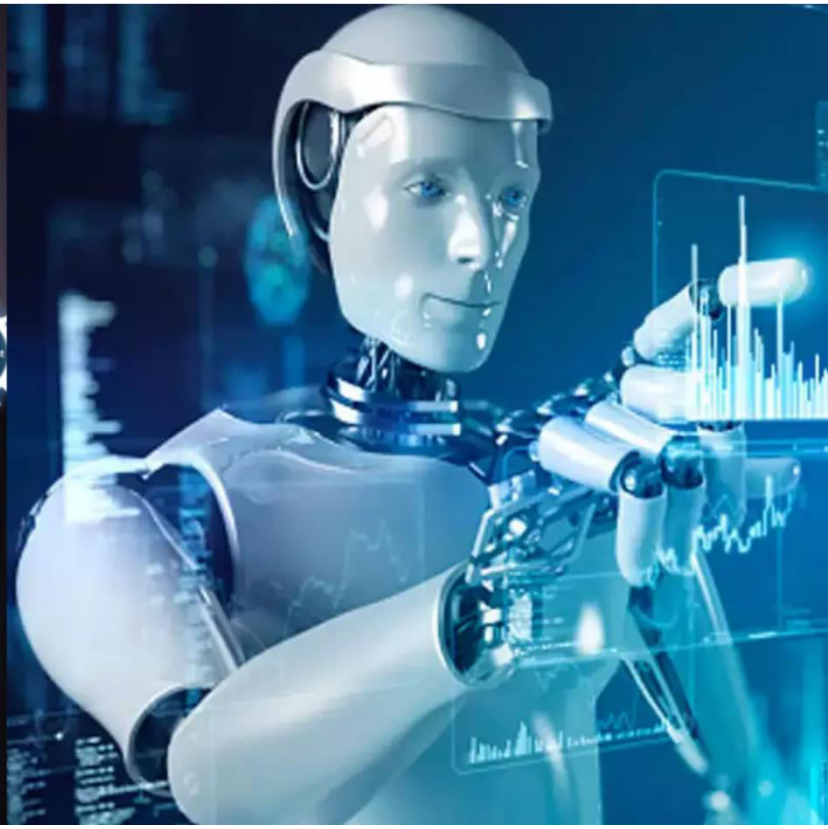
IJIRSET
International Journal of Innovative Research in Science | Engineering | Technology

ISSN(O): 2319-8753
ISSN(P): 2347-6710

International Journal of Innovative Research in Science Engineering and Technology (IJIRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.699

Volume 14, Issue 5, May 2025

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 5, May 2025

|DOI: 10.15680/IJIRSET.2025.1405198|

Leakage of Authorization-Data in IoT Device Sharing New Attacks and Countermeasures

K.Swathy, D.Viswanathan, Dr. S. Ranjithakumari

P G student, Department of Master of Computer Applications, MPNMJ Engineering College, Chennimalai, Erode, India

Associate Professor & HoD, Department of Computer Applications, MPNMJ Engineering College, Chennimalai,, Erode, India

Associate Professor, RVS College of Arts and Science, Coimbatore, India

ABSTRACT: Sharing among users is a common functionality in today's IoT clouds. Supporting device sharing are the delegation methods proposed by different IoT clouds, which we find are heterogeneous and ad-hoc — IoT clouds use various data(e.g., device ID, product ID, and access token) as authorization certificates. In this paper, we report the first systematic study on how the authorization-data are managed in IoT device sharing. Our study brought to light the security risks in today's IoT authorization-data management, identifying 6 authorization- data leakage flaws. To mitigate such flaws, we propose an approach to hide the authorization-data from the delegatee (the user authorized to access the devices) without disrupting the device sharing services. We propose SecHARE, an automated tool to patch the vulnerable IoT clouds. We applied SecHARE to 3 popular open-source IoT clouds. Results have shown the compatibility, effectiveness, and efficiency of SecHARE. We have made SecHARE publicly available.

KEYWORDS: Cyber-physical systems, IoT security, authorization-data protection.

