Human Factors in Cybersecurity: Issues and Challenges in Big Data

Xichen Zhang, Ali A. Ghorbani

Contact Email: xichen.zhang@unb.ca

Canadian Institute for Cybersecurity (CIC), University of New Brunswick (UNB)

*Accepted as a book chapter in "**Book on Security, Privacy, and Forensics Issues in Big Data**" IGI Global*

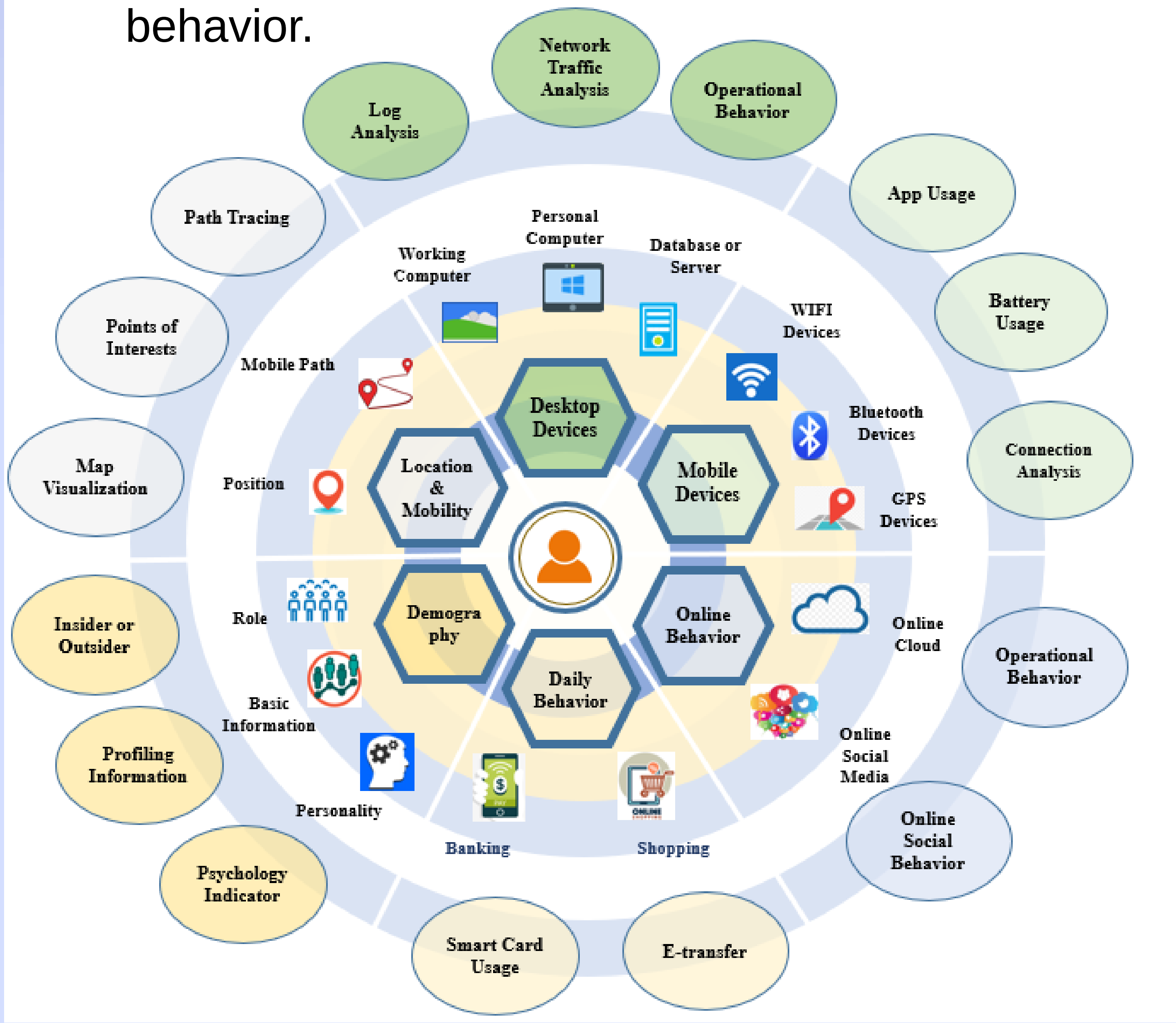
OBJECTIVE

In recent years, the growth of online Cloud services and the increasing number of remote users rise more complex security and privacy issues. Hence, human factors play crucial roles in the pervasiveness of cyber threats and attacks. As the fast and extensive development of cybersecurity technologies, novel and sophisticated approaches are used for fighting against digital cybercrimes. As a result, hackers need to seek new hacking methods to launch cyberattacks. With non-professional personnel being the weakest link, most of the advanced attacks rely heavily on human factors. Human's interaction with the electric devices and their performance in normal security procedure can bring potential cyber threats and vulnerabilities in daily actions. Under this