Better Safe than Sorry: Uncovering the Insecure Resource Management in App-in-App Cloud Services

Yizhe Shi, Zhemin Yang, Dingyi Liu,
Kangwei Zhong, Jiarun Dai, and Min Yang

Fudan University

App-in-App Ecosystem

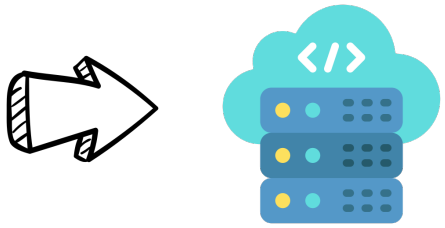
“Mini-apps in Super-apps”

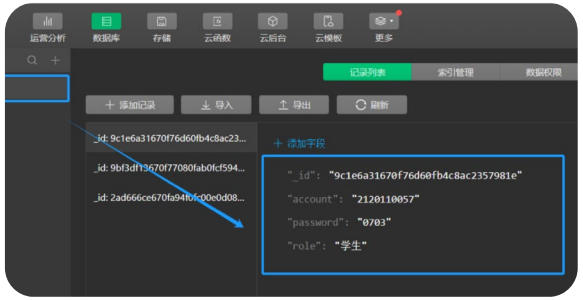
- Mini-app
  - Bring rich content and services
  - Native-app like experience
- Super-app: **“OS-like” role**
  - Provide sensitive resources
  - Manage mini-app lifecycle
  - Guarantee mini-app security

App-in-App Cloud Service

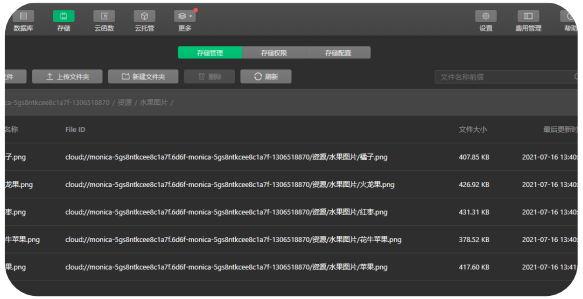
- **App-in-App Cloud Service**
  - **Serverless environment**
  - Simplify resource management for mini-app developers
  - Cloud database, cloud storage, cloud function

