Security and Privacy in Smart Systems

Manohar Mohith*, Naresh E, Vijaya Kumar B.P****
Dept. of Information Science and Engineering, M. S. Ramaiah Institute of Technology, MSR Nagar, Bengaluru, INDIA

Abstract- Smart systems are those that have the capability to modernize the way that perform daily activities, the applications of smart are extended but not limited to the way in which do some of the basic activities like start a car. Nowadays, even the government equipment are coming up with fascinating technologies to improve efficiency of its performance. These systems however also present the same amount of vulnerability as that of advantage. This is precedent to the fact that all of these smart systems have data vulnerability and many other privacy breach issues based on the type of its application. However, this should not be a factor to hinder innovation and this brings up the necessity to protect and preserve privacy.

This paper discusses about a smart system, it's technological stacks and security issues which evidently provides extensive basis to the Security and Privacy of these systems. It starts with the definition of a smart systems in an ecosystem considering a car as an example, it examines the various vulnerabilities in details considering the recent breaches by Cambridge Analytica as well. A mathematical approach to the cause of data breach has been considered to analyse its effects and finally the technological approaches to solving this issue. This paper explains not only about the existing approach to security but also the modern day practices to resolve it.

Index Terms- Smart Systems, Internet of things, Artificial Intelligence, Vulnerability, Security.

I. INTRODUCTION TO SMART SYSTEMS

What are smart systems? When the word 'smart' is used as an adjective with any of the common things present in this world, the general idea is that it has modern technologies integrated with it which may lead to, but, is not limited to reducing costs, improving conditions of living, decreasing time of processing, increasing scalability, feasibility, etc. It is the cluster of these smart systems that constitute the rapid growth in technology in today's modern world [1].

A smart system in the field of Information Technology is with respect to the Internet of Things(IoT) that maybe, in simple words, either controlled by humans in order to achieve something smart or autonomously programmed in order to solve some of the emerging problems due to the rapid technological advances. To do a set of inbuilt commands in either of the cases is IoT, while on the other hand, if it has the ability to learn from itself then it has Artificial Intelligence integrated into it. Nowadays, 'smartness' has been integrated into almost every small thing around us that eventually has built up to form one large smart ecosystem [11, 7].

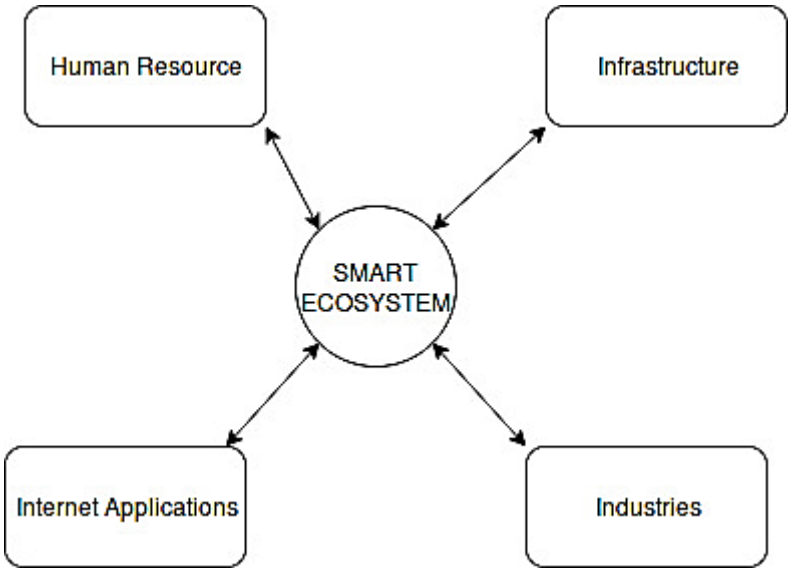

Fig 1. Smart ecosystem

II. WHY SMART SYSTEMS (IN THE FIELD OF IT)?

In the field of Information Technology, in order to ensure only forward growth in the technologies and no repetitions or redundancies, the connectivity or network plays an important role in this case as well as to integrate cognitive abilities in the systems used in daily life thereby to give it 'smartness'. This connectivity, as shown in Fig 1, which denotes the ecosystem as a whole plays an important role in improving the efficiency of the system which is the main intention [11, 7].

