IoT Security and Privacy Challenges: A Study on Enhanced Privacy Identification (EPID) - Standard based end to end IoT solution.

[1]S.Jaya Prasanna,[2] G. Sri Pradha, [3]Dr. J. Vanathi
[1]Asst. Professor, Department of Computer Science, T.S. Narayanaswami college of Arts and science, Navalur, Chennai 603103
[2]Research Scholar,State Resource Centre, Adyar, University of Madras, Chennai – 600005
[3]Head of the Department, B.Sc IT,Gurunanak College,Velachery Road, Chennai- 600042

Abstract : The next breakthrough in the IT industry is Internet of Things (IoT). Though it's a trending technology now, its concept is not very new to many of us. The foundation for IoT was laid back in early 2000's itself. Mr. Kevin Ashton, the Father of IoT did the groundwork for today's IoT long back [1]. His concept was very powerful but yet simple. If all the devices that we use in our day to day lives have some identifiers and sensors attached to it and if these devices are connected to each other through a network, then these devices can easily communicate between themselves and can also be remotely monitored by other computers. That is what we call as today's IoT. With the level of enrichments in this digital era, we are ready to move to "Network of Things" from "Network of Computers". But as more and more devices join the uncontrolled and complex network, securing IoT systems is a very big challenge. Right from device authorization, authentication, communication, integration every issue needs to be addressed. Various technologies and protocols have been used so far in meeting the above said challenges. Many establishments have been working on providing a secured IoT platform. Intel is one such organization working since 2008 on various approaches towards IoT security challenges.

1. Introduction

The Silicon giant Intel announced its first licencing of Enhanced Privacy ID (EPID) in August 2015. This technology was aimed in secure, scalable and interoperable IoT solutions. This EPID Technology has been adopted by leading companies like ATMEL and MICROCHIP. The SDK of EPID has been made open source and thereby motivating other device manufacturers to choose it as industry standards for device identification in IoT. In this paper, we are going to study the working principle, use cases, advantages and disadvantages of one such Technology Enhanced Privacy Identification, commonly known as EPID which complies with the Trusted Computing Group standards. [2]

2. What is EPID?

Enhanced Privacy Identification has been implemented mainly to address two major problems faced by the traditional PKI security methods. They are "Device Anonymity" and "Device Revocation". EPID is designed in such a way that it allows group of device's private keys to be combined as one and can be

attached as a common public group key. This public key can be used to identify the signature of a Member by using a private key. This private key is accessible only to the device Member. Hence, it provides a double layer identification security of IoT Connected device. This technology allows any anonymous device to be revoked from the network even without the knowledge of other devices in the network. Giants like Atmel and Microchip are using EPID as a common security platform for IoT Security.

PKI Limitations:

Public Key Infrastructure (PKI) provisions the supply and identification of encryption keys to permit handlers and devices across the internet to exchange data in a secured fashion. In a PKI, the Certificate Authority is accountable for authenticating all the requests, and for allotting valid IDs to associate to private/public key sets, using its master key. The biggest weakness is that the CA is the solitary point of faith, and failure, and its reliability is strongly dependent on how the CA maintains and securely stores its master key. That's the reason, PKI is fading and is not in good shape for the current IoT and Cloud Scenario. EPID overcomes this limitation because it works on the principle of Identity based Asymmetric Cryptography.

Key Features of EPID:

1. Every device in the IoT network is given an unchallengeable Identification.
2. As the name suggests, it has Enhanced Privacy security when compared to the traditional PKI implementation mentioned earlier in this paper.
3. EPID supports three forms of Revocation namely Private Key Based Revocation, Signature Based Revocation, Group Revocation which enables flexible revocation of a device depending on the scenario.

Roles of EPID:

EPID had three major roles to play:

a. Issuer: Creates and distributes group Id and Keys (public and private) to the Member and Verifier. Issuer also maintains the updated revocation list.
b. Member: The end device in the IoT platform. Members maintain their ID private. All the Members share the same level of access across the network.
c. Verifier: Verifies if the device trust worthy by checking and verifying the EPID signatures.

