(12) PATENT APPLICATION PUBLICATION
(19) INDIA
(22) Date of filing of Application :01/08/2023

(21) Application No.202311051689 A
(43) Publication Date : 01/09/2023

(54) Title of the invention : SYSTEM FOR RESEARCHING HASH FUNCTION VULNERABILITY INDEX AND HASH CHAIN ATTACKS

(51) International classification	:G06F0021570000, H04L0009320000, H04L0009060000, G06F0021550000, G06Q0010060000
(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)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)PANDEY, Sakshi
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 present disclosure relates to a system (100) that offers a comprehensive and dynamic platform for evaluating the vulnerabilities of hash functions and analysing the risks associated with hash chain constructions. This system (100) introduces a quantitative vulnerability metric, the Hash Function Vulnerability Index (HFVI), to assess the relative security of hash functions. By considering multiple factors, including known vulnerabilities, attack techniques, and mathematical properties, the system provides a comprehensive evaluation framework. It employs realistic attack scenario modeling to simulate practical exploit scenarios and quantify the effectiveness of hash chain attacks. The system (100) is designed to adapt and evolve, integrating new research findings and fostering collaboration within the cryptographic community. Through its capabilities in visualization, reporting, and customizable evaluation criteria, the system (100) facilitates informed decision-making and aids in enhancing the overall security of cryptographic systems.

No. of Pages : 28 No. of Claims : 10