Mini-apps





Cloud database

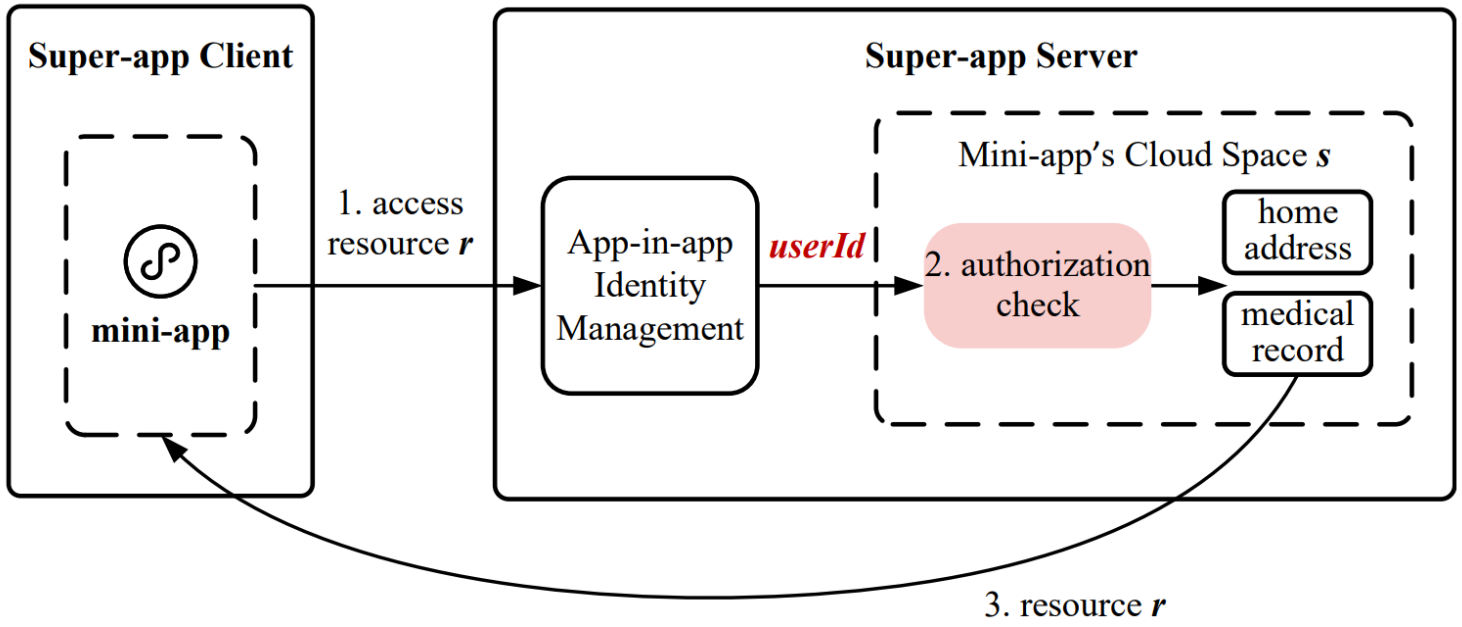


Cloud storage

App-in-App Cloud Service

- Security Mechanism: **Centralized User Identity-based Resource Control**
  - Authentication (Super-apps) + Authorization (Mini-apps)

The security responsibility is delegated to mini-app developers



Security Issues

- **Insecure Cloud Resource Management (ICREM):**
  - Mini-app developers adopt flawed practices when implementing user identity checks or resource access control

- Flawed authorization on the cloud side
- Privileged resources/functionalities exposure
- …

```
var o = Date.parse(new Date());
console.log("current timestamp:" + o);
var t = a.IDCardPaths;
console.log(t), wx.cloud.uploadFile({
    cloudPath: "ruzhu/" + o + ".png",
    filePath: t[0],
    success: function(a) {
        console.log("IDCard", a.fileID), e.setData({
            img: e.data.img.concat(a.fileID)
        });
    }
});
```

certificate exposure

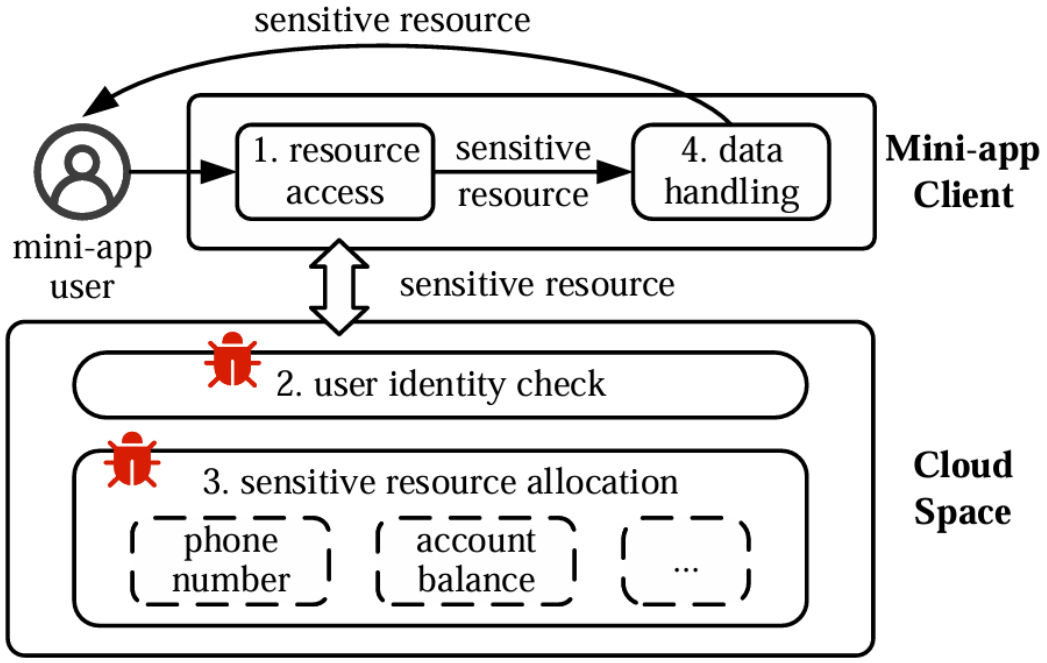
```
wx.cloud.callFunction({
    name: "getapikey",
    data: {
        apikeyname: "newkey"
    }
}).then(function(d) {
    var c = d.result.apikey;
    console.log("-----参与判断的usageCount值-----", i), i > 0 ? wx.request({
        url: "https://openaiapi-openapi-ofemoqcrtc.us-east-1.fcapp.run/v1/chat/
        completions",
        timeout: 18e4,
        data: {
            model: "gpt-3.5-turbo",
            messages: n,
            temperature: .7,
            max_tokens: 1e3
```