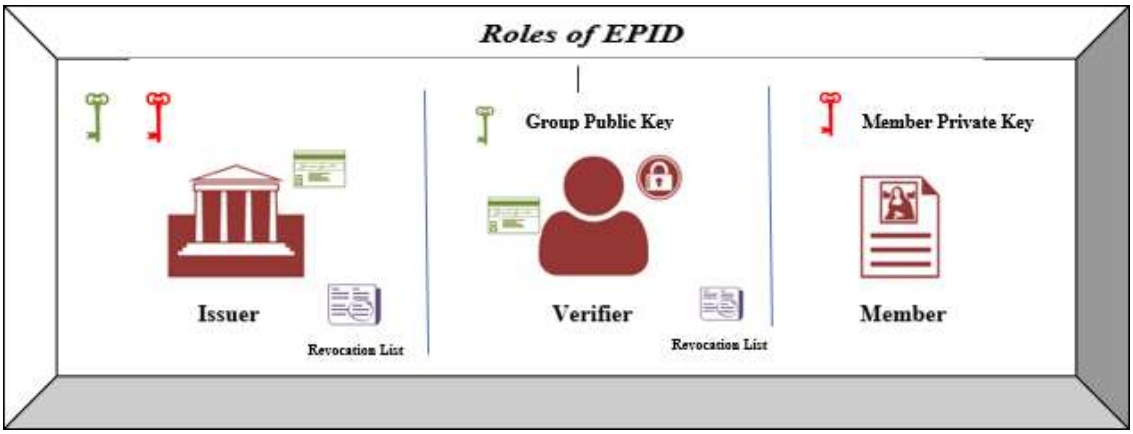
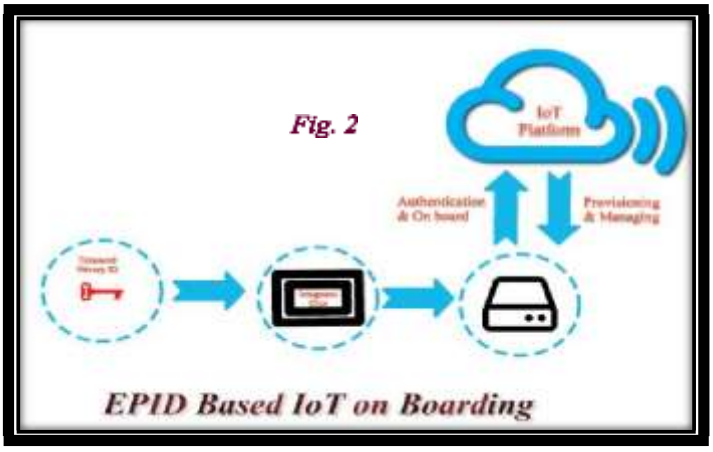


Fig 1: Roles of EPID

How does EPID w ork?

The first step to enabling EPID is the on boarding process. Privacy that is secured at the time of designing (PbD)[3] is an effective solution for many IoT devices. The EPID key is first embedded in the device during the manufacturing process itself.

This embedding the security key in the device enables increased security and doesn't require any human intervention thereafter on boarding. [5] Later, the vendor or the Member request to join the network. After receiving the new Members request, the Issuer generates the public key for the group and the private key for the Member. The private key is stored in the Member's storage area and is not shared with any one else in the network. The Issuer also destroys the private key of the Member after storing in the device. Whereas, the public group key is stored with the Issuer for future references and is also shared with Verifier. Now the Member is deployed in the network.



After adding the device to the network, the next step is Provisioning. By this, we mean to authenticate the newly added Member using the EPID digital signature which will be used for all future transactions. This job is done by the Verifier. The Member can request for the Public group ID from the Verifier. This request is acknowledged by sending the Public EPID key to the Member by

the Verifier. Now the device stores both its private Key and this public Group ID key in its secure storage.

EPID technology allows anonymous sharing of data across the network. Because of this, it becomes necessary to check whether the data is shared to the trusted device or to a counterfeit device. This is taken care by a process called Revocation. [4] The Issuer can revoke either a member, or a set of devices in a network or the entire group depending on the requirement. The entire flow of these processes is depicted pictorially below:

