Concerned About Privacy Leaks From Iot Devices? IIT Madras Researchers May Have A Solution!

Prasanna Karthik Vairam*
Indian Institute of Technology, Madras
Email: vprasannakarthik@gmail.com

With the proliferation of Internet of Things (IoT) devices such as smart TV and smartwatches, the issue of privacy leaks looms large over our households. This is primarily due to the access that these devices have to sensitive information about our personal lives. Let alone preventing, even identifying such privacy leaks is still an open problem in the field of communications and computer science.Researchers at IIT Madras have come up with a new Blockchain design that can be used to identify privacy leaks from IoT devices. Although Blockchains have been used to solve a plethora of problems in the past couple of years, making Blockchains work in IoT (where storage and computational resources are scarce) has been a glass ceiling, which these researchers have now broken.

Privacy leaks have been widely speculated for a long time, but it was not until the Facebook-Cambridge Analytica data scandal that common people learned of its seriousness. Facebook-Cambridge Analytica scandal showcased that the seemingly harmless "which famous film personality are you?" type quizzes could be used to sway the outcome of the US presidential elections. Leading researchers in this field believe that there is a high chance that there may exist many such privacy breaches which are not yet known to common people. In fact, the research community has been well aware of this and has been working towards identifying and protecting against such privacy leaks. Even government agencies around the world have started

---

* Mr. Prasanna Karthik Vairam, Ph.D. Scholar from Indian Institute of Technology, Madras, is pursuing his research on "Applications of Approximate Data Structures in Storage Constrained Untrusted Distributed Networks." His popular science story entitled "Concerned about Privacy Leaks from IoT Devices? IIT Madras Researchers may have a Solution!" has been selected for AWSAR Award.

taking notice of such privacy breaches and are working round -the -clock to protect sensitive information from leaking.

Many decades ago, researchers as well as companies invested much of their resources to answer the question 'Does the device do what it is supposed to do?' Due to the newness of computing technology, ensuring the correctness of computations was important. However, in recent times, the most important security question that needs to be answered is 'Do the devices do something that they are not supposed to do?' The answer to this question has eluded researchers for a while. Blockchains are seen as a promising technology to answer this question. In simple terms, a Blockchain is a tamper-resistant digital account book of critical/security events that occur in any IT infrastructure. Examples of such critical events include banking transactions, IoT device activities, and shipment activity of goods, depending on the scenario in which the Blockchain is deployed. For instance, when IoT devices are used in a house, the Blockchain will be capable of recording events such as activating air conditioner, switching on the microwave, and changes in temperature. The Blockchain will provide a comprehensive picture of the activities, based on which suspicious behaviour such as leakage of the temperature readings to the outside world can be detected and flagged. It is worth noting that accurately capturing the events is the challenging part, while there exists efficient methods in the fields of statistics to detect and flag suspicious activities.

Blockchains are not a completely novel technology but rather an ensemble of various data-structures and algorithms that have been well -known for the past three decades. Researchers argue that, despite re-using known technologies, it is the unique combination of these technologies that help Blockchains achieve high levels of security. The Blockchain is a peer-to-peer technology where some IoT devices sense critical events and the other IoT devices verify and record them in the Blockchain. The key idea is that an event gets recorded if and only if a majority of these devices agree upon its correctness i.e. security is ensured when at least 51% of the devices are honest. Also, once the devices agree on the validity of a critical event and add it to the Blockchain, it is impossible to retract at a later point in time; thereby preventing attackers from tampering the log.

At the heart of the Blockchain is the cryptographic data-structure called Merkle-tree, which was patented by Ralph Merkle in 1979. Merkle-tree efficiently verifies if a particular transaction is valid or not and also provides evidence supporting the claim. The Merkle-tree additionally captures the order in which transactions get accepted. "It is this data-structure that helps Blockchain help achieve security guarantees even when the participants are untrustworthy", says Professor Kamakoti, who leads this project at IIT Madras. However, on the downside, the computational, storage, and energy consumed by Merkle-tree is significant. As a result, traditional Blockchain designs require a tremendous amount of storage, huge computing power and a good network connection, all three of which are scarce in IoT environments.

The problem of adapting Blockchains for IoT environments has baffled researchers for the past couple of years, which is solved by ApproxBC, the solution proposed by researchers at IIT Madras. ApproxBC requires very limited storage and computing resources and can work even when the Internet connection is intermittent. The ApproxBCBlockchain design works by replacing the computation- and storage-heavy Merkle-tree with alternative lightweight cryptographic data-

structures. The key insight here is that alternative data-structures that provide slightly lesser security guarantee will consume far lesser resources. The first variant of ApproxBC replaces the Merkle-tree with another popular data-structure, namely, the Hashtable. Unlike Merkle-tree, Hashtable only captures the evidence of transactions but does not capture their order of acceptance. This relaxation is acceptable in a lot of real-world scenarios and results in huge resource savings. The second variant of ApproxBC uses the data-structure called evidence Bloom-Filter (e-BF), which was invented at IIT Madras. Unlike Hashtable, the e-BF data-structure can only confirm the validity of a transaction with a high-probability (as high as 96%) and not with complete certainty. As a result, it may sometimes' 'claim' that a security event happened, when in reality it did not, leading to inaccuracies. "One of the most difficult aspects of our research was to come up with an optimal design that achieves maximum possible space savings while still having an acceptable level of accuracy.", says Prof. Chester Rebeiro, an Assistant Professor at IIT Madras, who co-leads the project.

Applications that have severe resource constraints can use ApproxBC. Although there is a compromise on the level of accuracy, ApproxBC allows the application to enjoy all other security benefits of Blockchains. ApproxBC, when applied in an IoT environment, results in a conservative approach to ensuring security and privacy i.e. it may perceive a non-threat to be a threat approximately 4% of the time. The researchers argue that when it comes to privacy of common people, false alarms are acceptable. In response to an alarm, an audit can be performed on the ApproxBC digital account book to find out if it was due to an actual security event. In future, the researchers plan to extend ApproxBC to solve many real-world problems such as combating vehicle insurance frauds and power utility management systems.