(12) PATENT APPLICATION PUBLICATION
(19) INDIA
(22) Date of filing of Application :28/05/2021

(21) Application No.202121023839 A
(43) Publication Date : 02/07/2021

(54) Title of the invention : SMARTMON: MONITORING THE STATUS OF SMART DEVICES VIA NETWORK TRAFFIC

(51) International classification	:H04L0029060000, H04L0029080000, G05B0019418000, G05B0015020000, G06F0021560000
(31) Priority Document No	:NA
(32) Priority Date	:NA
(33) Name of priority country	:NA
(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)Dr. G. Murugan
Address of Applicant :Professor in Computer Engineering, St. John College of Engineering and Management, Vevoor, Manor Road, Palghar (E), Palghar, India Maharashtra India
2)Keerthipati Kumar
3)Dr. Manas Ranjan Nayak
4)Mr. Sidhanta Kumar Balabantary
5)Mr. Walunj Madhukar Baban
6)Dr. Nilesh Parihar
7)Mr. Amit kumar Sharma
8)Dr. A. V. Sudhakara Reddy
9)Dr. Harikumar Pallathadka
10)Dr. Sushma Jaiswal
11)r. Sankararao Majji
12)Kaviyaraj R
(72)**Name of Inventor :**
1)Dr. G. Murugan
2)Keerthipati Kumar
3)Dr. Manas Ranjan Nayak
4)Mr. Sidhanta Kumar Balabantary
5)Mr. Walunj Madhukar Baban
6)Dr. Nilesh Parihar
7)Mr. Amit kumar Sharma
8)Dr. A. V. Sudhakara Reddy
9)Dr. Harikumar Pallathadka
10)Dr. Sushma Jaiswal
11)r. Sankararao Majji
12)Kaviyaraj R

(57) Abstract :
The rapid growth of the IoT has led to unprecedented changes in our everyday lives. Among other things, the most common smart home technologies. They create a connected network in which automation is used to improve system Interoperability. In your home environment they use different devices. This type of automation typically runs on platforms that device providers including Samsung, Google and Amazon offer. But, because of malware, unknown applications by third party, and possibly lateral attacks, back-end cloud cannot always be trustworthy. For IoT platforms, in particular, two security threats can be identified which could gain unauthorized control of smart home devices. This thesis shows SmartMon, a framework which detects such violations of security by statically analysing the control logic and parking them with a dynamic execution pattern (SmartApp).

No. of Pages : 6 No. of Claims : 7

SMARTMON: MONITORING THE STATUS OF SMART DEVICES VIA NETWORK TRAFFIC

Abstract:

The rapid growth of the IoT has led to unprecedented changes in our everyday lives. Among other things, the most common smart home technologies. They create a connected network in which automation is used to improve system Interoperability. In your home environment they use different devices. This type of automation typically runs on platforms that device providers including Samsung, Google and Amazon offer. But, because of malware, unknown applications by third party, and possibly lateral attacks, back-end cloud cannot always be trustworthy. For IoT platforms, in particular, two security threats can be identified which could gain unauthorized control of smart home devices. This thesis shows SmartMon, a framework which detects such violations of security by statically analysing the control logic and parking them with a dynamic execution pattern (SmartApp).

Field of innovation:

In order to validate IoT device status and to detect misconduct, We have developed SmartMon. In comparison to previous studies, we ensure that our method is both reliable and minimally inviolate. And we use multiple sources, rather than single sources, to validate and forecast the design, which provides a more accurate result.

Background Art:

Samsung Smart Things is one of the largest and most user platforms with the integration of services from third parties among many IoT platforms. Things Smart are made up of three main components: the backend cloud of SmartThings, the smartphone application of SmartThings and the hub of SmartThings. In SmartThings platform, the IoT applications are called SmartApps and are groovy-built in SmartThings IDE. These SmartApps allow users to control and track their home devices according to their own applications. IoT app cannot run on smartphones directly because of its limited computing capability. Instead, SmartApps work on the cloud platform of SmartThing.