ChatGPT API Key

secret exposure

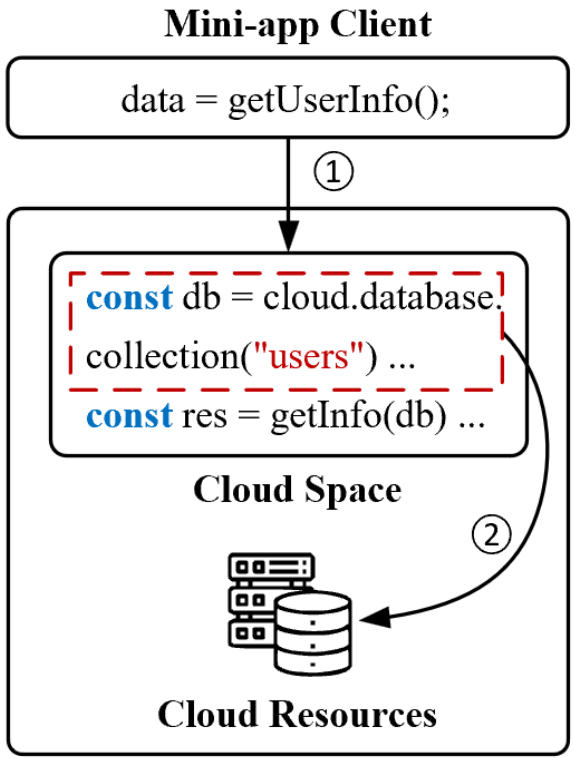
Decoding the Security Issues

- Key Stages in Cloud Resource Management
  - User Identity Check (UIC)
    - UIC-1: misplaced identity check
    - UIC-2: client-side parameter-based check
  - Sensitive Resource Allocation (SRA)
    - SRA-1: privileged resource exposure
    - SRA-2: excessive permission granting



