A Potential Threat to Security and Privacy Base on IOT

Shaikh Fiza Hamid
Department of Computer Engineering, Sharadchandra Pawar College of Engineering, otur, Pune India

Abstract **- Consumers Electronic IOT products are made with an improper security. Without proper security on this consumer electronic IOT products anyone like hackers can access the user data and the hacker can misused it. After getting the information the hackers can demand for anything to the user. In this paper we will use the five different acts for the security purpose which are BORROW, RENT, GIFT, RESALE, and RETIRE. In borrow process the IOT consumers takes the products, and another consumer uses with the intension of return after usage. In the rent process the IOT consumers takes the products and give it to another for the temporary usage and put charges on the products. In gift process the IOT consumers buy the product and give it to another without taking any charges or return after usage. In resale process the consumers resale the used product or bought previously product. In the retire process the IOT consumer throughout the used product or the product when it became out of services. But the retire act become "IOT Waste" and by this hacker can easily access the consumer information and it can misuse it. we have mentioned some challenges in this paper. And at last, we will tell about how you should use the IOT product with full of security and privacy without getting your information misused.**

Index Terms **- Internet of Things (IoT), Security & Privacy, Trust, Consumer Electronics.**

I.INTRODUCTION

The term Internet of Things was invented in 1999 initially to promote RFID technology. The popularity of the term IOT did not accelerate until 2010/2011 and reached mass market in early 2014. The Internet of Things definition is "Sensors and actuators embedded in physical object are linked through wired and wireless networks.

As we are going through our daily life the communication between user and electronic devices has become very easy. It has become very important part of a human life. We can normally see the communication between mobiles, tabs, laptop etc. but from nowadays we see the communication between washing machine, refrigerator, televisions, cars etc. the IOT devices or products is very good technology that human can use and operate properly. The IOT products are very understandable devices. The IOT products has reduced the workload for human being. Such as it stores the detailed information shares the personal information, health related information, daily conversations, banking details etc. using the IOT products the human work became very easy and comfortable, but there is one disadvantage in IOT devices that it stores the detailed information of the consumer. After storing the information, the information is viewed in the company and to the third party as well without the permission of the consumer. and this led to the crime because the hacker or intruders can misuse the consumers information.

After getting the consumers personal information it can demand for the wrong decision. If the consumers did not full fill the intruders demand he can damage the personality of the consumers which will lead to lifetime loss for the consumer. from this incident the IOT consumers are afraid to buy the IOT products. After seeing this the company is putting their full efforts on the IOT products with full of high degree on security and privacy.

While purchasing the IOT products the consumer confirm about the devices are durable and it will remain serviceable and fully functional.

In case of recycling, trading, selling, replacement and donating or throwing the IOT product this will lead to IOT waste and from this waste the intruder can misuse the consumer information without permission of the consumer. For this disadvantage we have created five acts to overcome this problem. Which are Borrow, Rent, Gift, Resale, and Retire.

Fig.1.Five Acts for Future Security and Privacy

The IOT devices and products service two purpose First is used for the general-purpose tasks for consumers comfort. And second one is when the product became IOT device it connects with the internet and communicate with other devices. with this five Acts it provides the security and privacy on the IOT product. The first act is Borrow in this process the IOT consumers takes the product and give it to another consumer for the use purpose and it uses with the intension of return process. The second Act is Rent the IOT consumers buy the product and give it to another and put charges on the services. The third Act is Gift the IOT consumer buy the product and gift to another consumer without putting any charges on it. The fourth Act is Resale in this act the IOT consumer sale the used or previously bought the product. The fifth act is Retire is the IOT product is thrown out when it became out of service and from this act it became "IOT Waste" and it is the big gate ways for the intruders to access the consumers personal information.

The main concepts to understand from this paper are as follows:

1. The First to Present the ecosystem of the IOT on the consumers devices and its different phases which are highly trained to collect, store, share, and communicate consumers private information.
2. The present five act which provides security and privacy on the IOT products. and this act has been explained further with case studies.
3. There are some IOT challenges which have to be resolved.
4. Some recommendation to be followed for the security and privacy purpose to the consumer.