The two main reasons in general for using smart systems are:

- User ease of experience
- Machine adaptability and efficiency
  [Here, efficiency refers to multiple parameters like speed, time, computing power, etc.] [7, 1]

Each system has its own perspective of how it can be improved in order to either improve its efficiency or improve the user experience, thus justifying its requirement in today's world.

III. SECURITY IN SMART SYSTEMS

First of all, the main question that has to be addressed is, why security? If the systems are so smart and integrated with intelligence (Artificial Intelligence), then why do they require security? To understand this, let us consider a case study of a smart car and then summarize few of the general points of security breaches in smart systems. There are many safety issues with respect to the driver and passengers as well during the journey, however, we will only be quoting the software vulnerability. [11, 3]. As a side note, to be clear, these vulnerabilities are only with respect to non-autonomous cars, however, autonomous cars have more vulnerability considering higher connectivity with the internet and other connected devices [16, 8].

3.1. Case study- Smart car: [3]

Let us consider all its applications with respect to every aspect of the car that makes it smart and what are the vulnerabilities in each case [7, 3].

- Interface
- Physical components
- Software Applications

Fig 2. Interconnectivity between smart devices

3.1.1. Interface: [8]

This is the software interface used to connect the user to the hardware of the car thus allowing him/her to make use of the smartness of the car to its maximum extent. As shown in Fig 2, which denotes the smart links nowadays, the connectivity makes the vulnerability of this part of the network to be the highest percentage which can also be linked to the movie 'The Fate and the Furious' that might not be too much of science fiction after all. The interface vulnerabilities could be of the following types: [7, 6]

- Infotainment system & connected networks: [6, 5]
  This is the radio/entertainment system present in the car thus allowing the user to get news updates, play shows and even run many other applications that are related to the infotainment field on the display system screen installed in the car or through the audio system installed (the network has great vulnerability if left unprotected). [10] The main hacks according to recent estimates have been mainly through the smartphones that are connected to the car which makes it easier for the hackers to access and control any of the physical parts of the car through the connected network.

- Navigation: [1]
  This is one of the globally used interface, whether it is to go to an unknown location or a known location. [12, 10] However, the vulnerabilities of this application are numerous especially considering the fact that the current location of the car is being publicly vulnerable to hackers. [5, 3] The attacks can be directly through the data obtained through the cloud, through manually accessing the smart car at its location or even remotely gaining access to the car through the location range at which it is currently on route.

- Advanced unlocking systems: [13, 10, 3]

With the arrival of keyless entry into this world, the vulnerability of the cars has gone up much more than ever expected. The vulnerabilities are shown accordingly in Table 1.

Table 1. Vulnerability of smart applications [6, 3]

Type of smart system	Journey	Vulnerability	Medium of attack	Risk level
Infotainment system + connected network	Pre journey	Data leak/loss	Cloud stored data/Account hack	Low
	During	Car access + data loss/leak	Intruder through car offline/cloud online	Medium
	Post	Easy access of data + full control of insecure car	Through the unknown connected network/ parking area hack	High
Navigation	Pre journey	Destination/relevant data loss	Through destination and house location details noted when connected to cloud	Low
	During	Location/full control of smart car	Cloud based location and other connected networks	High
	Post	Destination/relevant data loss	Through destination and physically vulnerable equipment at the destination	Medium
Advanced unlocking systems	Pre journey	Unlocking of car through connected devices at home	Access to the cloud network connected at home	High
	During	Cloud data loss/sensors hack	Sensors in range of the car	High
	Post	Complete control of unattended car	Sensors in range of the car	High
Smart car control(voice/remote)	Pre journey	Voice tracking/connected remote's vicinity	Manually in range of remote, bugging the car's network	High
	During	Cloud data loss/sensors hack	Not much chances unless manually accessible	Low
	Post	Voice tracking/connected remote's vicinity	Manually in range of remote, bugging the car's network	High

- Smart car control: [13, 8, 5]
  When the term smart car control arises, it is not only with respect to the voice controlled key that is at vicinity and in easily accessible range with respect to the hackers but also the variety of devices that are connected with the car that makes it more vulnerable and easier

to access [13, 12, 9]. The devices themselves can also be hacked to gain access to the car through various sensors and devices at its vicinity.

