# Threats and Protection on E-Sim

**Alex R Mathew**

***Abstract:** Threats involve various risks and threats are associated with the embedded SIM technology, for instance, the Internet of things (IoT) identity. IoT refers to the working capabilities enabling the allocation of unique identifiers (UID) to effectively connect with the related devices thus enhancing communication. An e-SIM application cannot produce reliable and actual data used to obtain the subscriber's anticipated outcome. The SIM technology does not provide some reliable data that can be employed by the user to formulate some serious productive outcomes. Failure by the technology to process and automatically provide the user with the notification suppose of any infringement or hacking. SIM-jacking is the other notable threats facing the embedded universal integrated connectivity card (e-UICC). Incompetent Log Rhythm Al Engine influences the fraudster hacking experience due to failure protections within the operational surrounding. The e-SIM technology system lacks timely threat, risk, and other various vital operations predictability to react to the experienced unbearable operations challenges induced by the fraudsters. Similarly, the embedded SIM incurs the insider threats whereby the service providers fail to secure the much-needed privacy concerning an individual's vital information. The situations of personal data leakage are witnessed within the system operations.The e-SIM hijacking enables the fraudsters to secretly obtain the victim's vital data of the subscriber, hijack, and receive the information intended to the individual to his/her personal phone. The process results to complete mobile account operations by the hacker resulting to further access to the victim's bank information and transfer of cash. The other threat experienced by e-SIM users is the provision of false information. The SIM subscribers normally fall into traps of the fraudsters by receiving short messages (SMS) citing assistance kind of news from the service providers, thus drawing the victim's bank amount. Identity fraud and device poisoning are other additional threats encountered in the application of e-SIM. Generally, the entire process of fraud invasion and victimization influence the victim's business decisions of the affected individuals. Protections focuses on the embedded SIM provides greater security in addition to a re-programmable technological system, unlike the physical SIM card. The subscriber's personal information is not contained within the e-SIM but with the service providers, thus enhancing its effectiveness. An e-SIM enables the consumers to effectively shift carriers between the T-Mobile and Sprint without physical movement, thus supportive of security systems. Despite the security measures put into place, e-SIM like any other SIM card experiences information theft. Therefore, the service providers should encounter the emerging fraudster effects by proper monitoring of the network system to enable security restrictions. The system should induce strict conditions that enable the evaluation and differentiation between the IoT and the non-IoT devices during their operation.***

***Keywords:** Cellular network, Charging, IoT and non-IoT devices, and Security.*

## I. INTRODUCTION

An embedded subscriber identification module (e-SIM) refers to a programmable electronic card implanted into a phone or electronic gadgets to facilitate connection, for instance, machine to machine (M2M) or cell phone connections. The inbuilt SIM enables the identification and validation of the user's personality as well as his/her carrier. Contrary to the physical SIM card, the embedded card permits the employer to tenuously alter the operator from their device without securing another SIM card. The technology enables mass storage of various profiles within the distinctive device, thus enhancing both personal and business applications. Despite the perceived scalable, secure, and reliable connectivity, e-SIM technology still faces numerous operational challenges. In the context provided, the paper focuses on discussing various threats and protections on e-SIM.

## II. PROPOSED METHODOLOGY BLOCK DIAGRAM

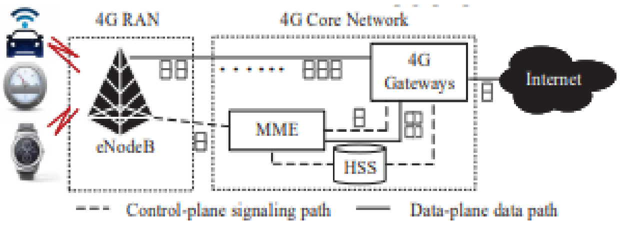

**Fig. 1: 4G network architecture with IoT support**

Source: https://doi.org/10.1109/tmc.2020.2984192

As stated by the Communications Fraud Control Association (CFCA), SIM-jacking is the most common threat experienced in information technology. SIM cards are the primary source of communication networks, thus, remains to be the attacking target of the fraudsters. The experiment was done using the internet of things devices such as the hotspots and smartwatch. An additional non-IoT device like the e-SIM cards and Android phones were employed in the practical [3]. The hotspots were installed into two different cars to provide network signals. For the security of the carriers and minimization of injuries during the study, the contained data was applied in the buying of plans. Thereafter, a fresh security weakness was tested through operative attacks on the mobile IoT amenities without the involvement of the damages induced. From the experiment, it was found that the cellular charging was affected by the masking of IoT and the application abuse [2], [4].