The structure of the paper as follows: II. Section consists of five acts. III section consist of consequences of privacy breaches. IV Challenges, V case study VI section consists of Recommendations of the IOT product. VII sections consist of Conclusion. VIII section consist of References.

II. FIVE ACTS OF IOT

The casual life of consumers daily life task has become very easy with this IOT products. the eco-friendly IOT products are easy to understand to the consumers and due to this the IOT came in demand and the consumers are interested in buying the IOT products. all these IOT product goes through a particular life cycle three major phases Beginning of Life (BOL) Middle of Life (MOL)End Of Life(EOL).

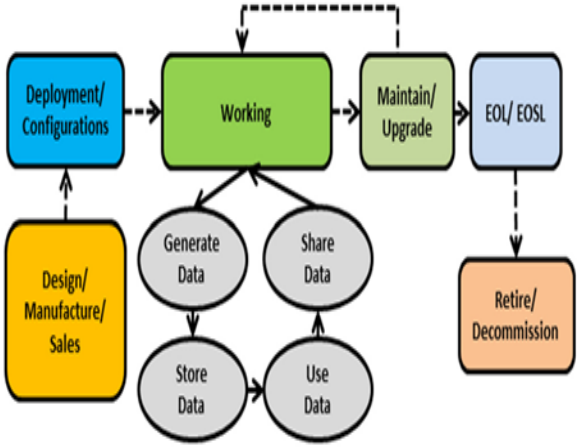

Fig.2. life cycle of IOT products

This is the life cycle of consumer electronic IOT products .it is a very simple and easy process to understand for any consumer. As we can see in fig.2 how it goes step by step and at last it become IOT waste.

Firstly, it gets properly designed. then deployment process is done to the consumer. then the consumers generate his data in the IOT product then the IOT device store data in it then the consumer use the data according to his work purpose and comfort. It shares the data and process is going further. After that maintain or upgrade process is done then the product become end of life which means the product become out of service and it thrown out. By throwing this product it will get access again by the hacker and it will misuse the personal information. To overcome this disadvantage the second fig is shown.

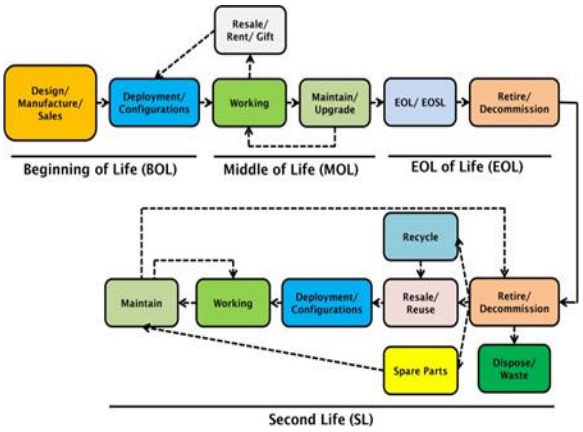

Fig.3 second life cycle of CEIOT product

As you can see the second lifecycle it is somewhat same to first lifecycle but after retire process the recycle process is mentioned in this life cycle. after recycle process if it works again, it gets resale or reuse if not then spare parts are taken out from the product and used in other CEIOT product and again deployment is done and working process starts and it became a used IOT product. this second life cycle demonstrate fully five Acts and it gives proper security and privacy to the consumer.

A. ACT OF BORROW

In the Act of Borrow the IOT consumer buy the product and another IOT consumer uses the product with the intension of returning after use. For example, one of our family relatives take the car for the use purpose and he is going to return the car after his usage complete. the owner is connected to car with help of any type of network like tracker etc. but the all the information of the car is connected to the main owner and this can lead to circulation of the personal information without the permission of the owner or first consumer.

