International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 07 Issue: 06 | June - 2023 SJIF Rating: 8.176 ISSN: 2582-3930

ARE SMART DEVICES SECURE AND CAN BE TRUSTED WITH OUR PRIVACY?

Kajol Jadhav[1], Varsha Kotwal[2], Dimpal Pandey[3]

[1]Kajol Jadhav MCA Student & ASM IMCOST College
[2]Varsha Kotwal MCA Student & ASM IMCOST College
[3]Dimpal Pandey MCA Student & ASM IMCOST College

Abstract - *Electronic devices have evolved into "smart" devices that are ubiquitous in our daily lives. Smart devices have become increasingly popular in all kinds of applications, from small household appliances to large industrial machines. Smart devices in our homes, businesses, buildings and cities can communicate with each other and the real world. These technologies offer new opportunities and benefits, but they also bring new threats.Smart device users should expect a significant increase in malware in the near future and significant breakthroughs in malware-related attacks. By manipulating the sensors, attackers can obtain information from a smart device, transfer malware to the device, or initiate a malicious activity to hack the device. In this paper, we address a number of risks and attacks that exploit smart devices for malicious purposes. We present a thorough examination of current threats and attacks against smart devices and highlight ways to protect smart devices from these threats. We also address smart device security and privacy issues related to threats and attacks, as well as future research directions.*

***Key Words*:** attacks, malware, security, sensors, smart devices, threats.

1.INTRODUCTION

The Internet is one of the most significant achievements in human history in the last 100 years. We have seen the need for seamless connectivity of smart devices evolve to provide consumers with a wide range of features and capabilities. Still, we are concerned about the vulnerabilities of the ecosystem.

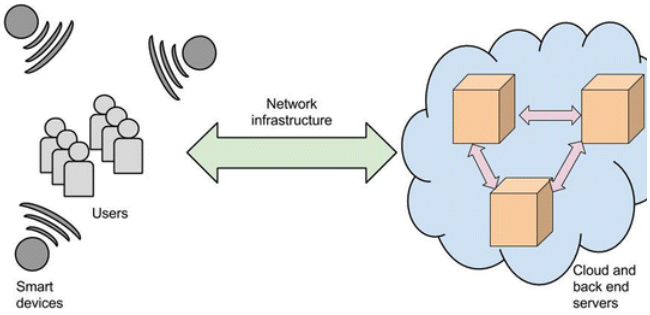
While these technologies offer new opportunities and capabilities, they also offer new threats. We must remember that information security is primarily a social issue, not a scientific one. The difficulties arise not from the products we use, but from the way we use them. This also means that individuals are generating more and more data. This often happens without people being fully aware of the implications of their behaviour. As already mentioned, the expansion and networking of multiple devices in a smart home leads to the creation of a large amount of personal data that, if disclosed, poses a security risk to individuals and data subjects. Once all this information has been collected, it is processed either by the service provider or by various third parties.

2. WHAT IS A SMART DEVICE?

Smart gadgets are interactive electronic devices that respond to simple commands and help users with everyday tasks.

Smartphones, tablets, phablets, smartwatches, smart glasses, and other personal electronics are among the most commonly used smart devices. While many smart devices are small, portable personal electronics, they are characterised by their ability to connect to a network and share and interact remotely. As a result, many televisions and refrigerators are also classified as smart devices.

IoT devices are Internet-connected smart devices that can communicate with other devices over the Internet and allow users with remote access to manage the device according to their needs.



A methodical and repeatable approach to building a scalable approach to smart devices, leading to the following definition: "A smart device is a context-aware electronic device capable of autonomous computation and data transmission over wired or wireless networks."

3. COMMUNICATION PROTOCOL

According to Wikipedia, communication protocol is defined as "a set of rules that allows two or more entities in a communications system to send data using any physical amount variation. The protocol specifies the communication rules, syntax, semantics, synchronization, and error recovery mechanisms."

In the 1980s, X10 was the only protocol that allowed the transmission of information between smart home appliances when it came to automating homes. Data was encoded in the electrical waveform of power delivered by a utility in a home, which was the primary communication path for X10. Because the protocol didn't include handshaking or error correction, it was highly unreliable. Just turning on a blender in the kitchen could be enough to disrupt all X10 connectivity in the home. Smart outlets, dimmers for outlet lamps, and smart switches were the most common X10 products offered to customers. X10 was the inventor of the term "plug and pray" because of these form factors.

Fortunately, there are now a variety of current smart home protocols and devices that support them.

4. SECURITY THREAT

Data collected by smart devices is stored and structured in the cloud to help you understand your habits.