3.1.2. Physical car components:

When it comes to the physical components of the car, every part of the car that is part of the 'smart' network is at huge risk if left unattended without proper security measures. Especially considering the plethora of functions that can voice/app controlled from devices such as the mobile, laptops, etc [13, 12, 10].

- Radio
- Digital display
- Air conditioning
- Windshield wipers
- Wiper fluid
- Transmission
- Brakes

All these car components are left to become extremely vulnerable when connected to the cloud however, what really is disturbing to know, are all the controlling components of the car are at the attacker's vicinity [12, 10]. This means that even how our car goes physically on the road is also at stake which raises a lot of safety issues as well [8].

3.1.3. Software Applications: [3]

These can be a wide range of software starting from the messaging app used in the car to the keyless control that is used in the car [5]. Any app basically connected to the car in turn to the cloud is vulnerable to attack either through the cloud or through the app used in the car. The access to this is partly our fault as well, considering that the data given to these apps are in abundance basically, pointing out where and when to attack. This clearly indicates the importance of using trusted apps over networks [13, 12].

Despite trust of the apps over a network, [6] the user is still liable for managing their own private data which is clear from the data that was being misused through the Cambridge Analytica incident which clearly proves, anything is possible if data is not protected.

The country-wise data, as per Fig 3, which denotes the Vulnerability data provided by Facebook during the recent data breach by Cambridge Analytica, clearly distinguishes the fact that smart connected networks are highly vulnerable to attacks since the United States is clearly abundant with the smart cars network. An example to prove the previous statement lies with Tesla [4]. which has integrated the smart network in such a way that if one car is successfully penetrated, the entire network of cars is open to vulnerability [9, 6, 5].

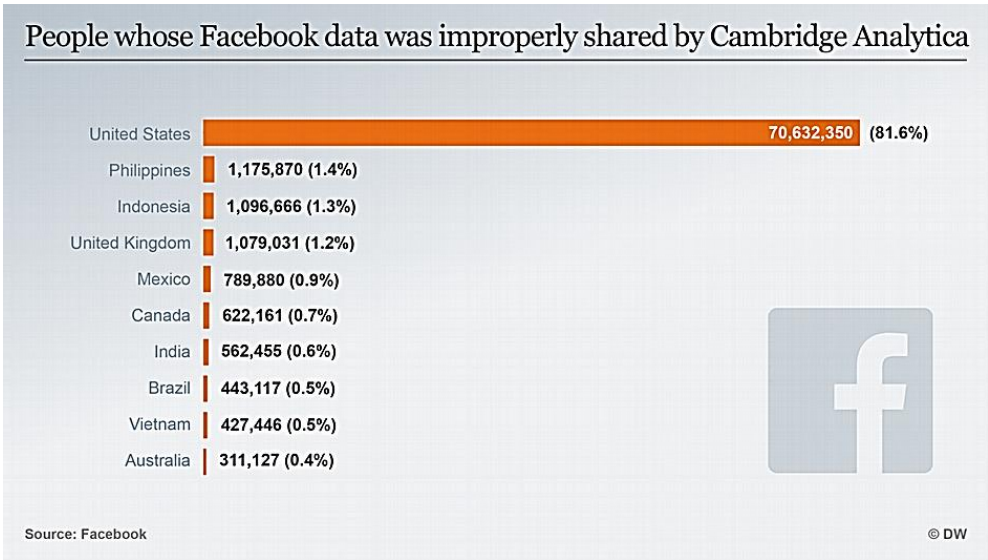

Fig 3. Vulnerability of data due to Cambridge Analytica (Country wise), by Facebook

The further part of the paper clearly discusses the general points of the security of smart systems, i.e., Why, what happens and how to stop it?