B.ACT OF RENT

In the Act of Rent the consumer takes the IOT product and give it to the another IOT user and put the charges on it and the consumer will pay the charges till he uses the IOT product .Nowadays we are seeing the smart houses .in smart houses all are electronic device which is fully depend or connected to the owners details like voice ,physical touch etc. the smart houses do the all work by sitting at one places he can share the information ,store the information , communication is done ,health related information is stored . by seeing all this process, the hacker can hack the house system easily and can mis use the information, and he will know how he can manipulate to the owner because all health-related information is stored in the house system. So, we should store the health-related information offline to be safe from the hackers.

C. ACT OF GIFT

In the Act of gift, the consumer or owner willingly want to gift the product to another person without any payment charges. He can give the use product as a gift to the consumer means second handed product but in this second handed gift it may get some risk of getting personal information misused because using second handed product first owner information may get access to the second user, he can use it any ways. So, we should always format the whole information from electronic devices which will be safe for the user only.

D.ACT OF RESALE

In this Act the consumers sale the used or previously bought product to any other person for the use. It will be sailed as s second handed product to IOT consumers. For example, a consumer brought a smart TV and used for some time and resale again and bought a new smart android tv.so this is the process of resale.

E.ACT OF RETIRE

In this Act the consumers throw out the product when it became out of service or the product has got expired. The consumer should properly dispose the product. the consumers should erase all the data from the expired product. if this process is not done the hacker can access the data from that product and he can misuse it.so the consumer should properly erase all the data.

III. CONSEQUENCES OF PRIVACY BREACH

We have seen that the IOT is connection device .it is a communication device with each other. And from this connected device any hacker can hack the information of the consumer. IOT product stores all the information at a cloud. cloud is one type of backup for the user in case it gets destroyed from the user. then user can easily access his information by just logging id and password. We have categorized this privacy breaches in three parts. First one is Hacker can use the consumers private data for his financial purpose. Second one is the hacker can share the private

information of the consumers for any bad intensions. Third one is the hacker or intruder can demand for the wrong decision to the consumer.

A. Use of Private Data for Financial Purpose

In this point the hacker can use the consumer personal or private data for his financial purpose. And he can black mail to the consumer.

B. Share Private Data for Bad Intension

In this point it is said that the consumer should delete or destroy the whole information from the device because if the hacker gets successful in accessing the consumer information he will share or circulate whole information with bad intension and he can damage the reputation of the consumer.

C. Manipulate Private Data for Wrong Decision

In this point after getting consumers personal information the hackers can demand for wrong decision and if it is not fulfilled then they can damage the consumers reputation.

IV CHALLENGES

The internet of things (IOT) has quickly become a huge part of how people live, communicate, and do business. All around the world, web-enabled devices are turning our world into a more switched –on place to live either.

A. SECURITY

Ask any security expert about the biggest headaches of the 21st century and they will likely bring up IOT devices. The reasons? In cyber security terms, IOT devices greatly expand the "attack surface", or the amount of potential areas for cybercriminals to penetrate a secure network.

Cybercriminals do not have to crack an IOT devices plastic enclosure to access sensitive materials. they can simply finesse their way in through one of the many security vulnerabilities that are found throughout the IOT. Many IOT devices have default passwords left unchanged unpatched software and other major security vulnerabilities.

B. REGULATION

The lack of strong IOT regulations is a big part of why the IOT remains a severe security risk, and the problem is likely to get worse as the potential attack surface expands to include ever more crucial device. when medical device, cars and children's toys are all connected to the internet it's not hard to imagine many potential disaster scenarios unfolding in the absence of sufficient regulation.

Quality control in IOT can be particularly tricky from a regulatory perspective. With huge numbers of IOT devices now being imported from countries like china that have different standards of quality and security many experts are callings for strong and universal security standards for IOT technology.

C. COMPATIBILITY

New waves of technology often feature a large stable of competitors jockeying for market share and IOT is certainly no exception. This can be good news since competition creates increased choices for consumers, but it can also create frustrating compatibility issues.