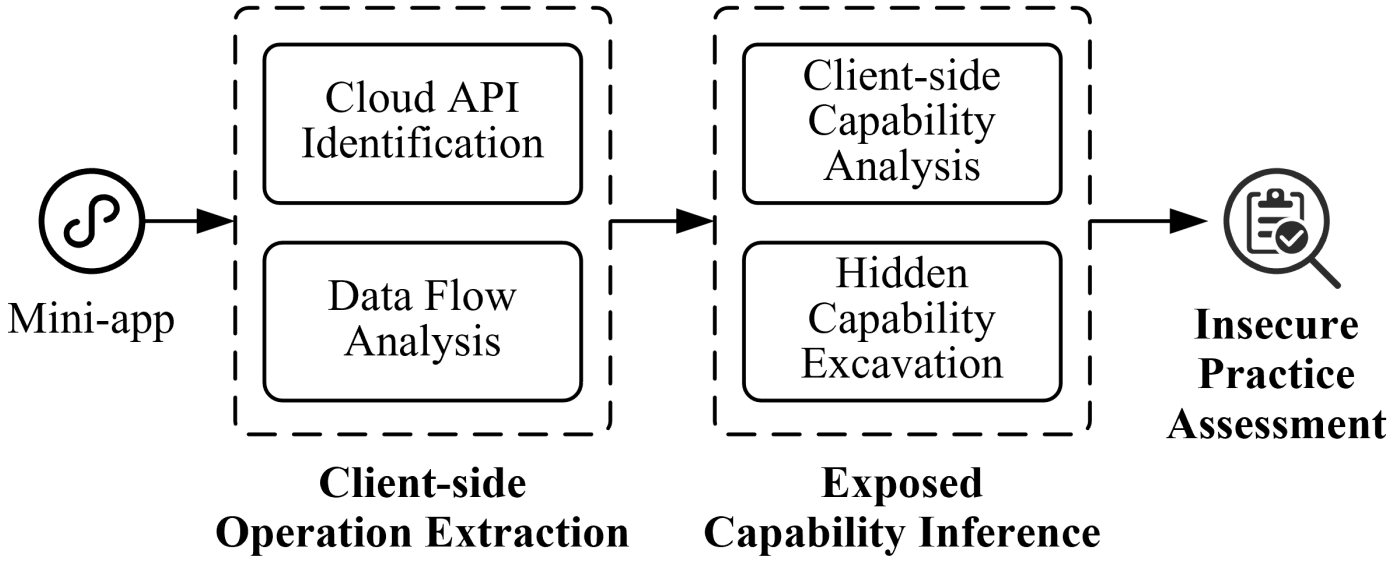
Challenge & Insight

- Challenges
  - Cloud-side code and resources are out of reach
  - Hard to avoid sensitive resource leakage during assessment
- Main Insights
  - Leverage client-side operations to uncover the potential cloud operations and resources
  - Zero-leakage dynamic probing based on the access state



Architecture

- **ICREMiner**
  - Phase #1: Client-side Operation Extraction
  - Phase #2: Exposed Capability Inference
  - Phase #3: Insecure Practice Assessment



Client-side Operation Extraction

- Client-side Operation Extraction
  - Locate cloud APIs and extract data dependencies to recover the mini-app behaviors

A

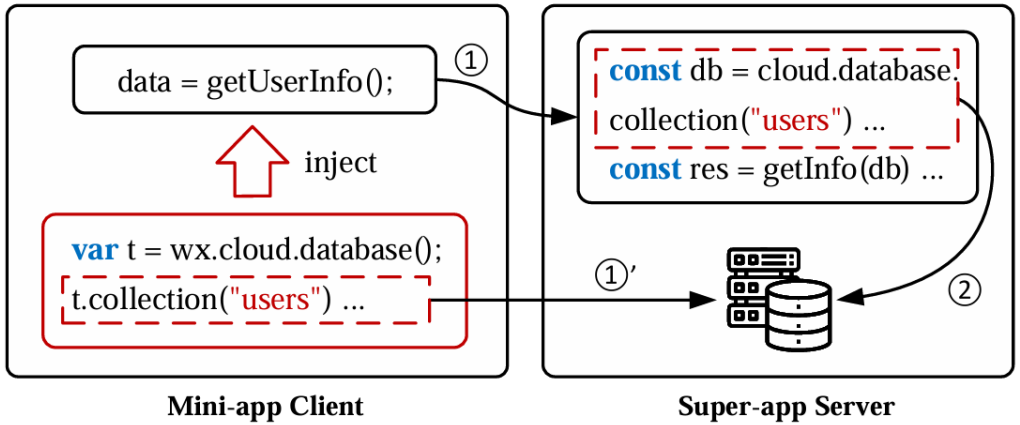
```
1  var t = wx.cloud.database({});
2  t.collection("users").where({
3    _openid: this.data.openid
4  }).get({
5    success: function(o) {
6      t.setData({
7        name: o.data.name,
8        gender: o.data.gender
9      });
10   }
11 });
```

B

```
1  wx.cloud.callFunction({
2    name: "setVip",
3    data: {
4      openid: t,
5      vip: 1
6    },
7    success: function(e) {
8      t.setData({
9      bought_vip: e.vip_code})
10   }
11 });
```