I.INTRODUCTION

TODAY'S IoT (Internet of Things) cloud platforms are providing more and more functionalities to meet the users' various requirements. Device sharing among multiple users is one of the most popular functionalities supported by the main stream IoT clouds (e.g., AWS IoT[1], Samsung Smart Things, Philips Hue and MiHome). Device sharing allows the owner/admin-user to delegate the access right to the device to other users and clouds (which we call the delegatee). Prominent examples include that the owner of a Philips Hue device inviting other Philips users to control her device (by issuing a whitelistID for the delegatee user) and the owner of a Smart Things smart home authorizing Google Home cloud to control her device (by sending the device ID of the SmartThings device and an OAuthtokento Google Home cloud). Serving this purpose are the delegation mechanisms proposed by different IoT vendors, which we found are heterogeneous and ad-hoc. In specific, different IoT clouds use different types of data (e.g., deviceID, product ID, OAuth token) as the authorization certificates(which we call the authorization-data, see SectionIII).Also, different types of data are with different changeability, for example, the device ID (set when the device is created) is usually unchangeable, while access tokens are usually changeable (e.g., updated by the owner). Previous researches have revealed that vulnerabilities in these IoT delegation mechanisms could expose users to security and safety risks[5]. However, little have done to systematically study how the authorization-data are managed (e.g., creation, distribution, and deletion) in the real-world IoTclouds.

The Internet of Things is the next step in the evolution of communication and business(IoT). Real-world objects can create, receive, and exchange data in a seamless manner thanks to the Internet of Things. Several Internet of Things apps aim to automate processes and enable inanimate physical devices to work without human involvement. Existing and future IoT systems offer a lot of potential in terms of improving user comfort, efficiency, and automation. To integrate such a world in an ever-increasing way, high levels of security, privacy, authentication, and attack recovery are required. Every data flow is noted and managed by the user in the User-Console. If the data is not shareable it will Alert-To-User (ATU). Then the data is getting stored in the InterPlanetary File System (IPFS), the

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 5, May 2025

|DOI: 10.15680/IJIRSET.2025.1405198|

IPFS hash related to the data & logs will be stored in Blockchain. Using Smart contract the user can decide to share which data to respective third party.

II. LITERATURE SURVEY

IoT Cloud Architecture and Its Device Sharing Device control and its automation: A typical IoT architecture include the IoT devices, the cloud and the user console (e.g.,mobile app or web app). To control an IoT device, as shownin Fig.1, the device owner first register her device to the cloud, with the device bound to her user account. To access the device, the owner initiates a request through her user console. Upon receiving the request, the cloud performs an authorization check on the user and send the command to the target device if the check passes. Moreover, users can define automation rules(a.k.a., trigger-action rules) for automated device control —when receiving the trigger of the rule, the cloud automatically performs the action. For example, a user can set an automation rule to work in that if the motion sensor detects movement, turn-on the light.

Device types: There are three types of IoT devices:
(1) The end device, devices that connect to the IoTcloud directly and do not manage sub-devices;
(2) The gateway device, a gateway device connects to the IoT cloud directly and manages/connects to other sub-devices;
(3) The sub-devices, asub-device is managed by and connected to a gateway device.

For example, IoT clouds including HomeKit,MiHomeand SmartThingsenables the owner to invite other users to join the owner's smart home system and delegateaccess rights to the devices to the invited users. Cross-cloud device sharing: Cross-cloud delegationisalso commonly seen in today's IoT clouds for owners to share the devices with users from third-party clouds.

III. METHODOLOGY

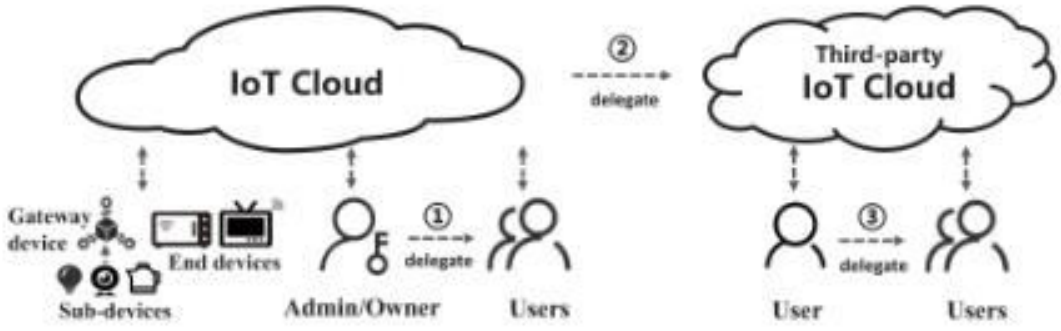


Fig. 1. IoT cloud architecture and its device sharing.