You are at risk if all the data stored on your devices fall into the wrong hands. And given the increasing sophistication of hackers, this is a legitimate concern.

About 80% of IoT devices are vulnerable to various types of attacks. Connecting traditional "standalone" smart devices like lighting, home appliances, and locks raises a host of cybersecurity issues. As some parents realized too late when hackers spoke to their young children via hijacked devices, even connected baby monitors are vulnerable to digital intruders. The extent of the damage depends on what's at stake when it comes to smart home device security breaches. Below are some of the most common security threats and attacks on smart home devices :

1. Identity Theft

If they gain access to your personal information such as credit card numbers, social security numbers, and bank account information, they may be able to take over your identity.

After they obtain the necessary information, they make illegal transactions and purchases in your name. You could put yourself in serious legal danger for something you have no idea about.

2 . Spying and Monitoring

Some smart home devices are capable of recording video and audio. Security cameras can help you keep an eye on your property by recording video and letting you know what's going on, even when you're not there.

Audio devices like Google Assistant and Amazon Alexa, on the other hand, listen to you and record everything you say.

Usually, you don't have to worry about this until a security breach occurs.

Hackers can gain unauthorized access to your smart home cameras and audio devices and use the system to execute their commands. Thus, they can record everything you do and say and potentially use it against you.

3. Location Tracking

Smart home devices are connected to a tracking system that uses the Global Positioning System (GPS) to automatically determine the location of your home. The signals from GPS are supposed to be secret, but because they are stored in the cloud, they are vulnerable to hackers. Unfortunately, anyone who goes into the trouble locating your address could be up to something nasty.

4. Data Manipulation

Installing a surveillance camera in your home allows you to keep an eye on your property even when you are not there. However, the validity of such information is questionable, especially since it can be manipulated by skilled hackers.

The data sent via smart home devices is not encrypted. An untrusted intruder could break into your home and leave without leaving any evidence on your security camera. He simply replaced the original data with an updated version to manipulate the data.

5 Third-Party Apps Flops

Remote access is one of the benefits of a smart home. In most cases, this is made possible by integrating third-party mobile apps.

If the apps aren't adequately secured, hackers can gain access to your devices and use them for criminal or fraudulent purposes. You'll be surprised to learn that someone else is manipulating your home devices remotely.

6. Device hijacking

An attacker takes control of a device by hijacking it. These attacks are difficult to detect, since the attacker does not change the basic functions of the device. Moreover, a single device has the potential to infect all smart devices in the home.

7. Denial of Service (DoS)

A denial-of-service (DoS) attack aims to make a computer or network resource inaccessible to its intended users by temporarily or indefinitely disrupting the services of a host connected to the Internet.

There are 2 types of DoS attack.

a. Distributed Denial of Service (DDoS)

In a distributed denial-of-service (DDoS) attack, a target is flooded with incoming traffic from multiple sources, making it impossible to stop the cyberattack by blocking a single source. In fact, DDoS attacks are on the rise due to the lack of security on IoT devices.

b.Permanent Denial of Service (PDoS)

Permanent denial-of-service (PDoS) attacks, also known as phishing, are attacks that damage a

device so severely that the hardware must be replaced or reinstalled.

5. HOW TO PREVENT SUCH ATTACKS

1. Identity Theft

Protecting your personal information and keeping a close eye on your billing cycle are the first steps to avoiding identity theft. Most smart home devices are controlled by cell phones. To prevent unwanted access, enable security measures on your phone. Use a virtual private network (VPN) and install virus detection software and firewalls on your computer if you use public Wi-Fi.

2. Spying and Monitoring

You need to be careful how you use your smart home devices to prevent attackers from eavesdropping and watching you. To prevent your conversations from being stolen, delete them first. If you're away from home or need absolute privacy, you should turn off your Wi-Fi. Use a secure Wi-Fi router to protect your Internet connection.

3. Location Tracking

If hackers illegally gain access to your GPS, they can track your location. Turning off your GPS is the best way to prevent others from tracking your location. Use a dedicated network for your

smart home devices - hackers can quickly compromise your security if you share a network with them.

4 . Data Manipulation

Using an advanced security system with File Integrity Monitoring is an excellent technique to prevent data tampering (FIM). When data tampering is detected, the system immediately creates backup copies of the movie and quickly sends out alerts. By comparing the movie on your system with the backup, you can ensure its integrity.

5. Third-Party Apps Flops

Be careful what permissions you give to third-party programmes during the installation process. You should enable only the access features that you need. Enable two-factor authentication to make your account even more secure. Verify all links that are displayed. Don't click on a link if you cannot verify its validity.