circumstance, how to profile human's daily behavior and evaluate users' malicious and vulnerable level should be paid more attention in both academia and industry. It is a necessity to present new information threats under these domains and propose promising approaches for addressing such issues. All in all, by consolidating malicious and vulnerable human daily behaviors, and extracting intelligent insights from human daily factors, cyber defenders and experts can effectively detect cyber attackers, and reduce the impact of those information threats. In this study, we first introduce the role of human factors in cyberspace, and the importance of profiling user behaviors in cybersecurity. Then, the potential security and privacy issues in daily human practice are discussed in detail. Finally some promising future directions are proposed.

OVERVIEW OF THE PROBLEM

➢ **Human-centric** Cybersecurity:

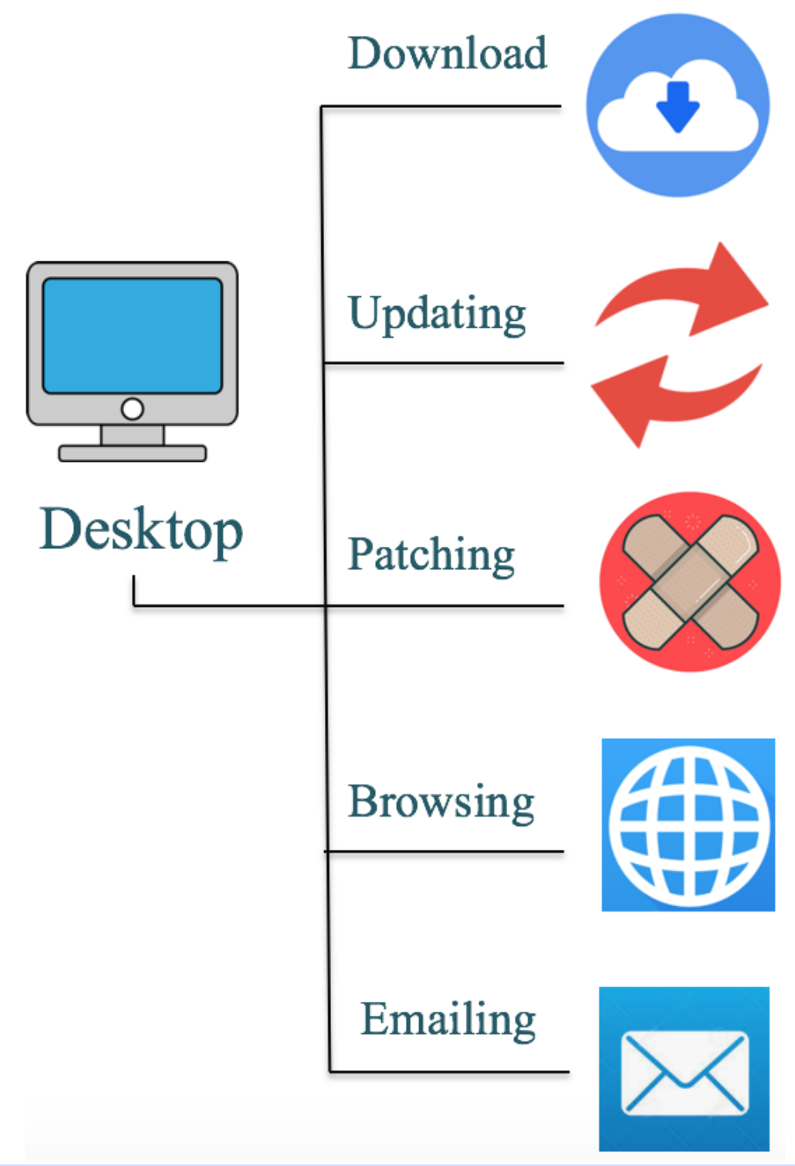
- Different types of vulnerable human-based daily behaviors: Desktop behavior, Mobile behavior, Online behavior, Daily behavior, Demographic information, Location-related behavior.