IV.CAUSES – VULNERABILITY AND THE NEED FOR SECURITY IN SMART SYSTEMS

With the exponential growth in the technology in today's world, it is very important to keep the smart devices safe. Also, considering the fact that all smart devices are interconnected. [12, 3]

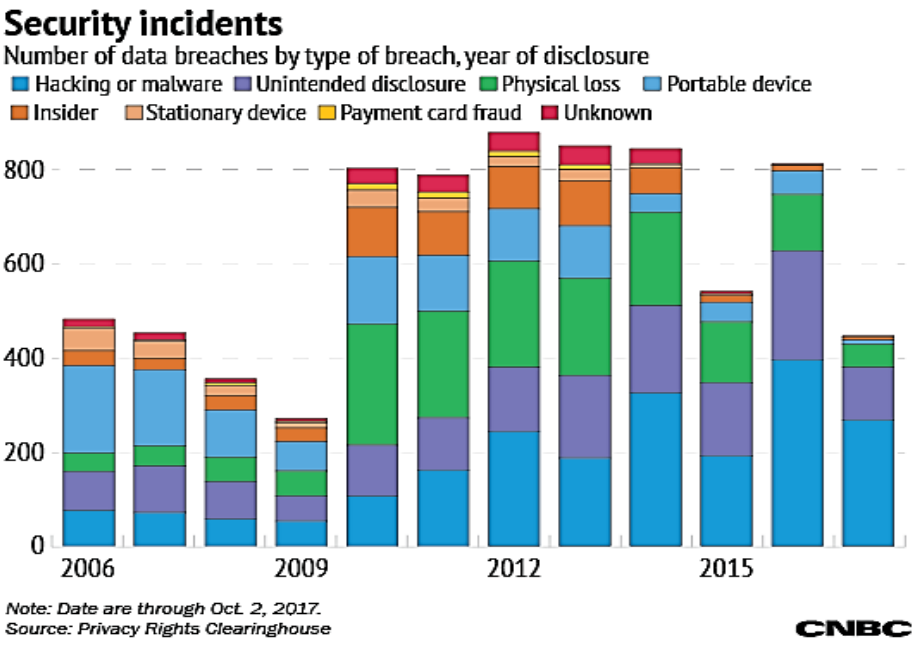

Fig 4. Security vulnerability of smart systems by type, by CNBC

Let us now consider the ‘v’ as amount of vulnerability of smart devices and ‘y’ the year under consideration. It is clear from Figure 4 that one conclusion can be drawn: [9]

$$v \propto y \quad \ldots(1)$$

Converting it into an equation, we need to assume a constant ‘k’ which represents the amount of vulnerability based on the smart device.[14]

i.e., $$v = ky \quad \ldots(2)$$

k is lesser for non-connected network smart devices than the connected ones. Also , if ‘n’ represents the number of smart devices, then, from Fig 4, which shows the statistics of data breaches, based on type provided by CNBC in the year 2017, we get

$$n \propto 2v \quad \ldots(3)$$

This clearly proves that, as the years go by, due to the increasing availability of smart devices to every individual, the vulnerability is going nowhere and on the contrary it is essentially doubling its rate [16, 10].

V. EFFECTS – WHAT DOES BREAKING INTO SMART SYSTEMS DO TO YOUR DATA

The main thing to be addressed are the concerns to what are the consequences of break-ins to the smart devices. With the existing technology of cloud connected devices, the vulnerability issue is now a major concern considering that all the devices are synced over the cloud, in other words, if one system is hacked, all the systems are doomed. However, what does it mean to be ‘doomed’? Some of the major concerns to smart hacks are listed below: [16, 2, 1]

- Data breach: [5]
  The main loss that occurs due to an attack is the loos of sensitive data that leads to a lot of other interconnected losses. [17, 15, 14] For example, loss of the car password through an attack might lead to the loss of the control towards the car and makes the user prone to safety.

- Control of smart devices: [15, 14, 12, 8]
  With the rising of use of Tech Giant’s latest cloud sync technology, it makes all the smart devices connected over a cloud vulnerable, meaning that if one of the device is attacked, it could mean an entire takeover of all the smart devices owned.

- Financial loss: [5, 1]
  This is the most unfortunate consequence of all the effects of an attack on any smart device. Devices may be targeted and attacked for financial benefits by the hackers, which is a nightmare if any of the smart devices contain sensitive financial information stored in it [15].