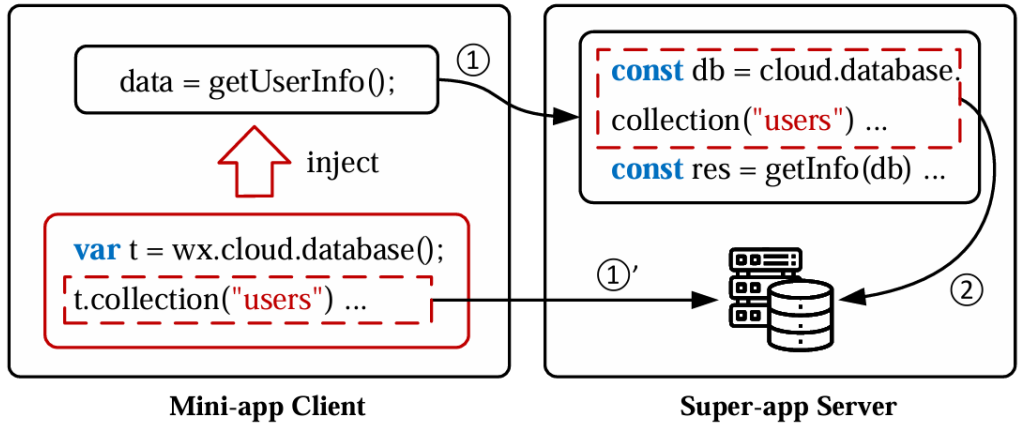
Exposed Capability Inference

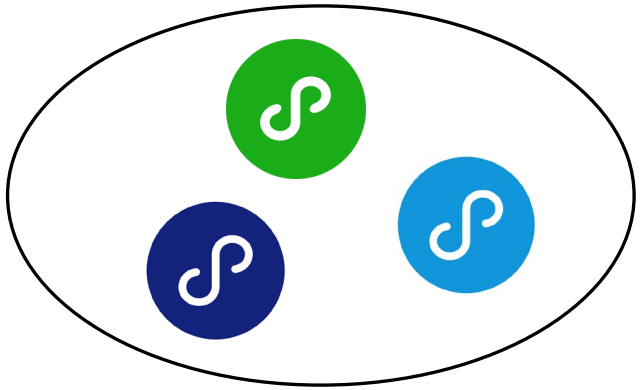
- **Hidden Capability:** Some cloud resources are not directly accessed in mini-app client



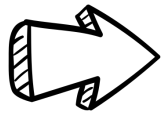
Exposed Capability Inference

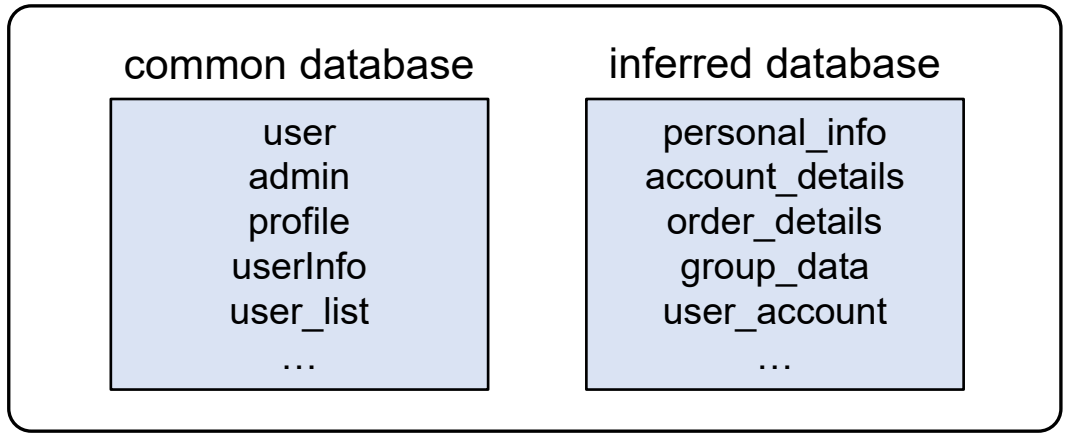
- **Hidden Capability:** Some cloud resources are not directly accessed in mini-app client
- Hidden Capability Excavation
  - Common Name Augmentation
  - LLM-based Inference
  - Mini-app Correlation