Continued compatibility for IOT devices also depends upon users keeping their devices updated and patched which as we have just discussed and be pretty difficult. When IOT devices that have to talk to each other are running different software versions all kinds of performance issues and security vulnerabilities can result. That is a big part of why it's so important that IOT consumers keep their devices patched and up to date.

D.BANDWIDTH

Connectivity is bigger challenge to the IOT than you might expect.as the size of the IOT market grows exponentially some experts are concerned that bandwidth intensive IOT applications such as video streaming will soon struggle for space on the IOT current server client model.

That is because the server client model uses as centralized server to authenticate and direct traffic on IOT networks. However as more and more devices begin to connect to these networks, they often struggle to bear the load.

E. CUSTOMER EXPECTATION

It's often said that it's better to under-promise and over –deliver many IOT manufacturers have learned this the hard way, with IOT startups falling often and leaving bewildered customers in their wake. When customers expectation and product reality do not match the results can be system failures orphaned technologies and lost productivity.

With such strong competition in the IOT market, customers whose expectations are not met hesitate to go elsewhere. Business looking to enter this competitive and innovative sectors should be prepared for a market that never sits still and customers who always want a smother and more advanced experience.

F. LACK OF CONSUMER AWARENESS

In this challenge the consumer did not know about the IOT device how it works and how. The consumer even not know about how, when, where the consumer information is store and who can see the information.so the consumer should be aware of the IOT device.

1.HANDLING IOT WASTE AFTER END OF LIFE

In this point we see that any product or anything has some expiry date. But for any product the destroy process is there. how the product should be destroyed. In this IOT devices if the product became end of life or out of service then it is thrown out and it became IOT waste from this IOT waste the hacker can easily access the consumer personal information and he can misuse it. And he can damage the reputation of the consumer .to overcome this disadvantage the non-tech savvy or non-hack savvy handle this IOT waste. And they stored the IOT waste.

V. CASE STUDIES IN IOT

As we have seen our five acts such as (borrow, rent, gift, resale, retire). With this five acts the security and privacy can be maintain and the working of the IOT device is maintain as well. In this another reason occur that is high cost of the product. some of the IOT product are cheap such as electric bulb, door lock etc. it can be repair easily and maintain properly. But some of the IOT products are expensive such as washing machine, smart TV. but if this thing gets out of service, then its spare parts is too expensive to repair the IOT device. In that case consumer thinks that instead of repairing it we should buy new product with year warranty and two-time service free. Here we have seen two case studies.

A. Case Study of Smart TV

As we are going to the modern world all work of human become easy. our case study is on smart tv as we are seeing in old time television the does not have any extra functional like recording, searching music, etc. but now a days we can all these functional are available at smart TV. And more and more people are attracted to it. The smart TV store the owners choices data such as which song owner want to listen etc. in case if the smart TV display gets damage and it's not showing any it's multimedia. Then instead of repairing it he can choose to buy new smart tv, because the new product gives years warranty and services free. the damage product consumer cannot resale because all the information is stored in that device like watched history, video recordings, etc. if it goes in wrong hand, he can misuse it and he can damage the reputation of the person. So, the consumer should dispose the product properly. A recent study shows that the information can access by using some backup tools or some use of software and it can be removed or deleted from the product. From this process the consumer can disposed the product easily.

B. Case Study of Smart Refrigerator

As we know that refrigerator its work is to cool the things .in this product the company does not take any seriousness about this product. in case it is not working properly it can be repaired again and it can work as usual. But these things depend on the consumers financial condition whether he can afford it. If the consumers financial condition sounds good, it can be possible other than the consumer have to buy the new product. if the consumer has to buy new product, he can gift the old refrigerator to the relative. The consumer can gift the product as a charity institution.

VI. RECOMMENDATIONS OF IOT PRODUCT

In this section we are here to tell you about some recommendations related to this IOT product security and privacy. Here are three different recommendation a consumer, a manufacturer, an internet service provider (ISP). As shown the in the fig 4. we will see one by one in this section.