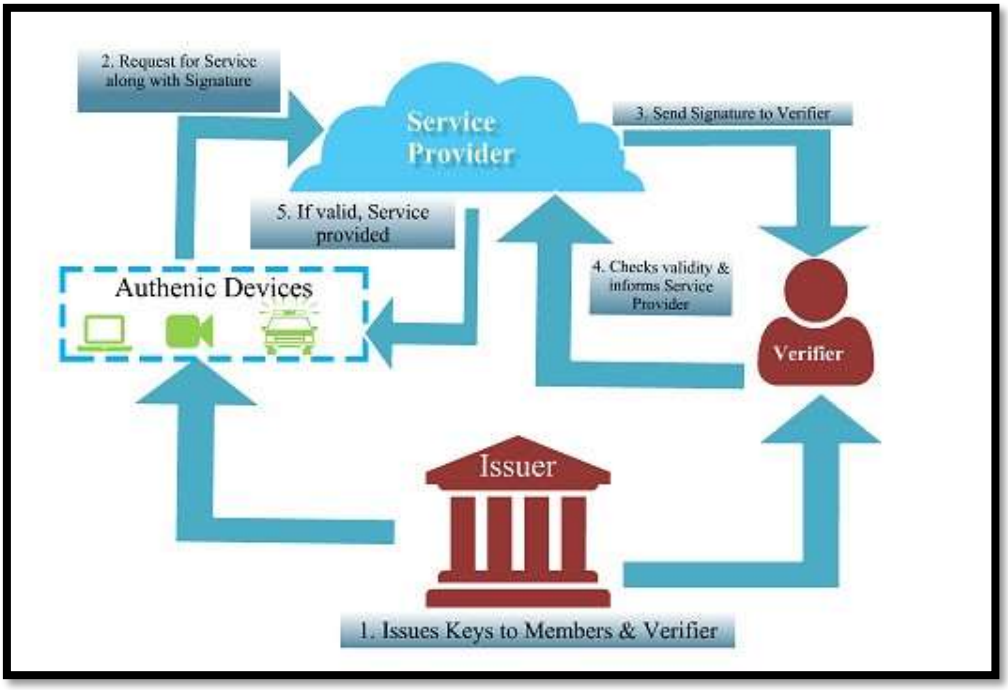


Fig. 3 EPID Process Flow

Use Cases of EPID:

1. **Wearable Technologies:**

   Health gadgets are being used increasing now a days to keep a track of our health parameters. This is one area where strong security is required to keep our personal data safe and secure. If any particular person wants to share his/her personal vital parameters to a general physician and also to a team of research Members, the same can be passed in the IoT network with EPID devices. The details are shared to the physician with all the particulars including the patient names and medical history etc. Whereas, the research team gets only the basic date required without revealing the identity and other personal details. This is illustrated in the figure given below:

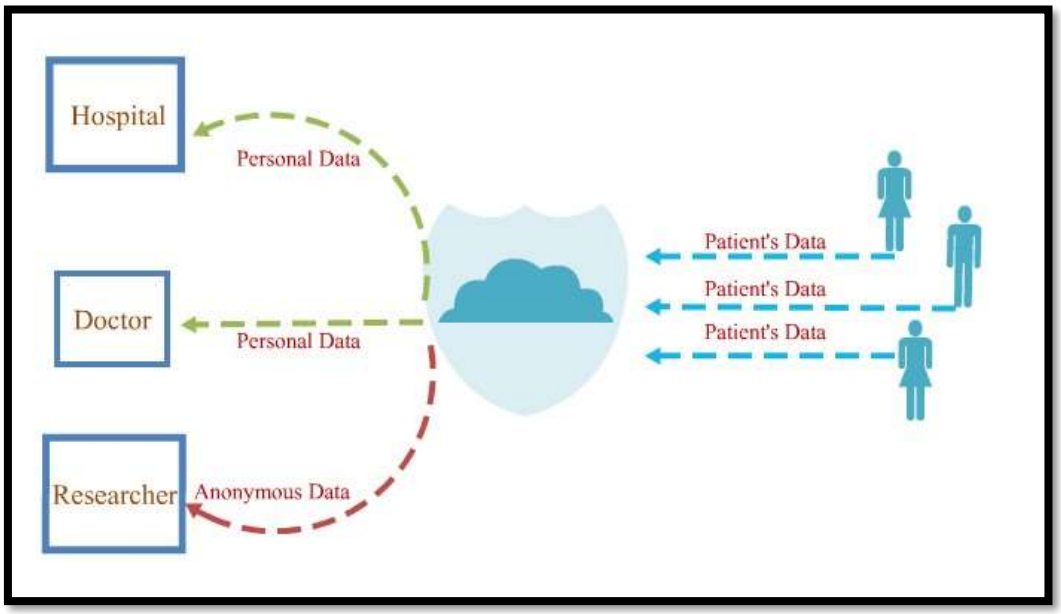


Fig 4. EPID for Protected Health Information (PHI)

