by the processor 202, the website URL with an original website 112A-M data based on the determined set of attributes using a machine learning-based validation model. At step 608, the method 600 includes generating, by the processor 202, a validation report for the website URL based on results of validation. At step 610, the method 600 includes outputting, by the processor 202, the validation report on a user interface of a

user device associated with the user 108 and a device associated with an original website owner 316.

[00030] The present systems reduce cyber fraud for user getting trap into accessing fake website 106A-N for financial fraud, social engineering frauds, privacy threats, sharing confidential information and possible cyber frauds through websites. There are currently no automatic options on the original website 112A-M available to check the URL which the user is accessing to determine whether it is genuine or fake.

[00031] Further, the present system provides mechanisms on plurality of website to verify whether the website is original or not. In an exemplary embodiment, bank X can provide provision in their website for its customers can check any received Bank x website URL is genuine or suspicious. In another example, financial institution may look for any possible fake website using their identity exists through their customers. In another example, an internet user received notification from institution to submit Know Your Customer (KYC) details through website, but user does not share whether the website is genuine or fake. In yet another example, student submitting education application through website with all their information through university but not sure the university website is genuine or not.

[00032] Every website will have property of domain name, sub domain name, IP address, owner, SSL certificate, validity date, domain age, hosted country as information. This information is available for both original website 112A-M and duplicate website 106A-N. The checking between these multiple information between original website 112A-M and duplicate website 106A-N through computer process is used to detect probability of duplicate website is fake or not. The checking is provided on both either on original website as option or as standalone facility for any user to check whether the website is original or duplicate. Once process is detected the reference website is fake the information/analysis report also will be notified to owner 316 of original website 112A-M.

[00033] The written description describes the subject matter herein to enable any person skilled in the art to make and use the embodiments. The scope of the subject matter embodiments is defined by the claims and may include other modifications that occur to those skilled in the art. Such other modifications are intended to be within the scope of the claims if they have similar elements that do not differ from the literal language of the claims or if they include equivalent elements with insubstantial differences from the literal language of the claims.

[00034] The embodiments herein can include hardware and software elements. The embodiments that are implemented in software include but are not limited to, firmware, resident software, microcode, etc. The functions performed by various modules described herein may be

implemented in other modules or combinations of other modules. For the purposes of this description, a computer-usable or computer readable medium can be any apparatus that can include, store, communicate, propagate, or transport the program for use by or in connection with the instruction execution system, apparatus, or device.

[00035] The medium can be an electronic, magnetic, optical, electromagnetic, infrared, or semiconductor system (or apparatus or device) or a propagation medium. Examples of a computer-readable medium include a semiconductor or solid-state memory, magnetic tape, a removable computer diskette, a random-access memory (RAM), a read-only memory (ROM), a rigid magnetic disk and an optical disk. Current examples of optical disks include compact disk-read only memory (CD-ROM), compact disk-read/write (CD-R/W) and DVD.

[00036] Input/output (I/O) devices (including but not limited to keyboards, displays, pointing devices, etc.) can be coupled to the system either directly or through intervening I/O controllers. Network adapters may also be coupled to the system to enable the data processing system to become coupled to other data processing systems or remote printers or storage devices through intervening private or public networks. Modems, cable modem and Ethernet cards are just a few of the currently available types of network adapters.

[00037] A representative hardware environment for practicing the embodiments may include a hardware configuration of an information handling/computer system in accordance with the embodiments herein. The system herein includes at least one processor or central processing unit (CPU). The CPUs are interconnected via system bus 208 to various devices such as a random-access memory (RAM), read-only memory (ROM), and an input/output (I/O) adapter. The I/O adapter can connect to peripheral devices, such as disk units and tape drives, or other program storage devices that are readable by the system. The system can read the inventive instructions on the program storage devices and follow these instructions to execute the methodology of the embodiments herein.

[00038] The system further includes a user interface adapter that connects a keyboard, mouse, speaker, microphone, and/or other user interface devices such as a touch screen device (not shown) to the bus to gather user input. Additionally, a communication adapter connects the bus to a data processing network, and a display adapter connects the bus to a display device which may be embodied as an output device such as a monitor, printer, or transmitter, for example.

[00039] A description of an embodiment with several components in communication with each other does not imply that all such components are required. On the contrary, a variety of optional components are described to illustrate the wide variety of possible embodiments

of the invention. When a single device or article is described herein, it will be apparent that more than one device/article (whether or not they cooperate) may be used in place of a single device/article. Similarly, where more than one device or article is described herein (whether or not they cooperate), it will be apparent that a single device/article may be used in place of the more than one device or article, or a different number of devices/articles may be used instead of the shown number of devices or programs. The functionality and/or the features of a device may be alternatively embodied by one or more other devices which are not explicitly described as having such functionality/features. Thus, other embodiments of the invention need not include the device itself.