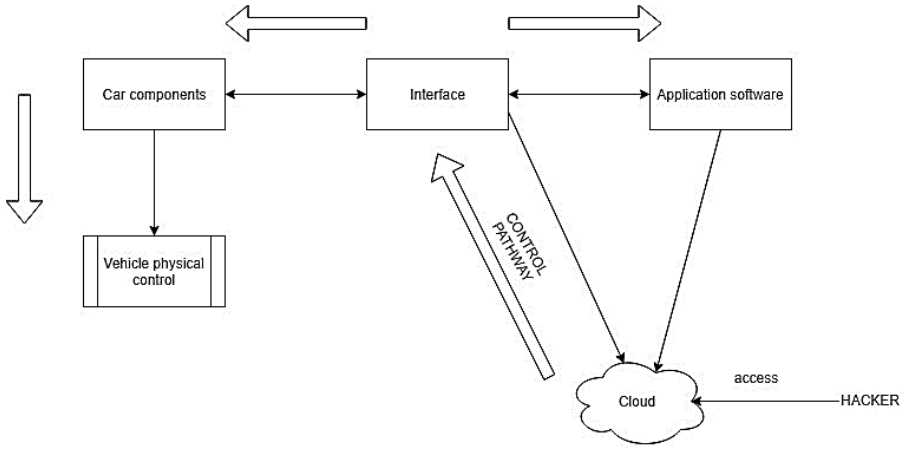

Fig 5. The vulnerability pathway access in smart cars [2]

Fig 5, which denotes the pathway of travel of control through the entire Smart network based on self-research, is an example and insight into what might happen if a hacker is able to get hold of one part of a network and thus increase its exposure, especially that of sensitive data. [17, 6]

VI. MEASURES – SECURITY THAT IS CUTTING EDGE AND SHOULD BE USED TODAY

Existing security technology for smart systems: [3, 1]

The existing although might not be that advanced in protection, but protects maximum amount of vulnerability of users against attackers. Some of the basic self-protection techniques include: [18, 10, 3, 1]

- Ensure connection with the manufacturer
- Regular updating of interface/application software's
- Keep smart devices in close vicinity
- Do not disclose sensitive data [2, 1]
- Ensure the genuineness of devices interconnected

Some of the existing technologies to protect these smart devices in pre and post attack include: [1]

- Cryptography/Encryption techniques: [16, 5]
  To encrypt the data within certain parameters that are known only to the user thereby ensuring privacy of data.

- Intrusion detection systems: [5, 3, 1]
  This is to mainly ensure that the smart systems are not taken advantage by detecting intrusion in the first place as a preventive measure to avoid breach in networks. This technique is the most effective measure in terms of costs. It also includes the domain of hash lock mechanism.

- Cyber-Physical Smart Systems: [19]
  This is to provide the smart system an AI based approach to prevent cyber attacks. This follows a concept of integrating both human and system with other systems as well which
  is wholly the entire concept of Tesla that ensures security of its systems through its connected network by learning from each other.

- IoT:
  This is a huge field of applications which if used in the right way, can be pulled over to the security field. From common knowledge, this fits in the field of communication thus involving a lot of the protocols to transfer (E.g.: TCP/IP). This being said, this technique involves providing security while it is being transferred.

All these technologies can be used in order to ensure safety of the smart devices at bay, however they do not ensure the safety of the devices themselves, which ultimately relies on the main fact that the owner has to be responsible [18, 14].

If the device does get hacked despite all these measures, the cybercrime control is the best approach in dealing with the situation. However, the details of which are out of scope in this paper.

VII. CONCLUSION

With the appearance of wireless communication in the car, and the connection of the under-the-hood elements with the outer world, new security threats arise on the area of Connected Cars. ICT security needs penetrate into the vehicles. Because of this, privacy and security of the owner must be handled and the well-known security principles must be taken into account during the design of such system: confidentiality, integrity, authenticity, availability and non-repudiation [23]. With the appearance of wireless communication in the car, and the connection of the under-the-hood elements with the outer world, new security threats arise on the area of Connected Cars. ICT security needs penetrate into the vehicles. Because of this, privacy and security of the owner must be handled and the well-known security principles must be taken into account during the design of such system: confidentiality, integrity, authenticity, availability and non-repudiation [23] With the appearance of wireless communication in the car, and the connection of the under-the-hood elements with the outer world, new security threats arise on the area of Connected Cars. ICT security needs penetrate into the vehicles. Because of this, privacy and security of the owner must be handled and the well-known security principles must be taken into account during the design of such system: confidentiality, integrity, authenticity, availability and non-repudiation [23] With the appearance of wireless communication in the car, and the connection of the under-the-hood elements with the outer world, new security threats arise on the area of Connected Cars. ICT security needs penetrate into the vehicles. Because of this, privacy and security of the owner must be handled and the well-known security principles must be taken into account during the design of such system: confidentiality, integrity, authenticity, availability and non-repudiation [23]

