(12) PATENT APPLICATION PUBLICATION
(19) INDIA
(22) Date of filing of Application :09/08/2023

(21) Application No.202311053444 A
(43) Publication Date : 01/09/2023

(54) Title of the invention : PREFIX DOMAIN MATCHING FOR ANTI-PHISHING PATTERN MATCHING SYSTEM

| | |
|---|---|
| (51) International classification | :H04L0051000000, G06F0021560000, H04L0067020000, H04L0061451100, G06Q0010100000 |
| (86) International Application No<br>Filing Date | :NA<br>:NA |
| (87) International Publication No | : NA |
| (61) Patent of Addition to Application Number<br>Filing Date | :NA<br>:NA |
| (62) Divisional to Application Number<br>Filing Date | :NA<br>:NA |

(71)**Name of Applicant :**
**1)Chitkara University**
Address of Applicant :Chitkara University, Chandigarh-Patiala National Highway, Village Jhansla, Rajpura, Punjab - 140401, India. Patiala ---------- ----------
**2)Bluest Mettle Solutions Private Limited**
**Name of Applicant : NA**
**Address of Applicant : NA**
(72)**Name of Inventor :**
**1)MISHRA, Rahul**
Address of Applicant :ODC-4, Panchshil Tech Park, inside Courtyard by Marriott premises, Hinjewadi Phase - 1, Pune - 411057, Maharashtra, India. Pune ---------- ----------
**2)SINGH, Dhiraj**
Address of Applicant :ODC-4, Panchshil Tech Park, inside Courtyard by Marriott premises, Hinjewadi Phase - 1, Pune - 411057, Maharashtra, India. Pune ---------- ----------
**3)MANTRI, Archana**
Address of Applicant :Chitkara University, Chandigarh-Patiala National Highway, Village Jhansla, Rajpura, Punjab - 140401, India. Patiala ---------- ----------

(57) Abstract :
The anti-phishing system (100) consists of several components that collaborate to identify and prevent phishing attempts. The blocklist database (102) stores information about identified phishing URLs, including details such as the URL itself, identification timestamps, and associated metadata. It can be located at the email server (104), client device (106), or a remote server. The email server (104) manages email communications and may include filtering mechanisms to detect potential phishing emails. The client devices (106) receive and filter emails, while the network facilitates communication between the email server, client devices, and the blocklist database. The matching engine (110) is responsible for comparing the domain name of a URL with the list of known legitimate domain names database, determining potential phishing URLs. The system (100) maintains a database of known legitimate domain names (112), which serves as a reference for the matching engine to verify the legitimacy of URLs. Together, these components work in harmony to protect users from accessing malicious URLs and mitigate the risks associated with phishing attacks.

No. of Pages : 22 No. of Claims : 10