IV. SECURITY OF IOT AUTHORIZATION DATAMANAGEMENT

In this section, we report a security analysis on the man-agement of authorization-data in IoT device sharing of 6leading IoT clouds, including

1. ThingsBoard
2. Kaa Enterprise
3. Kaa open-source
4. JetLinks
5. ThingsKit

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 5, May 2025

|DOI: 10.15680/IJIRSET.2025.1405198|

6. ThingsPanel

A. Problem Scope and Threat Model

The owner can share her devices to other users under the same cloud of the owner or under third-party clouds. In this paper, we mainly focus on identifying and fixing the flaws in the former scenario. To this end, we defined two user roles in the IoT system, the administrator and the ordinary user. The administrator (e.g.,Airbnb host) is the owner or system admin-user who can delegateother ordinary users (e.g., babysitters, Airbnb guests and tenants)to access her IoT devices. The access of ordinary user is subject to revocation and expiry.. Moreover, we assume that the user is unable to tamper or decrypt data that was not originally intended for their authorized access. Authorization-Data Leakage Flaws Our goal is to systematically study the life-cycle of the authorization-data (e.g., generation, transmission, invalidation,etc.)

To thisend, we run the cloud-ends of the aforementioned 6 cloud platforms in our testing servers. We used the MQTTX[42]to simulate the devices supporting MQTT protocol and usedPostman,simulate the devices supporting HTTP. We then operated the simulated devices to communicate with the clouds and conducted different configurations/operations in the user consoles of the cloud platforms, simulating the real-world usage of controlling/managing devices. During such simulations, weused Wire shark to collect the traffic between the devicesand the cloud platforms. Then, we mainly checked whether thedata transmitted to the delegatee users is critical to authorization and whether we can use such data to gain unauthorized access even after revocation.

V. DATA LEAKAGE DETECTION IN IoT CLOUDS

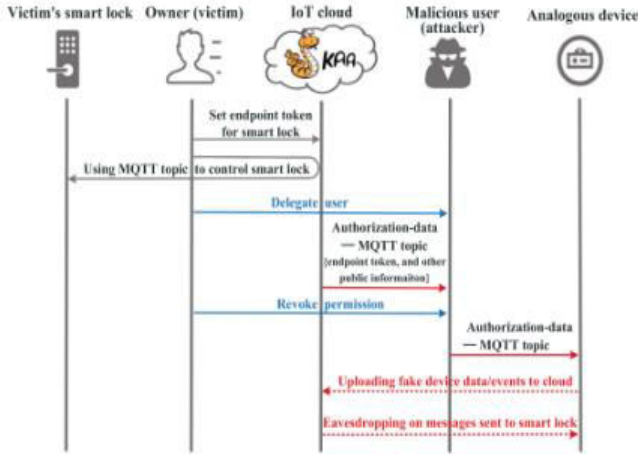


Fig. 2. Flaw 1 — MQTT topic leakage in Kaa Enterprise.

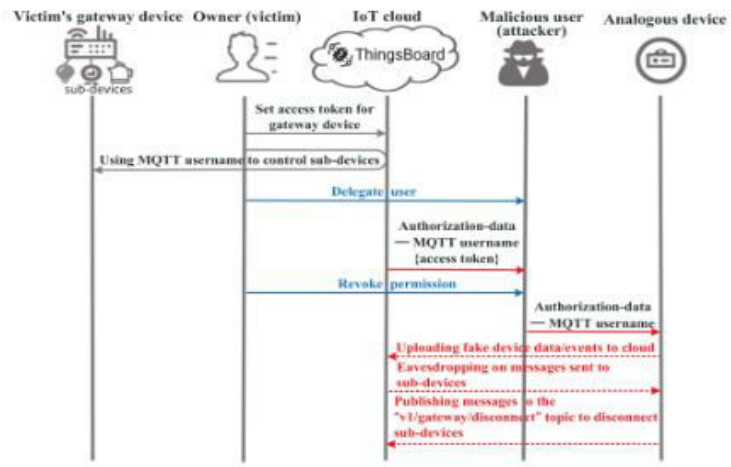


Fig. 3. Flaw 2 — MQTT username leakage in ThingsBoard.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 5, May 2025