[00040] The illustrated steps are set out to explain the exemplary embodiments shown, and it should be anticipated that ongoing technological development will change the manner in which particular functions are performed. These examples are presented herein for purposes of illustration, and not limitation. Further, the boundaries of the functional building blocks have been arbitrarily defined herein for the convenience of the description. Alternative boundaries can be defined so long as the specified functions and relationships thereof are appropriately performed. Alternatives (including equivalents, extensions, variations, deviations, etc., of those described herein) will be apparent to persons skilled in the relevant art(s) based on the teachings contained herein. Such alternatives fall within the scope and spirit of the disclosed embodiments. Also, the words "comprising," "having," "containing," and "including," and other similar forms are intended to be equivalent in meaning and be open-ended in that an item or items following any one of these words is not meant to be an exhaustive listing of such item or items or meant to be limited to only the listed item or items. It must also be noted that as used herein and in the appended claims, the singular forms “a,” “an,” and “the” include plural references unless the context clearly dictates otherwise.

[00041] Finally, the language used in the specification has been principally selected for readability and instructional purposes, and it may not have been selected to delineate or circumscribe the inventive subject matter. It is therefore intended that the scope of the invention be limited not by this detailed description, but rather by any claims that issue on an application based here on. Accordingly, the embodiments of the present invention are intended to be illustrative, but not limiting, of the scope of the invention, which is set forth in the following claims.

WE CLAIM

1. A system (102) for detecting and managing fake websites in a computing environment (100), the system (102) comprising:

one or more hardware processors (202); and

a memory (204) coupled to the one or more hardware processors (202), wherein the memory (204) comprises a plurality of modules (110) in the form of programmable instructions executable by the one or more hardware processors (202), wherein the plurality of modules (110) comprises:

a request handler module (210) configured to receive a request for validating a website URL from a user via a communication network (104), wherein the request comprises at least one of URL of a target website (106) and user data;

a website validation module (212) configured to:

determine a set of attributes corresponding to the website URL based on the received request, wherein the set of attributes comprise at least one of a static website attributes and a dynamic website attributes;

validate the website URL with an original website data based on the determined set of attributes using a machine learning-based validation model;

a report generation module (214) configured to generate a validation report for the website URL based on results of validation; and

an output module (216) configured to output the validation report on a user interface of a user device (108) associated with the user and a device associated with an original website owner (316).

2. The system (102) as claimed in claim 1, further comprising an alert generation module (220) configured to:

generate an alert message to the original website owner (316) if the results of validation indicate that the website URL corresponds to a fake website (106); and

send the generated alert message to the original website owner (316) using a communication channel (104).

3. The system (102) as claimed in claim 1, wherein in validating the website URL with the original website data based on the determined set of attributes using the machine learning-based validation model, the website validation module (212) is configured to:

generate dynamic website attributes for the website URL using the static website attributes and the received request;

map each of the static website attributes and the generated dynamic website attributes with a reference set of attributes corresponding to the original website (112);

rank each of the static website attributes and the generated dynamic website attributes based on the mapping using a machine learning based ranking model;

compute a probability value of website accuracy for the target website (106) based on a list of ranking;

compare the computed probability value with a threshold accuracy level allowed for the original website (112); and

determine if the target website (106) is a fake website (106) based on the comparison.

4. The system (102) as claimed in claim 1, wherein the static website attributes comprise at least one of a domain name, a sub-domain name, a geo location Sub domain name, a geo location of Domain and sub domain registration, a geo location of hosted IP address for domain / subdomain URL, a SSL certificate validity date dates, a SSL certificate algorithm type, a Domain / sub-domain SSL status, a Serial number of SSL certificate, a SSL certificate public key, Domain provider details.

5. The system (102) as claimed in claim 1, wherein the dynamic website attributes comprise at least one of a page content and check sum of the URL, email id, contact number, social media handle present in the website, a Logo and signed logo if applicable, a Domain, sub-domain and URL from black-list and white listed table lookup, a Purpose of the URL received by end user – financial, privacy, KYC, education, sales, marketing, Government, a domain / subdomain and URL lookup from 3rd party risk register, a Domain / subdomain and URL lookup from Government risk register, a Mechanism of URL redirection applied, a Response time of the URL, a Route to access the URL, a Number of hops to reach URL, a Regulatory status and response to access the URL, an Information type the URL is accessing, a Lookup from system created black list and white listed domain / sub domain and URLs, a Configurable business rules provided by original website owner (316).