correlated mini-apps

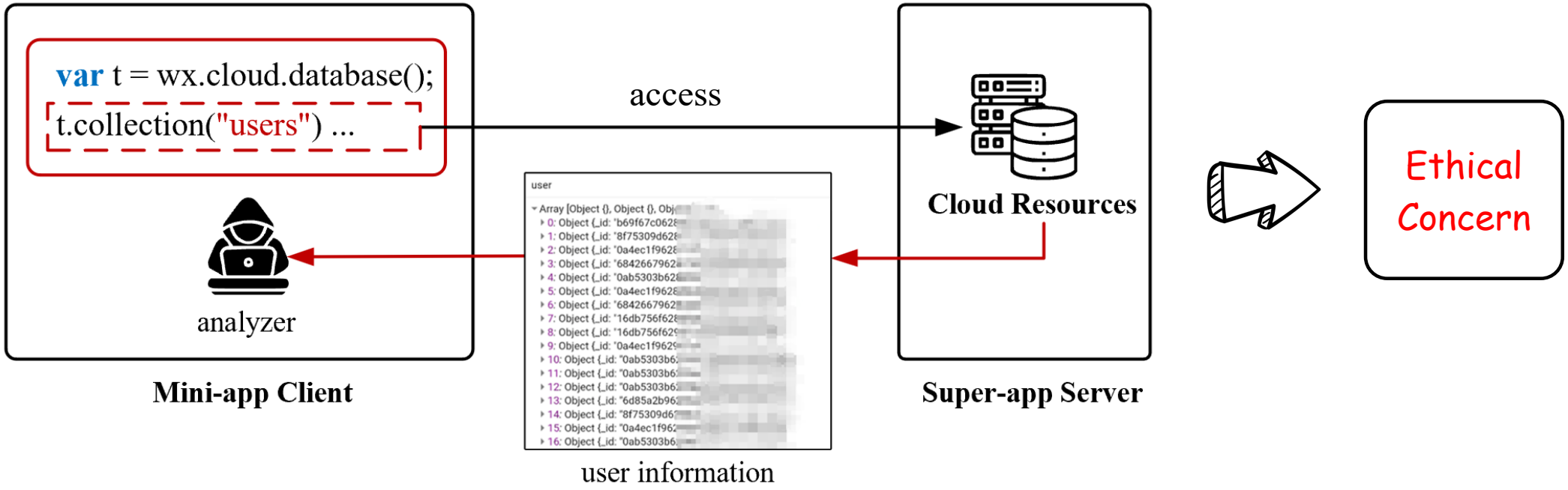




cloud space

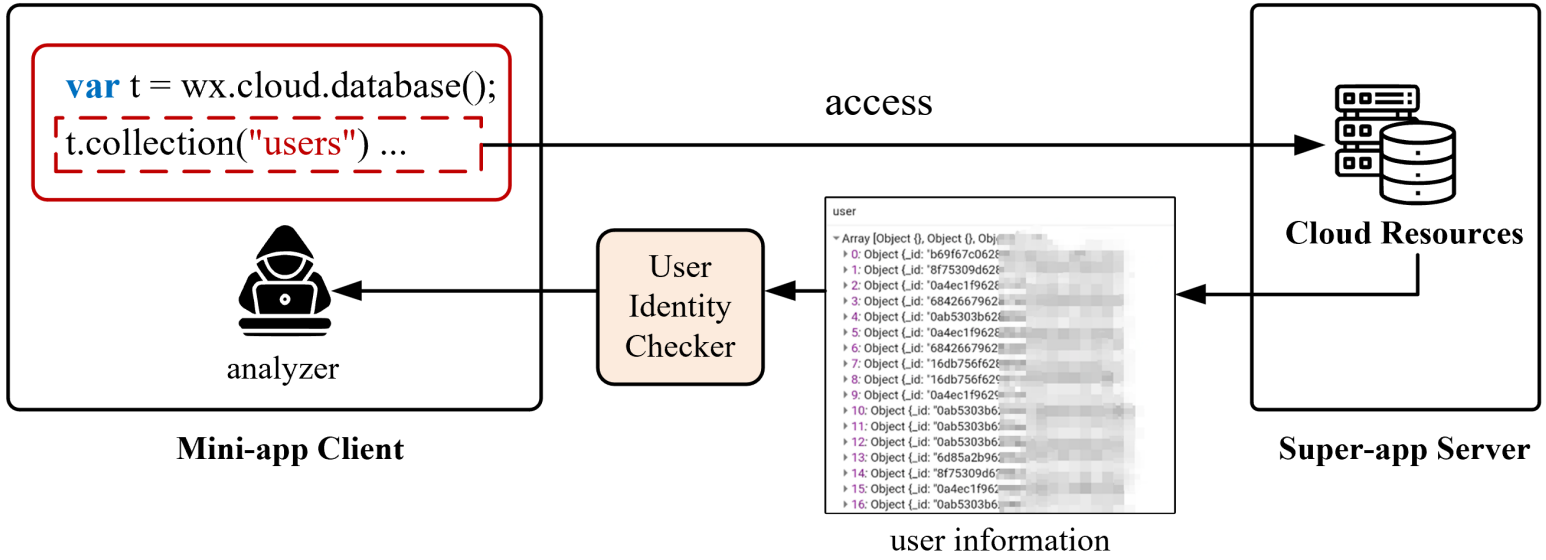
Insecure Practice Assessment

- **Principle: Mini-apps should not perform over-privileged operations (expose more-than-expected capabilities)**



Insecure Practice Assessment

- **Principle: Mini-apps should not perform over-privileged operations (expose more-than-expected capabilities)**
- Assessment of Cloud Database: Zero-leakage dynamic probing
  - Turn assessment to a binary judgement



Evaluation

- Dataset
  - Origin: 1,248,815 mini-apps
    - 985,503 WeChat mini-apps, 83,312 TikTok mini-apps, 93,128 Alipay mini-apps, 86,872 Baidu mini-apps
  - Filtered: 22,695 mini-apps
- Research Questions
  - RQ1: How many mini-apps are influenced by the ICREM risks in the wild?
  - RQ2: What real-world impacts are posed by ICREM risks?

Result Overview

- ICREMiner can effectively (97.26%) identify vulnerable mini-apps
- 2,815 mini-apps (12.40%) are affected by the insecure resource management
