



US011663146B2

(12) **United States Patent**  
**Simmons**

(10) **Patent No.:** **US 11,663,146 B2**  
(45) **Date of Patent:** **May 30, 2023**

(54) **SECURITY OF EMBEDDED DEVICES  
THROUGH A DEVICE LIFECYCLE WITH A  
DEVICE IDENTIFIER**

(56) **References Cited**

U.S. PATENT DOCUMENTS

(71) Applicant: **Microchip Technology Incorporated,**  
Chandler, AZ (US)

2006/0131743 A1 \* 6/2006 Erickson ..... G06F 21/71  
257/737  
2013/0339734 A1 \* 12/2013 Vernia ..... H04L 63/0428  
713/168

(72) Inventor: **Michael Simmons,** Chandler, AZ (US)

2018/0097639 A1 4/2018 Gulati et al.  
2019/0007212 A1 1/2019 Neve de Mevergnies et al.  
2020/0085105 A1 \* 3/2020 Barbaric ..... G06F 16/9554  
2021/0150165 A1 \* 5/2021 Sturgill ..... G06Q 10/0833

(73) Assignee: **Microchip Technology Incorporated,**  
Chandler, AZ (US)

(\*) Notice: Subject to any disclaimer, the term of this  
patent is extended or adjusted under 35  
U.S.C. 154(b) by 509 days.

OTHER PUBLICATIONS

(21) Appl. No.: **16/806,227**

(22) Filed: **Mar. 2, 2020**

Lesjak, Christian, et al. "A secure hardware module and system  
concept for local and remote industrial embedded system identification."  
Proceedings of the 2014 IEEE Emerging Technology and Factory  
Automation (ETFA). IEEE, 2014. (Year: 2014).  
International Search Report and Written Opinion, Application No.  
PCT/US2020/024854, 11 pages, dated Jul. 7, 2020.

(65) **Prior Publication Data**

US 2020/0409869 A1 Dec. 31, 2020

\* cited by examiner

*Primary Examiner* — Nicholas J Simonetti

(74) *Attorney, Agent, or Firm* — Slayden Grubert Beard  
PLLC

**Related U.S. Application Data**

(60) Provisional application No. 62/867,552, filed on Jun.  
27, 2019.

(51) **Int. Cl.**  
**G06F 12/14** (2006.01)  
**G06F 3/06** (2006.01)

(52) **U.S. Cl.**  
CPC ..... **G06F 12/1416** (2013.01); **G06F 3/0616**  
(2013.01); **G06F 3/0653** (2013.01); **G06F**  
**3/0659** (2013.01); **G06F 3/0679** (2013.01)

(58) **Field of Classification Search**  
CPC .. G06F 12/1416; G06F 3/0616; G06F 3/0653;  
G06F 3/0659; G06F 3/0679  
See application file for complete search history.

**ABSTRACT**

(57) An apparatus includes a database with device profiles, and  
a device programmer. The device programmer includes  
instructions. The instructions, when read and executed by a  
processor, cause the device programmer to identify a device  
identifier of an electronic device. The device programmer is  
further caused to, based upon the device identifier, access  
device data from the database. The device programmer is  
further caused to, based upon the device data, determine an  
area of memory of the electronic device that can be written.  
The device programmer is further caused to, based on the  
determination of the area of memory of the electronic device  
that can be written, write data to the area of memory.

**21 Claims, 4 Drawing Sheets**