2. **Financial Transactions:**

Security is the utmost concern when any finance related transaction over the network. This is one compelling domain target for hackers always. By combining Data Protection Technology (DPT) and EPID based hardware protection we can achieve end to end solution to protect any transaction. The moment a transaction is initiated the encryption of sensitive data takes place.

Any unencrypted data is processed in an environment that is both physical and logically secured from the application or the operating system or the memory of the Point of Sale (POS) Device.

3. **Connected Cars:**

EPID allows authenticating a device with or without anomality. This flexibility allows any device to share the data partially or fully to any other recipient device. Connected cars can stand as a very good example in this scenario. If a car owner wants to share his car's real time data to a trusted mechanic for some predictive maintenance that can be done with EPID. In case, if the same car owner wants to send only limited and restricted data to some traffic sensor the same can also be sent, thereby enabling a flexibility to the owner to share the data he/she wishes to share with privacy tailored in accordance to the situation.

Pros of EPID:

1. EPID is open source, in the sense, any IoT manufacturer can embed this chip on to his

device.

2. It provides excellent security solutions to most IoT challenges like Password Hacking, Man in the middle attack and DOS attack.
3. EPID would allow the manufacturer to authenticate remotely that the device in the network is genuine and is not counterfeit.
4. EPID solution is dynamic, in the sense, the Keys can be generated during the time of operation.
5. Cost model is calculated in terms of cost/devices in contrast with traditional PKI model of cost/Key Used.
6. EPID is contributed towards ISO/IEC (20008 and 20009) and also towards Trusted Computing Group (TCG) Standards. [6]

Cons of EPID:

1. The obvious disadvantage of EPID is, its exclusive for Intel. Though it encourages the usage of EPID in manufacturers devices, the licence is held with silicon giant.
2. The manufacturer should redesign or modify their product design to inculcate a third-party chip in their device which definitely incurs an increase in their cost.

3. Conclusion

In this paper we analysed and discussed the security and privacy challenges based on Enhanced Privacy Identification (EPID) standard IoT solutions. We first discussed about the limitations of Public Key Infra structure (PKI), and then briefed about EPID key features, roles, working method, use cases, pros and cons of EPID. Because of the said limitations, EPID remains a restricted solution for IoT deployment. It is predicted that by 2020 more than 30 billion connected devices will be in IoT Network. With such high predictions, it's sure that many organisations are currently working towards providing effective IoT solutions that are scalable, adaptive and easy to implement. If more such low cost, low risk foundations for IoT solutions emerge, then this will definitely help the IoT industry to move forward with greater confidence, security and reliability, making it a boon to the generations to come.

References

1. Sarma, S., Brock, D.L., Ashton, K.: The Networked Physical World. TR MIT-AUTOIDWH-001,MIT Auto-ID Center (2000)
2. Ruan X. (2014) Privacy at the Next Level: Intel’s Enhanced Privacy Identification (EPID) Technology. In: Platform Embedded Security Technology Revealed. Apress, Berkeley, CA
3. P. Porambage, M. Ylianttila, C. Schmitt, P. Kumar, A. Gurtov and A. V. Vasilakos, "The

Quest for Privacy in the Internet of Things," in IEEE Cloud Computing, vol. 3, no. 2, pp. 36-45, Mar.-Apr. 2016.

4. E. Brickell and J. Li, "Enhanced Privacy ID: A Direct Anonymous Attestation Scheme with Enhanced Revocation Capabilities," in IEEE Transactions on Dependable and Secure Computing, vol. 9, no. 3, pp. 345-360, May-June 2012.
5. Intel Corporation: Security Device on Board https://www.intel.com/content/www/us/en/internet-of-things/solution-briefs/iot-provisioning-with-intel-secure-device-onboard.html
6. Intel Corporation: EPID Fact Sheet http://download.intel.com/newsroom/kits/idf/2015_fall/pdfs/Intel_EPID_Fact_Sheet.p df