**Revised Manuscript Received on August 12, 2020.**

***** Correspondence Author
**Alex R Mathew***, Bethany College, USA. E-mail: amathew@bethanywv.edu

On testing the liability of IoT devices, three major vulnerabilities were determined from the induced masked attacks whereas the non-IoT devices showed two exposures from the masqueraded attacks. The exposures were noted to have originated from the absence of reciprocated connections between the devices, for instance, cellular devices and the IoT cards as well as cell devices and the infrastructures [1]. The attacks impacted the identification inability between the IoT and non-IoT plans. As a result, both the two devices had a successful camouflage attacking effect without any recognition by the carriers. The impact shows that, for effective verification of cellular devices, mutual agreement between the devices is a key factor. The subscriber's presence and confirmation are primarily determined by the reciprocated pact with the service providers, for example, the international mobile subscriber identity (IMSI). It is the IMSI in addition to the subscriber's secret key that enables the authentication of the user's cellular device since they are documented on the SIM card.

- ***Flow Chart***

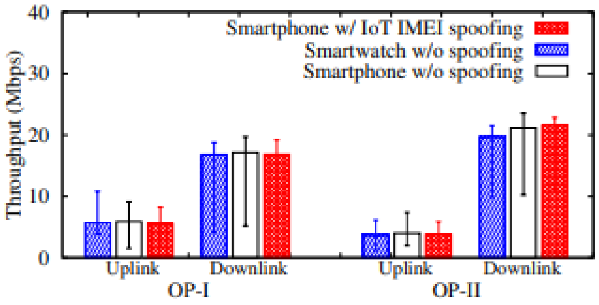

**Fig. 2: The chart demonstrating TCP link throughput at 10th, 50th, and 90th percentiles for an IoT device**

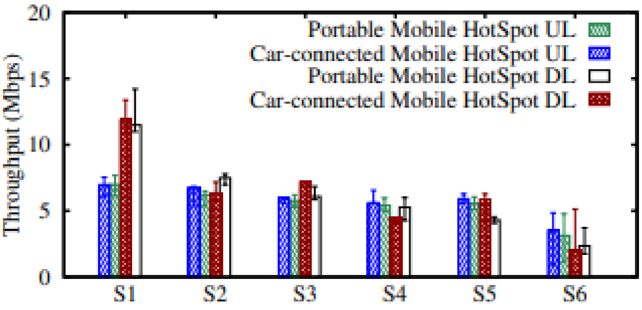

**Fig. 3: The chart showing TCP output outcome at 10th, 50th, and 90th percentiles plots.**

- Source: https://doi.org/10.1109/tmc.2020.2984192

## III. RESULT AND DISCUSSION

From the experiment conducted, the two combinations involving the IoT devices and cellular devices in addition to cellular devices and the infrastructure were exposed to the masking attacks (Jang, 2020, p. 1176). However, not only were they exposed but could also not identify the origin of the threat induced. Even though the two combinations of mobile phones shared network infrastructures with IoT devices, additional security support was needed for protection purposes. The radio accessory network (RAN) permitted the transmission of IoT information from IoT plans to the services providers through the usage of IoT technology. In the IoT machinery, there existed mobility management entities (MMEs) network system facilitating the subscriber's authentication, mobility, and infrastructure reservations [11]. The other system included a home subscriber server (HSS) that enhanced documentation of the user's profile data in addition to the subscription. The other operating system involved was the 4G gateway data that facilitated the information transmission amongst cellular device, internet, and random accessory network. Cellular devices vulnerability was exposed and similarly validated whereas the cards operated for the IoT plans. Despite the configuration of network settings, mobile phones effectively accessed the network after the acquisition of the IP addresses [10]. The cellular devices are commonly identified and detected by the service providers with their various international mobile equipment identities (IMEI). It is through the process that the fraudsters employed their hacking techniques to access the subscriber's profile data. There is much exposer when the service providers offer network services to both the IoT and non-IoT plans simultaneously. It is through the camouflaging process that the attackers find their pathway to hack the networking system of the subscriber. The applied devices expressed an equivalent