US011218304B2

(12) **United States Patent**
**Lurey et al.**

(10) **Patent No.: US 11,218,304 B2**
(45) **Date of Patent: Jan. 4, 2022**

(54) **SYSTEM AND METHOD FOR DETECTING BREACHED PASSWORDS WITHOUT DISCLOSING IDENTIFIABLE INFORMATION**

(71) Applicant: **Keeper Security, Inc.**, Chicago, IL (US)

(72) Inventors: **Craig B. Lurey**, Chicago, IL (US); **Darren S. Guccione**, Chicago, IL (US)

(73) Assignee: **KEEPER SECURITY, INC.**, Chicago, IL (US)

( * ) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 147 days.

(21) Appl. No.: **16/578,854**

(22) Filed: **Sep. 23, 2019**

(65) **Prior Publication Data**

US 2021/0091938 A1 Mar. 25, 2021

(51) **Int. Cl.**

| | |
|---|---|
| ***H04L 9/08*** | (2006.01) |
| ***H04L 9/32*** | (2006.01) |
| ***G06F 21/60*** | (2013.01) |

(52) **U.S. Cl.**

CPC ..... ***H04L 9/0863*** (2013.01); ***G06F 21/602*** (2013.01); ***H04L 9/0869*** (2013.01); ***H04L 9/3242*** (2013.01)

(58) **Field of Classification Search**

CPC ... H04L 9/0863; H04L 9/0869; H04L 9/3242; H04L 63/00; H04L 2209/42; H04L 9/0897; H04L 9/3218; H04L 63/14667; H04L 63/083; H04L 63/06; H04L 63/10; H04L 29/06; H04L 63/0421; H04L 63/1466; G06F 21/602; G06F 21/45

See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

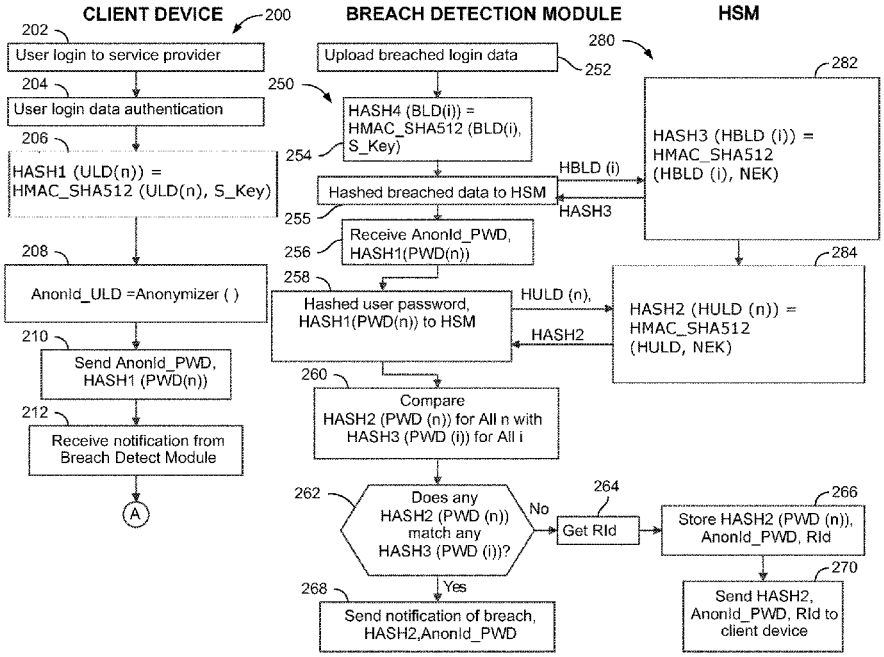
| | | | | |
|---|---|---|---|---|
| 2003/0200437 | A1* | 10/2003 | Oishi | H04L 9/3013 713/175 |
| 2010/0199098 | A1* | 8/2010 | King | H04L 9/0866 713/182 |
| 2013/0238496 | A1* | 9/2013 | Monster | G06Q 20/06 705/40 |
| 2018/0205757 | A1* | 7/2018 | Versteeg | H04L 63/1466 |
| 2018/0288050 | A1* | 10/2018 | Chen | H04W 12/08 |
| 2019/0229909 | A1* | 7/2019 | Patel | H04L 63/102 |

* cited by examiner

*Primary Examiner* — J. Brant Murphy

(74) *Attorney, Agent, or Firm* — Klintworth & Rozenblat IP LLP

(57) **ABSTRACT**

Systems and methods for detecting breached user login records in a zero-knowledge architecture. A breach detection module obtains login data that has been breached from breached data sources and service providers. The breached data is hashed with a system key and the breached data hashes are hashed in a hardware security module (HSM) using a hashing method and a non-exportable key. Clients provide user login data that has been hashed using the hashing method by the client device to the breach detection module. The breach detection module hashes the hashed user login data and compares the hashed user login hashes with the hashed breached data hashes and sends a breach alert to the client device if any hashes match.

**19 Claims, 7 Drawing Sheets**