6 . Device Hijacking

Before buying a smart device, it's important to do your research.

Strengthen your Wi-Fi security because your smart home's Wi-Fi network is at its heart, making it a vulnerable point of attack. You should create a strong, unique password for every device you own.

1. Denial of Service (DoS) attack

Any attempt at a DDoS attack must be stopped with network security. Since a hacker can only make an impact if it has enough time to build up requests, early detection of a DDoS attack is critical to limiting the blast radius. Continuous monitoring (CM), which analyses traffic in real time and detects signs of DDoS activity, is an excellent way to detect traces of DDoS activity. To amplify the effect of a DDoS attack, the hacker would likely send requests to every device on your network. Limit network transmissions between devices to counteract this strategy.

6 . RESEARCH METHODOLOGIES

HYBRID MODEL

A model may contain both descriptive and analytic components. In a descriptive model, the logical relations can be examined, and conclusions can be drawn to reason about the system. However, logical

analysis leads to very different conclusions than a quantitative chemical study of system properties.

First, we conducted a survey of citizens using an online form creation and data collection service to obtain information about people's awareness.

7. PUBLIC SURVEY

We deployed our data collection programme, often referred to as a survey bot, to a variety of individuals and collected information on various aspects of their understanding of cryptocurrencies.

7.1 QUESTIONNAIRE

Do you feel comfortable having smart devices around you?

Do you know the dangers posed by smart devices?

How important is it for you to be able to communicate with your home while you're away?

How likely is it that you would hire a professional to monitor your home? (For example, an alarm monitoring service that is available 24 hours a day, 7 days a week)

How likely is it that you would hire a professional to monitor your home? (For example, an alarm monitoring service that is available 24 hours a day, 7 days a week)

How secure do you think your home network is?

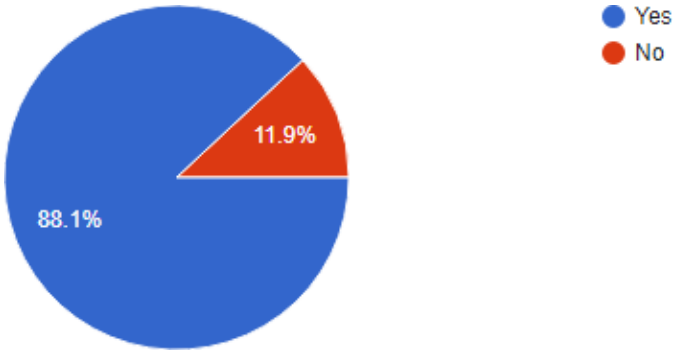
Do you sometimes feel that the smart devices around you are secretly recording or watching you?

Are you worried that smart devices have security vulnerabilities that could allow hackers to gain access to your

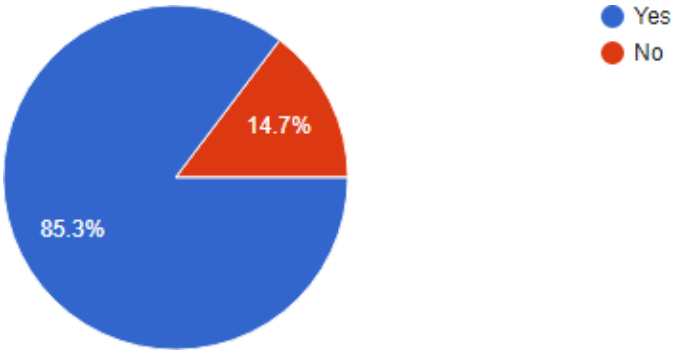
Would it stop you from buying a smart device if I told you that most of them do not meet basic safety standards?

7.2 RESULTS

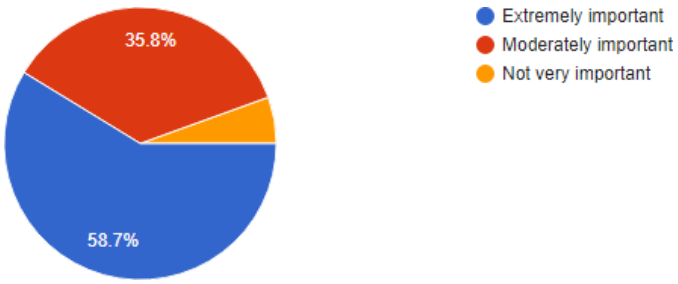
When people were asked if they felt comfortable having smart devices around, about 88% agreed, the rest not so much.