The iot smart app is performed in a sandbox that ensures the protection of the SmartApp. For security concerns, the groovy sandbox environment deactivates some of the features of the object-oriented language. For instance, a new class or library cannot be initialized but a user is allowed to write its own function and define its own variables. The SmartApp also provides an API which is secured by Oauth-based authentication to meet HTTP requests of the external application. A method can be invoked by supplying its name as a string parameter by supporting dynamic method in vocational process that is close to other programming languages like Java.

Objective:

Our aim is to assess whether the status of a clever device is real, whether it occurred as described by the app functionality and apply my Chinese learning model further to predict the

status of the device and device based upon collected data. Since this paper focuses on clarifying and handling smart home-based application-level problems, we believe that our model contains no compromise on other components. For instance, another attack type like attacks on SmartThings hardware, like the DNS re-binding attacks described in the article, which attackers use to exploit the browser and plug-ins for a large-scale DNS re-bind attack. Another case not listed in this article is that attackers use only cheap device-based attacks to submit requests for leaked data from a distance of around meters. Also in our architecture there is no web-based attachment to the smart cloud or specific platform.

Summary of Innovation:

We are presenting an IoT event detector to detect misbehavior and malware inside Samsung's SmartThings setting. There are three elements of the IoT Event Detector: the DFA construction module, a Travel Collection module, and the Misbehavior Detection module. Each module functions individually and functions together with a united system with high precision and performance. The DFA Building Module performs the analysis functions of SmartApps source code by static analysis and extractions of DFA (Control Logic) from SmartAppps. In real time, Smart Device data are collected from the Traffic Collection module. The SmartApp module, written in groovy, activates all Smart Devices installed, monitors their status and, in the event of a specific event, sends out their status via a given API. Misbehavior Detection module is on the Gateway and Smart Devices data is concurrently receiving, validating it with a permission list and creating validation results from our Traffic Collection Module and cloud server.

Decryption:

After we analyze and know the source code logic of SmartApps, we are now focused on acquiring and transmitting data at the same time as the system status changes. The monitors program in this section is running on the Smart Things cloud and the system type configuration of raspberry pi should be first designed to facilitate the functionality of this application. System Design has its own system style handler on the Samsung SmartThing platform that sets out its functionality and capabilities. We found that SmartThings cloud offers an API for sending commands to specific IP addresses by obtaining or putting http requests in other handlers of device sort. However, SmartThings cloud doesn't support the rasp berry pi officially, the raspberry pi system manager is not available. Afterwards, we write our own raspberry pi system type handlers in 252 groovy locks in accordance with the basic logic of the device type handler. We allow switching levels, color control, color temperature and refresh capability for raspberry pi in this device form handling device. Color Temperature is the feature we apply for sending system data as it will send http-placed request containing all the detailed information in the monitoring application, via the Set Color process. The Switch Level and Switch features the ability to regulate the opening and closed status. We initialize the Hub Action object within the Set Color method, which is an object that handles various data and sends SmartThings hub commands, and defines the Put, Path and data body method. With this Hub Action object, we can send SmartThings data to raspberry platform.

Claims:

We claim,

1. We introduce SmartMon as a malfunctioning detection device to detect misconductions such as event spoofing or privileges in SmartApps for the Samsung SmartThings Framework.
2. Our SmartMon enables smart device status to be inferred and validated and analyzed in real time.
3. SmartMon includes a DFA construction, traffic collection, malfunctioning, and event prediction module.
4. SmartMon includes main components.
5. The build module DFA can expert SmartApp logic successfully from source code through a solid-precision static analysis.
6. The traffic collection module snaps the status of smart devices via SmartApp monitor and transfers data in real time to the misconduct sensing module.
7. Misbehavior module is able to verify multiple source traffic collector system status and high performance event prediction module.