INSIDER AND OUTSIDER

	Insider and Insider Threats	Outsider and Outsider Threats
Privilege	Partial or wholly access to the information and resources.	Have no access to the internal resources.
Example	• Employees • Contractors • Administrators	• Hackers • Cybercriminals • Terrorists
Resource available	• Authentication Info. • Employee Info. • Hardware & software • Database	• Only external resources
Common threats	• Physical theft • Privilege abuse • Copying sensitive data • Data leakage	• Social engineering • Hacking • Phishing • Malware ……

DESKTOP BEHAVIORS



➢ **Malicious file download,** (e.g., mimic the legitimate download behavior) & **application download** (e.g., malware download)

➢ The **vulnerability** of the products and the OS is highly related to the potential cyber risks, as well as the **customers' updating & patching habit** (e.g., how often? authenticated patch/update)

➢ Bad **browsing behavior** can cause potential cyber attacks (e.g., # of visits, duration, authenticated URL or not, browser vision, landing or exit page)

➢ **Bad email receiving behavior** can lead to phishing attack (e.g., open email from unknown sender, click unknown attachment, open unauthenticated link in the email)

MOBILE BEHAVIORS

➢ **Mobile Terminal Issues:**

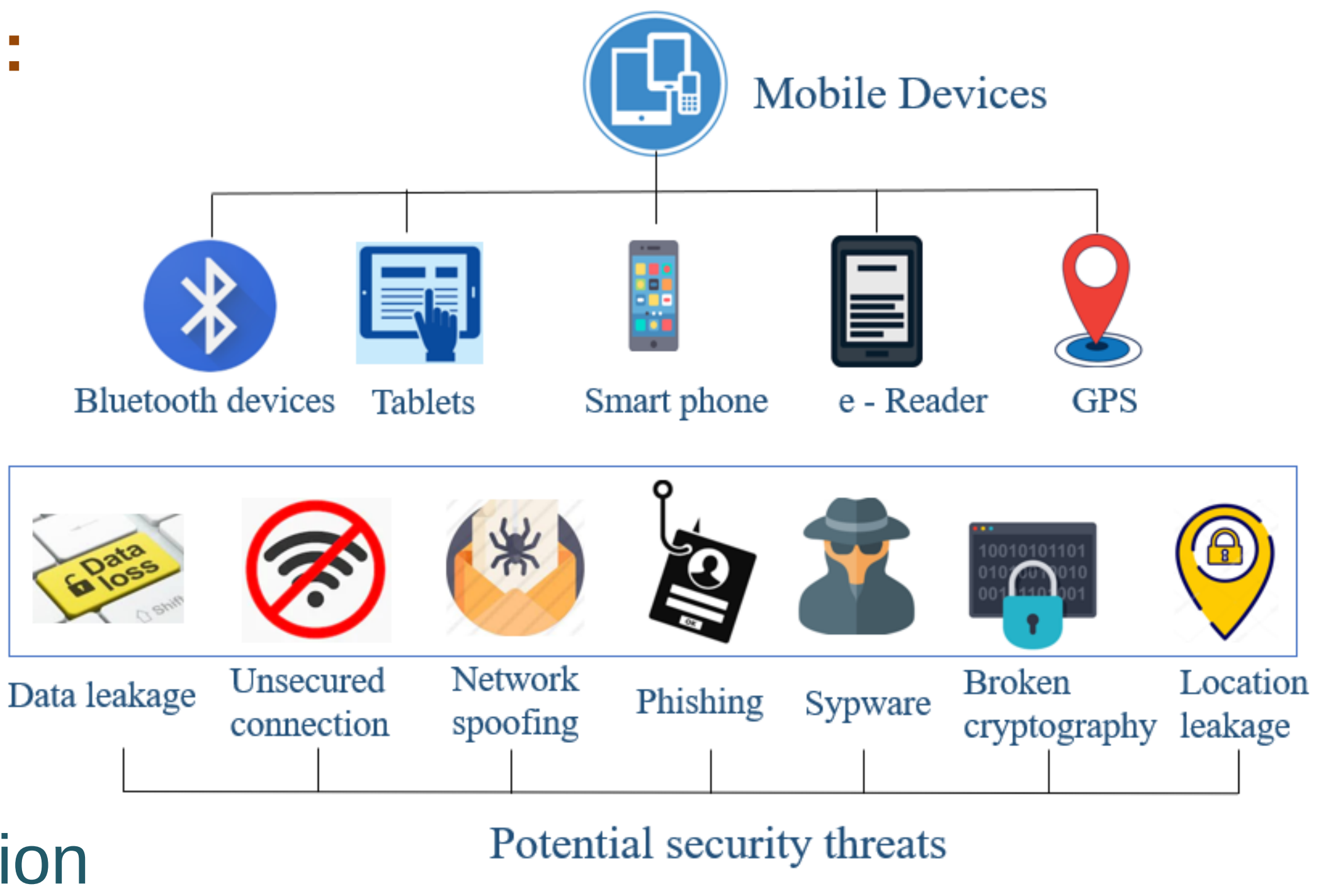
- Mobile Malware
- Software Vulnerability