A. Recommendations for CEIOT manufacturer

In this section it is totally dependent on the manufacturer of the CEIOT product. Such as (hardware and software) and service provider (cloud, utility etc.). From making of life to end of life. Of the product. The manufacturer should check the product whether it is working properly or not. the information is storing or not and various things. They should make the proper product if the product update came it should

remind to the user before it is getting out of updated. They should also see that in case it gets out of service the consumer wants to retire the product then all information gets deleted or logoff from the product and make sure the product is dead. Because of product the consumer profile should not be damaged. the product should store only important information not more detailed information about the consumer. As fig 4 shows the process.

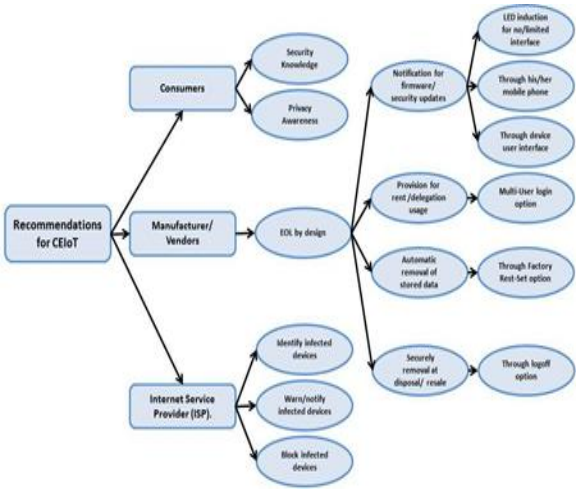

Fig .4. Recommendations for CEIOT product

B. Recommendations for CEIOT Consumer

In this section it is said while purchasing the IOT product the consumer should be aware about the product how to use. the consumers main responsibility to take his information security. while buying the IOT product he should take detailed information about the product. And how to dispose the product when it gets out of service. Before disposing the product, he should make sure that all information has been deleted and the product is totally dead. by doing this he can be safe.

C. Recommendation for Internet Service Provider

In this section it is said that the internet service provider should always be careful he can tell whose data is hacked and he can catch the hacker through the IP address of the computer. He can also tell the consumer that whether his information generating too much on the product. and it can be hacked easily. the internet service provider should aware the consumer to store the less information on the IOT product.

VII. CONCLSION

From this paper we have studied much more about the Internet Of Things(IOT).then somewhat history of the IOT in the Introduction part .we have seen five acts which are Borrow, Rent ,Gift ,Resale Retire and their work .how they provide security and privacy to the product .by doing this five process the product will be in working condition and provide good output.in the next section some consequences of the privacy breach how the hacker can misuse the consumer personal data and can demand for the wrong decision .after that we have seen challenge of the IOT product six challenges. then how to handle the IOT waste. this is the main point of the paper because if the product is thrown directly the hacker can easily access the information of the consumer and he can blackmail to the consumer, so this was the main point in this. Next section was case study two case study was there first is smart TV and second is smart refrigerator .in case study we have learnt that before disposing the product we should delete the whole information and make sure that the product is totally dead. Next section was recommendations there were three recommendations first manufacture, second consumer, third is internet service provider. In this recommendation main point Is while buying the IOT product the consumer should be aware of the product and he should take detailed information about the product how to use and how to dispose after it get out of service. And at last, from this paper, we learn about how we can put security and privacy to our information on the IOT product. And how can we be safe.

REFERENCES

[1] Wazir Zada Khan, Senior Member, IEEE, Mohammed y Aalsalem, Member, IEEE, and Muhammad Khurram Khan, Senior Member, IEEE, “Communal Act of IOT Consumer: A Potential Threat to Security And Privacy”.
[2] https://www.iot-now.com/2020/06/03/103228-5-challenges-still-facing-the-internet-of-things/
[3] https://iot-analytics.com/internet-of-things-definition/
[4] https://en.wikipedia.org/wiki/Cloud_computing
[5] https://www.altexsoft.com/blog/business/11-key-enterprise-iot-security-recommendations/
[6] https://bridgera.com/iot-waste-management-renewing-the-face-of-waste/