|DOI: 10.15680/IJIRSET.2025.1405198|

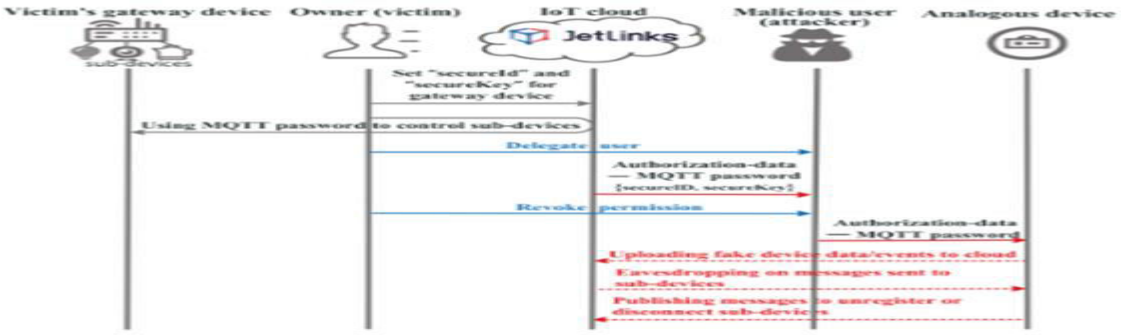


Fig. 4. Flaw 3 — MQTT password leakage in JetLinks.

Fig. 5. Flaw 4 — URL leakage in ThingsBoard and Kaa Enterprise.

VI. SECURITY AND EVALUATION

Implementation of SecHARE

The implementation of SecHARE as follows with its source codes released online.The configuration andCAG. As aforementioned, the configuration(provided by the user ofSecHARE)specifiesthe names of the variables/methods/functions related to the authorization-data. To help automatically generate thecon-figurationfile,CAGuses the QDox[46]to extract thedefinitions of the classes/interfaces/methods from the sourcecode and uses Spoon[47]to build the AST model. Note that,theconfigurationalso specifies the information neededto connect/access the database (e.g., the name of the database,the username and the password needed to connect the database),which is used to store the relationship between the authorization-data and shadow authorization-data.TheCO:Taking theconfigurationfile as input,COgen-erates theAop.xmlfile in the format required by AspectJ[48].TheAop.xmlfile would then be input to theDAA. Also, fromtheconfigurationfile,COextracts the names of relativevariables and methods/functions and sends them to thePG. Atlast,COsends the database-related parameters (e.g., databaseusername, password, etc.) toDO.TheDO: DOprovides generalized database operation APIs,supporting both SQL and NoSQL databases. Currently,DOsupports most SQL databases (a.k.a., Relational Database Management Systems) and the popular NoSQL database MongoDB. we create the SEC to include all the possible behaviors neededto insert/weave into the vulnerable IoT clouds. Specifically,we define code templates for data transferring, database read,database write and database deletion.

Then,PGlocates thevulnerable methods/functions in the original classes based onthe input fromCO, and automatically generates the patchingcodes using the templates in the SECTand the APIs provided by DO.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

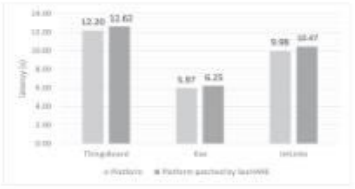
|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 5, May 2025

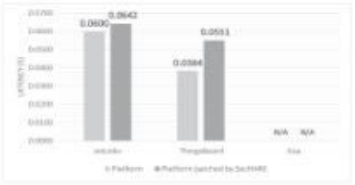
|DOI: 10.15680/IJIRSET.2025.1405198|

Example 1: Patching Sharedevice().

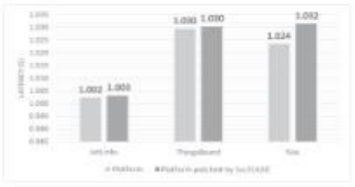
```
1  shareDevice (device, delegateeUser)  {
2      ...
3      deviceID = getDevice(device, delegateeUser);
4      sendToDelegateeUser(deviceID, delegateeUser);
5      ...
6  }
7
8  getDevice(device, delegateeUser)  {
9      ...
10     shadowData = generateShadowData(device.ID);
11     storeMapping(device.ID, shadowData,
   delegateeUser.ID);
12     return shadowData;
13     return device.ID;
14 }
```