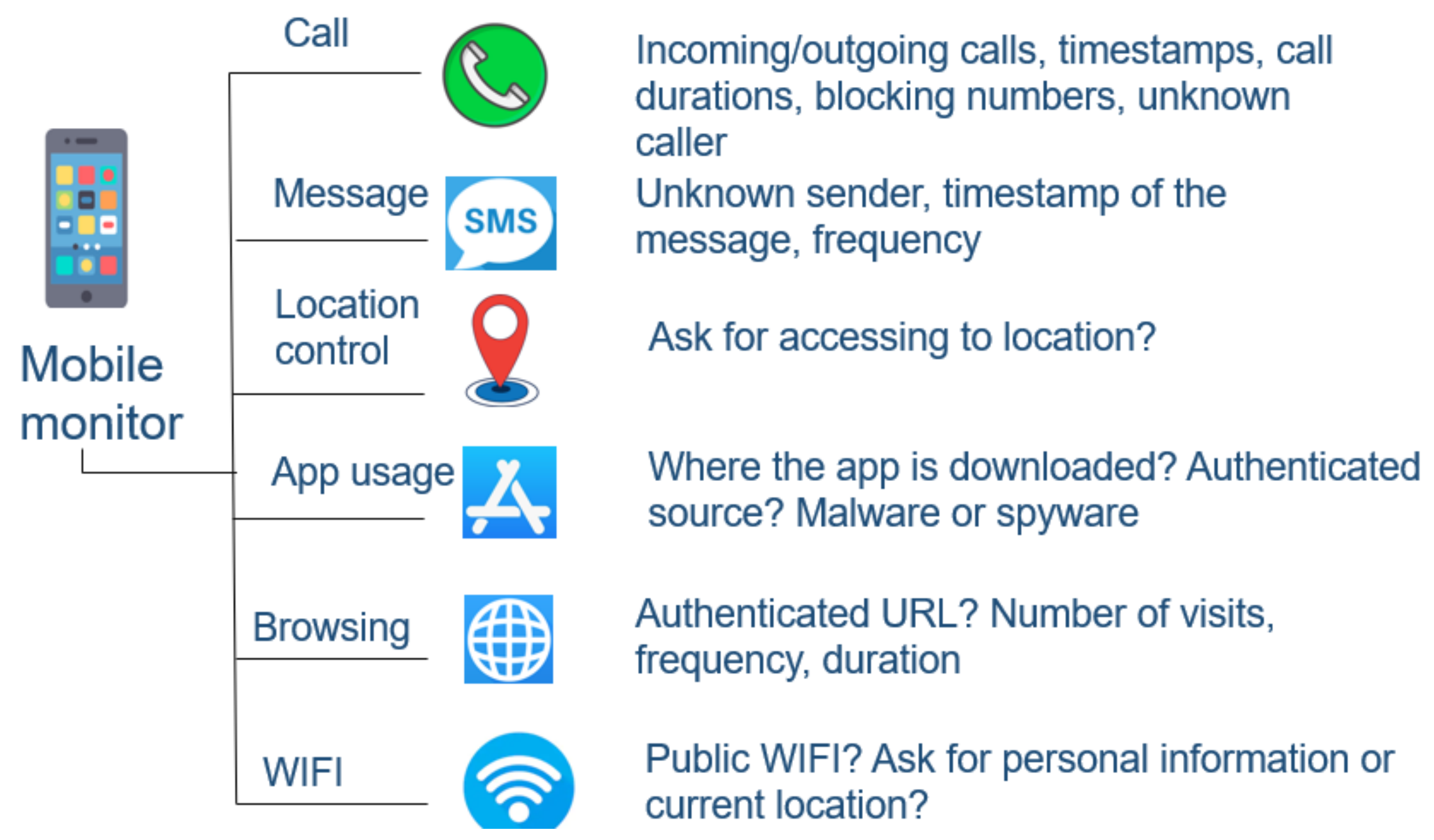
➢ **Mobile Network Issues:**

- Malicious Public Wi-Fi
- Rouge Hotspot
- Bluetooth Attack

➢ **Mobile Cloud Issues:**

- Mobile Cloud storage
- Mobile Cloud computation





Incoming/outgoing calls, timestamps, call durations, blocking numbers, unknown caller

Unknown sender, timestamp of the message, frequency

Ask for accessing to location?

Where the app is downloaded? Authenticated source? Malware or spyware

Authenticated URL? Number of visits, frequency, duration

Public WIFI? Ask for personal information or current location?

ONLINE BEHAVIORS

Online Behaviors
Social Media
Financial Actions
Online Cloud

➢ **Social Media:**

- Fake and misleading content: fake news, fake reviews, fake political claims, fake ads
- Potentially malicious fake context: social bots, cyborg, hackers, malicious advertisers

➢ **Financial Actions:**

- Online banking: compromised banking apps, reused credentials
- Online shopping: fake review, lack of disclosure, phishing websites, information data leakage, online trading, location-based privacy

➢ **Online Cloud:**

- Data confidentiality, integrity, and availability in online Cloud
- Cloud-based attacks: network-based attacks, virtual machine based attacks, storage-based attacks

➢ **Others** : security and privacy issues in Cloud-based data mining tasks

References: Top 7 Mobile Security Threats: Smart Phones, Tablets, & Mobile Internet Devices – What the Future has in Store. https://usa.kaspersky.com/resource-center/threats/top-seven-mobile-security-threats-smart-phones-tablets-and-mobile-internet-devices-what-the-future-has-in-store. Accessed date: Dec 13rd, 2018.