With the rise in the ‘smart’ era, however exciting it is to the people to keep up with the trending technology, [1] it is also important to keep any data or vulnerable equipment related to those smart devices at close quarters and under utmost discretion to avoid it from being misused for various unlawful purposes. This is clearly stated proven from the recent Facebook & Cambridge Analytica data breach incident [9].

In the technical perspective, when we start from the very basics of a system consisting of many smart devices that are connected together in an ecosystem as long as we keep trying to improve the ease of use and machine adaptability, vulnerability always increases exponentially. Whether it is a smart car or any other smart device, it is always open to a data or control breach for either personal/financial reasons of the attacker towards the victim. However, modern day technologies do provide solutions to cope with these attacks that range from cryptography techniques, intrusion detection to cyber-physical systems and IoT.

REFERENCES

[1] Carsten Maple, "Security and privacy in the internet of things", 2017.

[2] Huichen Lin & Neil W. Bergmann , "IoT Privacy and Security Challenges for Smart Home Environments", 2016.

[3] Mauro Conti, Ali Dehghantanha, Katrin Franke & Steve Watson, "Internet of Things Security and Forensics: Challenges and Opportunities", 2018.

[4] Zhen Ling , Junzhou Luo , Yiling Xu , Chao Gao , Kui Wu & Xinwen Fu, "Security Vulnerabilities of Internet of Things: A Case Study of the Smart Plug System", 2017.

[5] Sarah J. Darby, "Smart technology in the home: time for more clarity", 2018.

[6] Tamás Bécsi, Szilárd Aradi & Péter Gáspár, "Security issues and vulnerabilities in connected car systems", 2015.

[7] P. Varaiya, "Smart cars on smart roads: problems of control", 1993.

[8] Fei-Yue Wang, Daniel Zeng & Liuqing Yang, "Smart Cars on Smart Roads: An IEEE Intelligent Transportation Systems Society Update", 2016.

[9] JC Reindl, "With more tech comes more hacking risk for smart cars connecting vehicles to one another and the world around them poses a substantial cybersecurity hurdle that automakers must overcome.", 2018.

[10] Clayton Weeks, "How to prevent your car from being hacked", 2018.

[11] NiluferTuptuk & StephenHailes, "Security of smart manufacturing systems", 2018.

[12] Amara Dinesh Kumar, Koti Naga Renu Chebrolu, Vinayakumar R & Soman KP, "A Brief Survey on Autonomous Vehicle Possible Attacks, Exploits and Vulnerabilities", 2018.

[13] Scott l. Wenzel, "Not even remotely liable: smart car hacking liability", 2017.

[14] Ishtiaq Roufa , Rob Millerb , Hossen Mustafaa , Travis Taylora , Sangho Ohb Wenyuan Xua , Marco Gruteserb , Wade Trappeb & Ivan Seskarb, "Security and Privacy Vulnerabilities of In-Car Wireless Networks: A Tire Pressure Monitoring System Case Study", 2010.

[15] A K M Bahalul Haque, "Need for critical cyber defence, security strategy and privacy policy in bangladesh - hype or reality?", 2019.

[16] Hamidreza Damghani, Heliasadat Hosseinian & Leila Damghani, "Privacy Risks of Hybrid Broadcast Broadband TV (HbbTV)", 2019.

[17] Randall Young,Lixuan Zhang & Victor R. Prybutok, "Hacking into the Minds of Hackers", 2007.

[18] Meenaakshi N. Munjal, "Ethical hacking: an impact on society", 2014.

[19] Prof. Dr.-Ing. Reiner Anderl, "Industrie 4.0 - Advanced Engineering of Smart Products and Smart Production", 2014