presentation on both the uplink and downlink network operations. The network operators did not subject enough limitations on the IoT plans during the information transmission [12]. The network resources are normally shared by numerous electronics across the web system that enhances its ineffectiveness in relationship to the subscribers. Some notable causes of vulnerability within the random accessory networks include the usage of IoT SIM cards in equal measure as the non-IoT devices. Through this, the system weakness is determined and equally detected by the perceived fraudsters, thus enabling them to have their unwanted hacking motives. As such, no appropriate and mutual connection is witnessed between the IoT cards and the non-IoT devices thus enhancing the vulnerability state of the perceived SIM-jacking and information theft [5], [9]. The other influence of the witnessed insecurity cases in the inability of the service providers to detect and differentiate between the IoT and non-IoT devices during the service delivery.

The effect is primarily subjected by the lack of proper authentication mechanisms to incorporate the needed connections between mutually programmed devices according to the IoT device's standards. The service providers are also considered the cause of certain threats received by the SIM operators, for instance, their failure to restrict the data application by its subscribers [6], [8]. Failure by the infrastructure to regulate the data usage in their systems facilitates the operations slip within the IoT devices. As such, the device operators are primarily compelled to rely on the provider's operational effects. Therefore, the perceived attacks are impacted by the inability of the infrastructure to identify between the IoT and non-IoT plans. As a result, both the two devices had a successful camouflage attacking effect without any recognition by the carriers. The impact shows that, for effective verification of cellular devices, mutual agreement between the devices is a key factor [7]. The subscriber's presence and confirmation were primarily determined by the reciprocated pact with the service providers, for example, the international mobile subscriber identity (IMSI).

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication

It is the IMSI in addition to the subscriber's secret key that enables the authentication of the user's cellular device since they are documented on the SIM card.

## IV. CONCLUSON AND FUTURE SCOPE

Even though the application of the embedded universal integrated connectivity card (e-UICC) is witnessed across the globe, security remains a challenging factor. As such, the fraudsters have initiated the hacking of e-SIM technology system to seek vital personal information from the subscribers. Therefore, the security of the system is noted to be a significant factor in its advancement because the subscriber's privacy is protected. From the experiment conducted, safety implication is significant during the IoT service charging process. It is through the IoT device service is whereby the perceived threat originates from various vulnerabilities and attacks. However, the vulnerabilities are induced by a lack of reciprocated connections between the cellular devices and the service providers/infrastructure or IoT cards. To encounter the security challenges, the application of the anti-abuse resolution to alleviate the vulnerability witnessed due to lack of shared authentication effect would be the most appropriate action. Nevertheless, e-SIM is considered more secure than a physical SIM.