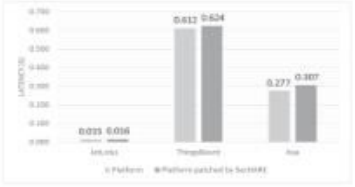
(a) system startup latency



(b) device creation latency



(c) device connection latency



(d) device control operation latency

VII. EVALUATION

A. The Impacts ofAuthorization

Data Leakage Prevalence of vulnerable authorization-data management:Bin et al.[5]identified several authorization-data leakage flaws in cross-cloud delegation, while we focused on the securityissues of authorization-data management within a single IoTcloud. As shown in TableI, we identified 6 new flaws with 3of them (Flaw 2, Flaw 4 and Flaw 5) affecting more than oneIoT cloud, which shows the prevalence of the authorization-dataleakage problem.

B. Performance Evaluation

Selecting IoT clouds for flaw identification:Since we focusedon the security issues in the IoT device sharing within a singlecloud, we only studied the clouds that support such functionalityand enforce access control mechanisms. Also, we prioritized thegeneral IoT clouds — the clouds can be applied to multiple IoTscenarios (e.g., smart home, smart city, smart energy, etc.). Atlast, we prioritized the clouds with better popularity — moreGitHub stars for the open-source clouds and more customers forthe commercial cloud

C. Selecting IoT platforms for defense evaluation

SecHAREfixes the flaws by patching the source codes of the clouds. Hence,we only evaluatedSecHAREupon the open-source clouds. Fur-ther, multiple programming languages (e.g., Java, Go, C++,C, etc.) are used to implement the open-source IoT cloud

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 5, May 2025

|DOI: 10.15680/IJIRSET.2025.1405198|

D. SecurityBenefit

As discussed in SectionIV, the attacker can leverage theleaked authorization-data to communicate with the cloud evenafter his access right is revoked. We evaluated whether theattacker can achieve that in the cloud that has been patched bySecHARE

VIII. CONCLUSION

In this paper, we systematically study how the authorization-data are managed in the real-world IoT device sharing and itssecurity implications. Our research reveals that authorization-data leakage is prevalent in the IoT clouds, with 6 flaws identifiedin 6 popular IoT clouds. To mitigate the problem, we proposedSecHAREto automatically patch the vulnerable codes of theIoT clouds. We appliedSecHAREto 3 open-source IoT clouds.Our evaluation shows thatSecHAREis easy to use by the IoTvendors, effective and efficient in securing authorization-data.Our new understanding and new techniques will provide betterprotection for today's IoT cloud platforms, as well as those tobe built in the years to come.

REFERENCES

[1] "AWS IoT," 2023. Accessed: Mar. 2023. [Online]. Available:https://aws.amazon.com/iot/
[2]SmartThings Samsung," 2023. Accessed: Mar. 2023. [Online]. Available:https://www.smartthings.com/
[3] "Philips HUE," 2023. Accessed: Mar. 2023. [Online]. Available: https://www2.meethue.com/
[4] "MiHome," 2023. Accessed: Mar. 2023. [Online]. Available: https://xiaomi-mi.com/mi-smart-home/
[5] B. Yuan et al., "Shattered chain of trust: Understanding security risks incross-cloud IoT access delegation," inProc. 29th USENIX Secur. Symp.,2020, pp. 1183–1200.
[6] "OAuth 2.0," 2023. Accessed: Mar. 2023. [Online]. Available: https://oauth.net/2/
[7] Z. B. Celik et al., "Sensitive information tracking in commodity IoT," inProc. 27th USENIX Secur. Symp., 2018, pp. 1687–1704.
[8]Y. Sameshima and P. T. Kirstein, "Authorization with security attributesand privilege delegation: Access control beyond the ACL,"Comput. Com-mun., vol. 20, no. 5, pp. 376–384, 1997.
[9] E. Fernandes, J. Jung, and A. Prakash, "Security analysis of emergingsmart home applications," inProc. IEEE 37th Symp. Secur. Privacy, 2016,pp. 636–654.
[10] E. Fernandes, A. Rahmati, J. Jung, and A. Prakash, "Decentralized actionintegrity for trigger-action IoT platforms," inProc. 25th Annu. Netw.Distrib. Syst. Secur. Symp., 2018.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details