- The majority of vulnerable mini-apps are WeChat mini-apps

Super -app	Cloud Database		Cloud Storage		Cloud Routine	
	# app	% total	# app	% total	# app	% total
WeChat	2057	9.39%	673	3.07%	247	1.13%
TikTok	26	9.09%	10	3.50%	10	3.50%
Alipay	13	4.22%	15	4.87%	15	4.87%
Baidu	16	7.84%	11	5.39%	12	5.88%
Overall	2112	9.31%	709	3.12%	284	1.25%

Cloud Service	Preliminary Results			False Positives/Insensitive Operations			Sensitive Operations		
	# op	# app	% total	# op	# app	% op	# op	# app	% op
cloud database	6759	2133	9.45%	57	53	0.84%	6702	2112	99.16%
cloud storage	1147	1022	4.53%	124	103	10.81%	1023	709	89.19%
cloud routine	383	316	1.40%	46	42	12.01%	337	284	87.99%
Total	8289	3057	13.54%	227	197	2.74%	8062	2815	97.26%

Result Overview

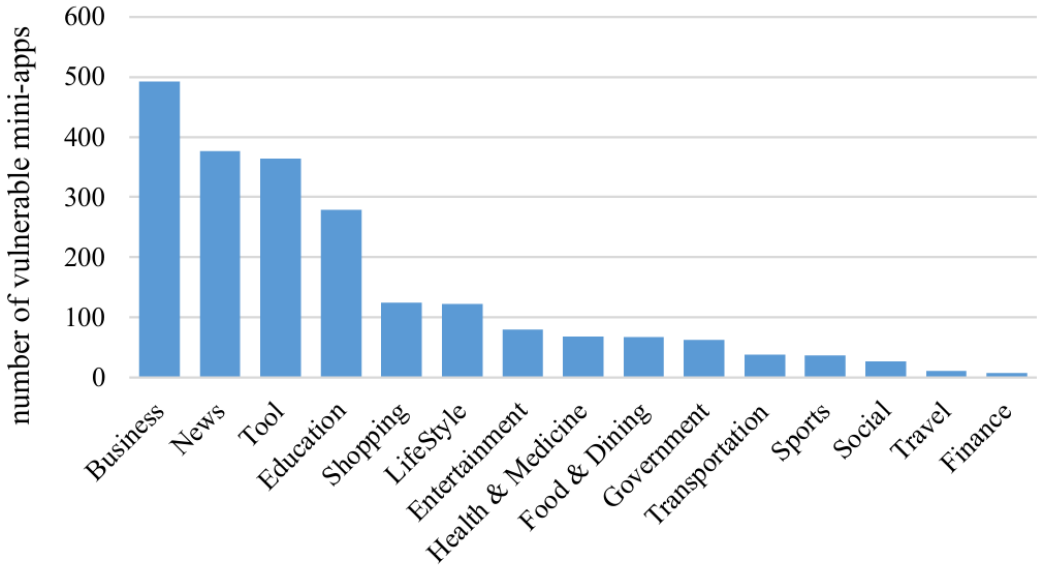
- Hidden Capability Excavation
  - ICREMiner uncovers 4,202 hidden cloud resources, and identifies 539 vulnerable mini-apps (36.27%)
  - LLM-based inference performs better than other methods