## REFERENCES

1. M. M. Danziger, L. M. Shekhtman, A. Bashan, Y. Berezin, and S. Havlin, 2016. Vulnerability of interdependent networks and networks of networks. In *Interconnected networks* (pp. 79-99). Springer, Cham.
2. J. Franklin, C. Brown, S. Dog, N. McNab, S. Voss-Northrop, M. Peck, and B. Stidham, 2016. *Assessing Threats to Mobile Devices & Infrastructure: the Mobile Threat Catalogue* (No. NIST Internal or Interagency Report (NISTIR) 8144 (Draft)). National Institute of Standards and Technology.
3. J. M. Heikkilä, 2017. *Information security risk analysis and mitigation methods for industrial internet in industrial vendor segment* (Master's thesis).
4. Y. Huang, and P. Mishra, 2020, March. Vulnerability-aware Dynamic Reconfiguration of Partially Protected Caches. In *2020 21st International Symposium on Quality Electronic Design (ISQED)* (pp. 255-260). IEEE.
5. S. R. Hussain, M. Echeverria, A. Singla, O. Chowdhury, and E. Bertino, 2019, May. Insecure connection bootstrapping in cellular networks: the root of all evil. In *Proceedings of the 12th Conference on Security and Privacy in Wireless and Mobile Networks* (pp. 1-11).
6. M. Jakobsson, 2020. Social Engineering Resistant 2FA. *arXiv preprint arXiv:2001.06075*.
7. Y. S. Jang, 2020. Detection of SQL Injection Vulnerability in Embedded SQL. *IEICE Transactions on Information and Systems*, *103*(5), pp.1173-1176.
8. M. Khan, P. Ginzboorg, K. Järvinen, and V. Niemi, 2018, November. Defeating the downgrade attack on identity privacy in 5G. In *International Conference on Research in Security Standardisation* (pp. 95-119). Springer, Cham.
9. P. Pathak, N. Vyas, and S. Joshi, 2017. Security Challenges for Communications on IOT & Big Data. *International Journal of Advanced Research in Computer Science*, *8*(3).
10. K. Sung, B. Levine, and M. Zheleva, 2020, July. Protecting location privacy from untrusted wireless service providers. In *Proceedings of the 13th ACM Conference on Security and Privacy in Wireless and Mobile Networks* (pp. 266-277).
11. Y. Wang, J. Shen, J. Lin, and R. Lou, 2019. Staged method of code similarity analysis for firmware vulnerability detection. *IEEE Access*, *7*, pp.14171-14185.
12. T. Xie, G. H. Tu, C. Y. Li, and C. Peng, 2020. How Can IoT Services Pose New Security Threats In Operational Cellular Networks? *IEEE Transactions on Mobile Computing*.

## AUTHORS PROFILE

**Alex R Mathew***, Ph.D. in Computer Science and Engineering (Cyber Security) Certified Information Systems Security Professional- CISSP - (ISC)2 ISO 27001 Lead Auditor EC Council Certified Instructor (CEI) EC Council Certified Network Defender (CND) EC Council Certified Secure Computer User (CSCU)

1) Microsoft Certified Solutions Expert – MCSE - (Microsoft)
Certified Ethical Hacker – CEH- (EC-Council)
Computer Hacking Forensic Investigator - CHFI- (EC-Council)
Cisco Certified Network Associate (CCNA) – (Cisco)
Cisco Certified Network Associate (CCNA R &S) – (Cisco)
IBM Certified Ecommerce Specialist
ZAP Certified Web Designer
*Security+* (CompTIA)
ECSA -EC-Council Certified System Analyst (EC Council)
CREST Practitioner Security Analyst- CPSA
Memberships:
IEEE, ACM, Cisco, EC Council, CompTIA, IBM, Microsoft, CSTA.

Alex's areas of expertise include Cyber Security, Ethical Hacking, Cyber Crimes and Digital Forensics Investigation. He is a Certified Information Systems Security Professional and the founder of several cyber security awareness initiatives in India, Asia, Cyprus and Middle East. With over 20 years' experience of consulting and training has developed a large skill set and certification set. He was instrumental initiating and organizing a number of conferences.

He has 100+ publications with IEEE, ACM and Scopus Indexed International Journals. Dr.Alex has received a number of awards including the Best Professor, Best Presenter, Best Researcher 2019 etc. He is a frequently invited speaker and panelist, reviewer at International conferences related to Cyber Security, Technology, Innovation and education. Alex's profile describes a confident and outgoing individual who enjoys the company of other people. He has a persuasive, open style with others, and develops interpersonal relationships quickly and relatively easily. His levels of self-confidence mean that he rarely doubts his abilities in a social situation, although he may find it a little harder to deal with practical or impersonal situations. Alex's communicative and open style means that he tends to be trusting of others, or at least confide information more readily than many other personality types. Because of his social orientation, however, he finds it rather difficult to deal with rejection by other people, thriving as he does on their positive attention. His current research activities are directed towards Cyber Security, Internet of Things (IoT), Cloud security, Augmented & Virtual Reality, Robotics and Intelligent Systems Security in Next Generation Networks, Smart Technologies, Cybercrimes Investigations. Dr. Alex is inquisitive and always looking for innovative solutions to even more basic issues. That inquisitive nature translated very well into his career as an educator and researcher.