

Secured Sim Ejection

Sahaya Joseph Rohan.A, Sengodan.D, Kavin Kumar.S, Eswanth Raj.S

Department of Artificial Intelligence & Machine learning,
SNS College of Technology,
Coimbatore ,India

sahaya.a.aiml.2021@snsct.org, sengodan.d.aiml.2021@snsct.org, kavin.s.aiml.2021@snsct.org, eswanth.s.aiml.2021@snsct.org

Abstract- A SIM card, also known as a subscriber identity module, is a smart card that stores identification information that pinpoints a smartphone to a specific mobile network. Data that SIM cards contain include user identity, location and phone number, network authorization data, personal security keys, contact lists and stored text messages. SIM cards allow a mobile user to use this data and the features that come with them. We all use sim card but without the knowledge about the consequences of losing a sim card. Once we lose a sim card, we let it free and move on to another sim card. Have you ever wondered that our sim stores a lot of data but what if it goes to someone's hand, all our personal details are leaked and there are even chances of selling them in the dark web? By applying this project, it is easy to avoid the circumstances of losing a sim card. We don't have a proper protection for our sim card. It can be easily inserted and also easily ejected. Understand that you are in a danger if you have lost your sim card. But this is not going to happen again. This project fully focusses on securing the sim card by giving utmost protection to the sim card. This involves a security page to be authenticated if someone needs to eject the sim. Sim Ejection wouldn't be easier after the implementation of this project.

Keywords- dark web, SIM cards, personal security keys etc.

I. INTRODUCTION

A SIM card (full form Subscriber Identity Module or Subscriber Identification Module) is an integrated circuit (IC) intended to securely store the international mobile subscriber identity (IMSI) number and its related key, which are used to identify and authenticate subscribers on mobile telephony devices (such as mobile phones and computers). Technically the actual physical card is known as a universal integrated circuit card (UICC); this smart card is usually made of PVC with embedded contacts and semiconductors, with the SIM as its primary component. In practice the term "SIM card" refers to the entire unit and not simply the IC.

A SIM contains a unique serial number (ICCID), international mobile subscriber identity (IMSI) number, security authentication and ciphering information, temporary information related to the local network, a list of the services the user has access to, and two passwords: a personal identification number (PIN) for ordinary use, and a personal unblocking key (PUK) for PIN unlocking. In Europe, the serial SIM number (SSN) is also sometimes accompanied by an international article number (IAN) or a European article number (EAN) required when registering online for the subscription of a prepaid card. It is also possible to store contact information on many SIM cards.

1. Data Stored in Sim Card:

- ICCID - Integrated circuit card identifier
- IIN - Issuer identification number.
- Individual account identification number

- Check digit
- IMSI - International mobile subscriber identity Authentication key
- Location area identity
- SMS messages and contacts

II. SYSTEM

1. Existing System:

We usually eject the sim from the device by performing the following steps:

- First, we turn off our phone.
- Secondly, locate our SIM-eject tool. If we don't have one, we use a small paperclip.
- Then we insert the tool (or paperclip) into the small hole next to the SIM slot and push gently but firmly until the tray pops out.
- We then slide the tray out from the device, and remove the SIM card by simply lifting it out of the tray.

2. Drawbacks of the Existing system:

The existing method lacks a lot behind in security. The sim card can be ejected and inserted into the phone very easily. The sim ejection and insertion require zero efforts. Anyone who is using the phone can eject the sim in a very short period of time. The only tool required to eject a sim is a sharp object that may be a sim ejection tool or even a needle or a paper clip. Once you lose your sim understand that you are in a danger, all your data are leaked and can be used by anyone for any purpose. The proposed system

may be simple in ejection and also simple in insertion but not a secured one.

3. Proposed System:

In the proposed system the mechanism is completely changed. We will not be performing any of the steps that we perform in the existing system. This mechanism truly focuses on safety purposes. We planned according to the requirements and brought out a perfect solution for this issue. In the proposed system we are not going to be using a sim ejection tool. The only common thing between both the system is the sim tray and the sim. This mechanism is completely a motorized one and works with zero faults. This system uses the mechanism used in a pop-up camera, in which the sim tray is going to be connected to a motor which moves up and down, if the user enters the correct password the sim tray automatically pop's out from the device.

The step by step working process of the proposed system is:

Step 1: Usually when we long press the power button, we get three options: Power off, Restart, Emergency mode (Depending on the device).



Fig 1. Step-1 Working process.