6. The system (102) is claimed in claim 1, wherein also used as detection mechanism of fake email id, fake contact number, fake social media handles or similar digital identities.

7. The system (102) as claimed in claim 1, wherein in generating the validation report for the website URL based on results of validation, the report generation module (214) is configured to:

generate one or more AI-driven insights for the target website (106) based on the results of validation; and

generate the validation report for the website URL, wherein the validation report comprises the generated one or more AI-driven insights, one or more issues associated with the target website, root causes for the one or more issues and recommendations for resolving the one or more issues.

8. The system (102) as claimed in claim 1, further comprising a blockchain validation module (218) configured to:

verify the results of validation using a blockchain network system comprising one or more authorized expert block nodes;

determine whether the target website (106) belongs to a critical cyber-attack based on the verification;

generate emergency messages comprising information associated with the target website (106) and the type of critical cyber-attack determined; and

broadcast the generated emergency messages to one or more authorities using a communication network (104).

9. A method (600) for detecting and managing fake websites (106) in a computing environment (100) comprising:

receiving, by a processor (202), a request for validating a website URL from a user (108) via a communication network (104), wherein the request comprises at least one of URL of a target website (106) and user data;

determining, by the processor (202), a set of attributes corresponding to the website URL based on the received request, wherein the set of attributes comprise at least one of a static website attribute and a dynamic website attributes;

validating, by the processor (202), the website URL with an original website (112) data based on the determined set of attributes using a machine learning-based validation model;

generating, by the processor (202), a validation report for the website URL based on results of validation; and

outputting, by the processor (202), the validation report on a user interface of a user device (108) associated with the user and a device associated with an original website owner (316).

10. The method (600) as claimed in claim 8, further comprising:

generating, by the processor (202), an alert message to the original website owner (316) if the results of validation indicate that the website URL corresponds to a fake website (106); and

sending, by the processor (106), the generated alert message to the original website owner (316) using a communication channel (104).

11. The method (600) as claimed in claim 8, wherein validating the website URL with the original website data based on the determined set of attributes using the machine learning-based validation model comprises:

generating, by the processor (202), dynamic website attributes for the website URL using the static website attributes and the received request;

mapping, by the processor (202), each of the static website attributes and the generated dynamic website attributes with a reference set of attributes corresponding to the original website (112);

ranking, by the processor (202), each of the static website attributes and the generated dynamic website attributes based on the mapping using a machine learning based ranking model;

computing, by the processor (202), a probability value of website accuracy for the target website (106) based on a list of ranking;

comparing, by the processor (202), the computed probability value with a threshold accuracy level allowed for the original website (112); and

determining, by the processor (202), if the target website (106) is a fake website based on the comparison.

12. The method (600) as claimed in claim 8, wherein the static website attributes comprise at least one of a domain name, a sub-domain name, a geo location Sub domain name, a geo location of Domain and sub domain registration, a geo location of hosted IP address for domain / subdomain URL, a SSL certificate validity date dates, a SSL certificate algorithm

type, a Domain / sub-domain SSL status, a Serial number of SSL certificate, a SSL certificate public key, Domain provider details.

13. The method (600) as claimed in claim 8, wherein the dynamic website attributes comprise at least one of a page content and check sum of the URL, email id, contact number, social media handle present in the website a Logo and signed logo if applicable, a Domain, sub-domain and URL from black-list and white listed table lookup, a Purpose of the URL received by end user – financial, privacy, KYC, education, sales, marketing, Government, a domain / subdomain and URL look up from 3rd party risk register, a Domain / subdomain and URL lookup from Government risk register, a Mechanism of URL redirection applied, a Response time of the URL, a Route to access the URL, a Number of hops to reach URL, a Regulatory status and response to access the URL, an Information type the URL is accessing, a Lookup from system created black list and white listed domain / sub domain and URLs, a Configurable business rules provided by original website owner (316).

14. The method (600) as claimed in claim 8, wherein generating the validation report for the website URL based on results of validation comprises:

generating, by the processor (202), one or more AI-driven insights for the target website (106) based on the results of validation; and

generating, by the processor (202), the validation report for the website URL, wherein the validation report comprises the generated one or more AI-driven insights, one or more issues associated with the target website, root causes for the one or more issues and recommendations for resolving the one or more issues.

15. The method (600) as claimed in claim 8, further comprising:

verifying, by the processor (202), the results of validation using a blockchain network system comprising one or more authorized expert block nodes;

determining, by the processor (202), whether the target website (106) belongs to a critical cyber attack based on the verification;

generating, by the processor (202), emergency messages comprising information associated with the target website (106) and the type of critical cyber-attack determined; and

broadcasting, by the processor (202), the generated emergency messages to one or more authorities using a communication network (104).