Method	Detection Results		Insecure Practices	
	# op	# app	# op	# app
Common Name Augmentation	1197	879	195	180
LLM-based Inference	3309	810	1100	390
Mini-app Correlation	141	57	40	20
ICREMiner	4202	1486	1262	539

Method	Detection Results		Insecure Practices	
	# op	# app	# op	# app
Gemini-based Inference	3309	810	1100	390
GPT-based Inference	3103	740	1050	363
Deepseek-based Inference	2691	629	931	308
Llama-based Inference	3131	789	1053	372
Bert-based Inference	1180	565	191	176

Result Overview

- Many mini-app developers misplace the user identity check and assign write permissions to sensitive resources
- Vulnerable mini-apps are mainly distributed across categories rich in sensitive data



Super-app	User Identity Check						Sensitive Resource Allocation					
	UIC-1			UIC-2			SRA-1			SRA-2		
	# op	# app	% total	# op	# app	% total	# op	# app	% total	# op	# app	% total
WeChat	1765	886	32.65%	4306	1846	67.94%	93	81	2.98%	1762	984	36.22%
TikTok	12	12	30.77%	19	12	30.77%	15	10	25.64%	9	7	17.95%
Alipay	13	13	39.39%	24	22	66.67%	8	8	24.24%	0	0	0
Baidu	7	7	26.92%	22	16	61.54%	7	7	26.92%	3	2	7.69%
Overall	1797	919	32.65%	4371	1896	67.35%	123	106	3.77%	1774	993	35.28%

Result Overview

- Multiple types of sensitive data are exposed through vulnerable mini-apps

Cloud Database		**Cloud Storage**	**Cloud Routine**	
collection name	cloud data	file content	function name	description
userinfo	user name, gender, country, etc	user photo	payment	update user's balance after a payment is made
orders	buyer name, buyer phone number, goods list, etc	employee information	groupbill	get user information using the user ID
shop_orders	user information	student card picture	getuserinfo	get user information using the user ID
user_info	user name, phone number, password, etc	vehicle license	queryuser	get user information using the user ID
loginUser	account, company name, password, etc	medical license	getqysessionkey	get the credential session_key
admins	admin name, account, password, etc	user photo	login	login into the account (return the credential app_secret)
Employee	user name, email address, position, etc	user photo	login	login into the account (return the credential session_key)
users	country, gender, phone number, etc	user certificate	gethistory	get user's browser history using the user ID
payment	user name, card number, order information, etc	curriculum vitae	getrole	get user information using the phone number
todos	action, user name, etc	ID card picture	sendtongyipaymsg	send messages to other mini-app users

Other Observations

- “Write Operation” Vulnerability
  - 993 mini-apps have vulnerable write operations
  - Enable users to write sensitive personal information, such as account balance
  - Enable users to write system resources, such as notification content
- Templated Cloud Services
  - 125 vulnerable mini-apps (4.4%) are developed using templates
- …

Summary

- We conduct the first systematic study on security risks of insecure cloud resource management in the app-in-app ecosystem

- We propose a novel approach, called ICREMiner, that combines static analysis and dynamic probing to automatically analyze the ICREM risks

- We conduct a large-scale, empirical study on real-world mini-apps and have identified 2,815 mini-apps that are affected by this vulnerability. We also made responsible vulnerability disclosure and propose corresponding mitigation strategies

Thank You!