FORM 1
THE PATENTS ACT, 1970
(39 of 1970)
&
THE PATENTS RULES, 2003
APPLICATION FOR GRANT OF PATENT
[See sections 7,54 & 135 and rule 20(1)]

(FOR OFFICE USE ONLY)

Application No.: .....
Filing Date: .....
Amount of Fee Paid: .....
CBR No.: .....
Signature: .....

1. APPLICANT(S):

Sr.No.	Name	Nationality	Address	Country	State
1	Dr. G. Murugan	India	Professor in Computer Engineering, St. John College of Engineering and Management, Vevoor, Manor Road, Palghar (E), Palghar, India	India	Maharashtra
2	Keerthipati Kumar	India	Research Scholar VISTAS Chennai	India	Tamil Nadu
3	Dr. Manas Ranjan Nayak	India	Assistant professor, School of Computer Engineering, Kiit(DU), Bhubaneswar.	India	Orissa
4	Mr. Sidhanta Kumar Balabantary	India	Assistant Professor Gandhi Institute For Education & Technology, Baniatangi, Bhubaneswar, Khurda,	India	Orissa
5	Mr. Walunj Madhukar Baban	India	Assistant Professor Department Of Electronic Science Abasaheb Garware College karve Road, Pune	India	Maharashtra
6	Dr. Nilesh Parihar	India	Professor Department of ECE CLG CAMPUS, SUMERPUR, PALI, , JODHPUR	India	Rajasthan
7	Mr. Amit kumar Sharma	India	Assistant professor CSE PSITCOE/AKTU, Kanpur, UP, India	India	Uttar Pradesh
8	Dr. A. V. Sudhakara Reddy	India	Associate Professor Department of	India	Telangana

			EEE Malla Reddy Engineering College Secunderabad		
9	Dr. Harikumar Pallathadka	India	Director, Manipur International University, Imphal, Manipur, India	India	Manipur
10	Dr. Sushma Jaiswal	India	Assistant Professor, Department of Computer Science & Information Technology (CSIT), Guru Ghasidas Vishwavidyalaya (A Central University), Bilaspur	India	Chattisgarh
11	r. Sankararao Majji	India	Assistant Professor Department of ECE GRIET, Hyderabad	India	Telangana
12	Kaviyaraj R	India	Research Scholar Department of Computer Science and Engineering SRM IST	India	Tamil Nadu

2. INVENTOR(S):

Sr.No.	Name	Nationality	Address	Country	State
1	Dr. G. Murugan	India	Professor in Computer Engineering, St. John College of Engineering and Management, Vevoor, Manor Road, Palghar (E), Palghar, India	India	Maharashtra
2	Keerthipati Kumar	India	Research Scholar VISTAS Chennai	India	Tamil Nadu
3	Dr. Manas Ranjan Nayak	India	Assistant professor, School of Computer Engineering, Kiit(DU), Bhubaneswar.	India	Orissa
4	Mr. Sidhanta Kumar Balabantary	India	Assistant Professor Gandhi Institute For Education & Technology, Baniatangi, Bhubaneswar, Khurda,	India	Orissa

5	Mr. Walunj Madhukar Baban	India	Assistant Professor Department Of Electronic Science Abasaheb Garware College karve Road, Pune	India	Maharashtra
6	Dr. Nilesh Parihar	India	Professor Department of ECE CLG CAMPUS, SUMERPUR, PALI, , JODHPUR	India	Rajasthan
7	Mr. Amit kumar Sharma	India	Assistant professor CSE PSITCOE/AKTU, Kanpur, UP, India	India	Uttar Pradesh
8	Dr. A. V. Sudhakara Reddy	India	Associate Professor Department of EEE Malla Reddy Engineering College Secunderabad	India	Telangana
9	Dr. Harikumar Pallathadka	India	Director, Manipur International University, Imphal, Manipur, India	India	Manipur
10	Dr. Sushma Jaiswal	India	Assistant Professor, Department of Computer Science & Information Technology (CSIT), Guru Ghasidas Vishwavidyalaya (A Central University), Bilaspur	India	Chattisgarh
11	r. Sankararao Majji	India	Assistant Professor Department of ECE GRIET, Hyderabad	India	Telangana
12	Kaviyaraj R	India	Research Scholar Department of Computer Science and Engineering SRM IST	India	Tamil Nadu