Step 2: With this we are adding the fourth option: Power off, Restart, Emergency mode (Depending on the device), Sim Ejection.



Fig 2. Step-2 Working process.

Step 3: When you click on this icon, it directs you to an authentication page where you need to enter the password.

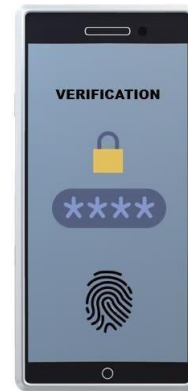


Fig 3. Step-3 Working process.

Step 4: If you enter the correct password, the sim will get ejected automatically using a motorized mechanism else you will not be able to eject the sim. These processes are later on explained in the later part.

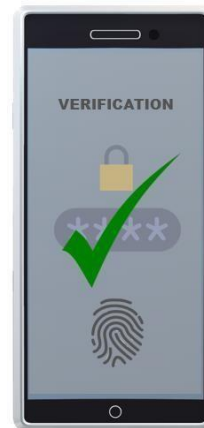


Fig 4. Step-4 Working process.



Fig 5. Step-4.1 Motorized Pop up Mechanism.

III. FLOWSYSTEM

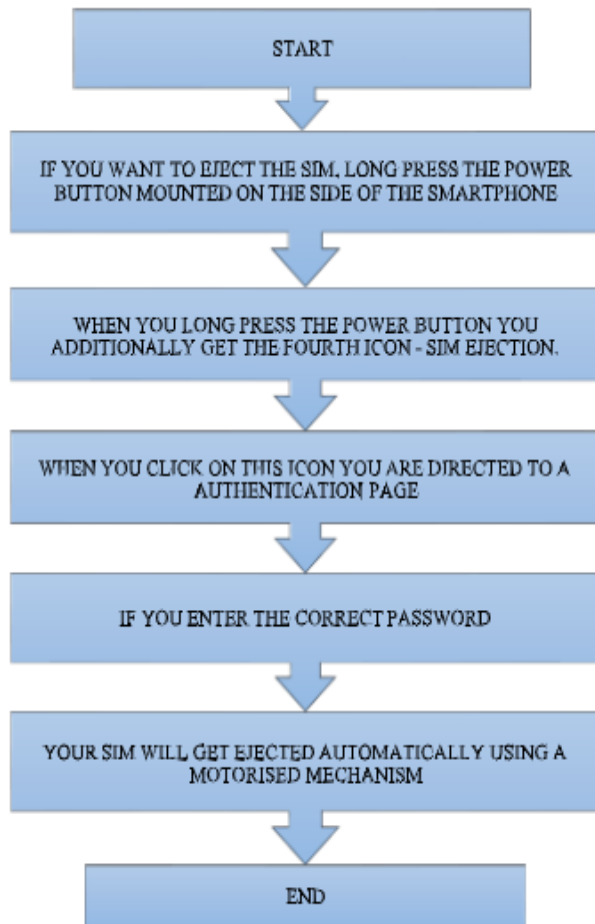


Fig 6. Flow Chart.

IV. CONCLUSION

As final stage of this development, we have tested this proposed system to confirm feasibility of the system. This paper introduced an efficient way to secure the sim card ejection. In this paper, we discuss the design of proposed safety system for sim ejection. The project discusses the importance of sim card and the circumstances in losing a sim card, most of the people don't have the knowledge regarding the circumstances of losing a sim card. In this project I have clearly explained about the data stored in a sim card.

This project describes the effective solution for this fatal problem which states what are the system updates that could be brought into practice during the manufacturing process. This solution cannot be applied to an existing device; this can only be added to a device during the manufacturing process. This could be considered as an effective solution and brought into practice by the manufacturing companies taking the circumstances more seriously.

REFERENCES

- [1] Aibinu, A. M., Onumanyi, A. J., Folorunso, T. A., Ipinoyi, M., & Adda, A. (2016). Development of Embedded-Multiple Operators Enabled SIM (E-MOES) Card System for Mobile-Phone Initiated and Executed Handover, 20.
- [2] Edsbäcker, P. (2011). SIM cards for cellular networks An introduction to SIM card application development. MID SWEDEN UNIVERSITY.
- [3] Husemann, D. (2001). Standards in the smart card world. Computer Networks, 36(4), 473–487. [https://doi.org/10.1016/S1389-1286\(01\)00167-0](https://doi.org/10.1016/S1389-1286(01)00167-0)
- [4] NCC. (2016). Development of Multiple Subscribers Identity Module (SIM) cards Reader and Analyser