3. TITLE OF THE INVENTION: SMARTMON: MONITORING THE STATUS OF SMART DEVICES VIA NETWORK TRAFFIC

4. ADDRESS FOR CORRESPONDENCE OF APPLICANT / AUTHORISED PATENT AGENT IN INDIA:

SRM Univeristy

Telephone No.:
Fax No.:
Mobile No: .....
E-mail: kaviyaraj.r@gmail.com

5. PRIORITY PARTICULARS OF THE APPLICATION(S) FILED IN CONVENTION COUNTRY:

Sr.No.	Country	Application Number	Filing Date	Name of the Applicant	Tilte of the Invention

6. PARTICULARS FOR FILING PATENT COOPERATION TREATY (PCT) NATIONAL PHASE APPLICATION:

International Application Number	International Filing Date as Allotted by the Receiving Office
PCT//	

7. PARTICULARS FOR FILING DIVISIONAL APPLICATION

Original (first) Application Number	Date of Filing of Original (first) Application

8. PARTICULARS FOR FILING PATENT OF ADDITION:

Main Application / Patent Number:	Date of Filing of Main Application

9. DECLARATIONS:

(i) Declaration by the inventor(s)

I/We ,Dr. G. Murugan,Keerthipati Kumar,Dr. Manas Ranjan Nayak,Mr. Sidhanta Kumar Balabantary,Mr. Walunj Madhukar Baban,Dr. Nilesh Parihar,Mr. Amit kumar Sharma,Dr. A. V. Sudhakara Reddy,Dr. Harikumar Pallathadka,Dr. Sushma Jaiswal,r. Sankararao Majji,Kaviyaraj R, is/are the true & first inventor(s) for this invention and declare that the applicant(s) herein is/are my/our assignee or legal representative.

(a) Date: 28/05/2021

(b) Signature(s) of the inventor(s): .....

(c) Name(s): Dr. G. Murugan,Keerthipati Kumar,Dr. Manas Ranjan Nayak,Mr. Sidhanta Kumar Balabantary,Mr. Walunj Madhukar Baban,Dr. Nilesh Parihar,Mr. Amit kumar Sharma,Dr. A. V. Sudhakara Reddy,Dr. Harikumar Pallathadka,Dr. Sushma Jaiswal,r. Sankararao Majji,Kaviyaraj R

(ii) Declaration by the applicant(s) in the convention country

I/We, the applicant(s) in the convention country declare that the applicant(s) herein is/are my/our assignee or legal representative.

(a) Date: 28/05/2021

(b) Signature(s) : .....

(c) Name(s) of the singnatory: Dr. G. Murugan,Keerthipati Kumar,Dr. Manas Ranjan Nayak,Mr. Sidhanta Kumar Balabantary,Mr. Walunj Madhukar Baban,Dr. Nilesh Parihar,Mr. Amit kumar Sharma,Dr. A. V. Sudhakara Reddy,Dr. Harikumar Pallathadka,Dr. Sushma Jaiswal,r. Sankararao Majji,Kaviyaraj R

(iii) Declaration by the applicant(s)

- **The Complete specification relationg to the invention is filed with this application.**
- **I am/We are, in the possession of the above mentioned invention.**
- **There is no lawful ground of objection to the grant of the Patent to me/us.**
- **I am/We are, the assignee or legal representative to true first inventors.**

10. FOLLOWING ARE THE ATTACHMENTS WITH THE APPLICATION:

Sr.	Document Description	FileName

I/We hereby declare that to the best of my/our knowledge, information and belief the fact and matters stated hering are correct and I/We request that a patent may be granted to me/us for the said invention.

Dated this(Final Payment Date): 28/05/2021

Signature: .....

Name: Kaviyaraj R

To The Controller of Patents

The Patent office at MUMBAI

This form is electronically generated.