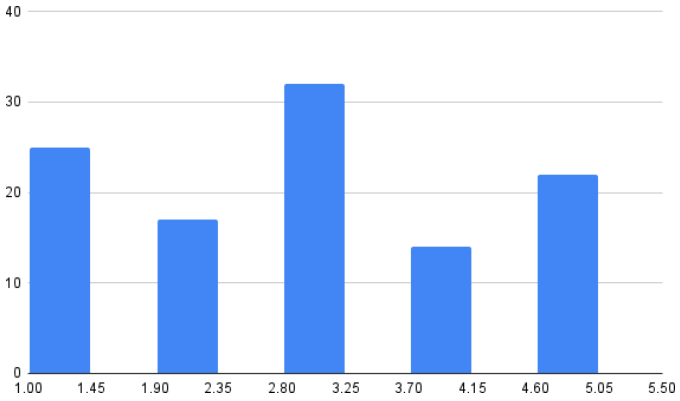
When asked if they were aware of any threats related to smart devices, about 85% were aware and 15% were not.



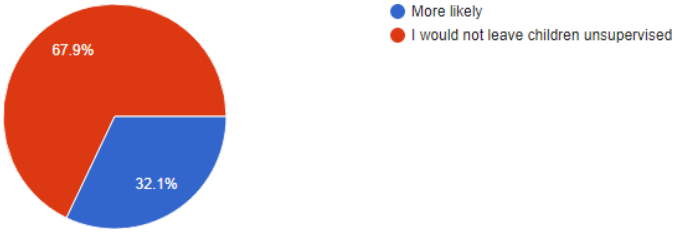
When asked how important it was for them to be connected to their home while away, 59% of respondents said it was very important for them to be connected for security reasons, while the rest said it didn't matter to them to stay connected.



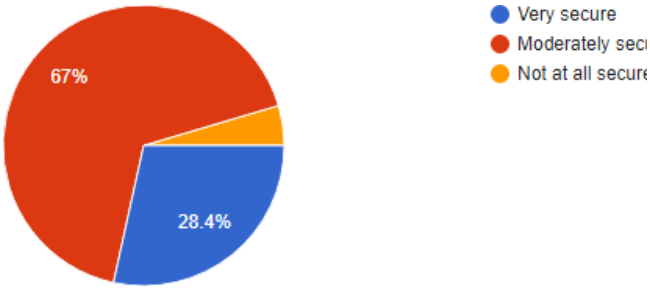
When asked how likely they were to consider professional surveillance of their home (24*7), the following response diagram emerges:



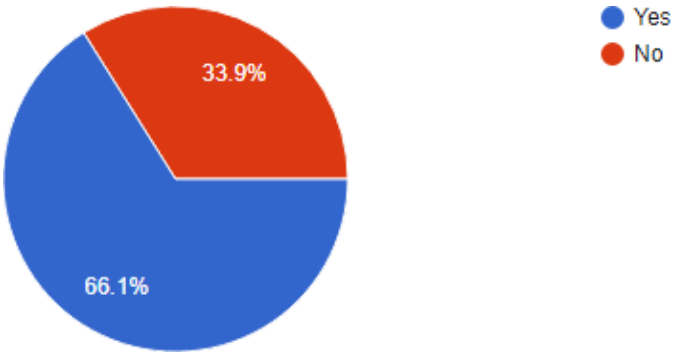
When asked how likely they would be to leave their children unsupervised at home when they were younger if they were able to monitor and secure their home remotely, about 68% of respondents said they would not leave their children unsupervised, while the rest would be fine with their home being secured by high-tech security devices.



A secured home network is very important to protect all data on smart devices. When asked how secure they thought their home network was, only 28% of respondents were confident that their home network was secure, while about 72% of respondents were not confident that their home network was secure.

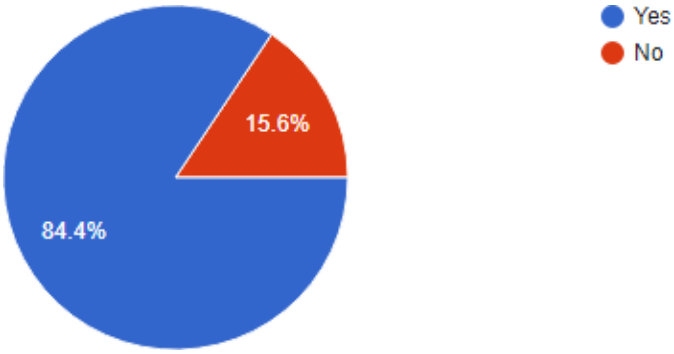


When asked if they ever felt that the smart devices surrounding them were secretly recording or watching them, 66% of respondents answered yes.

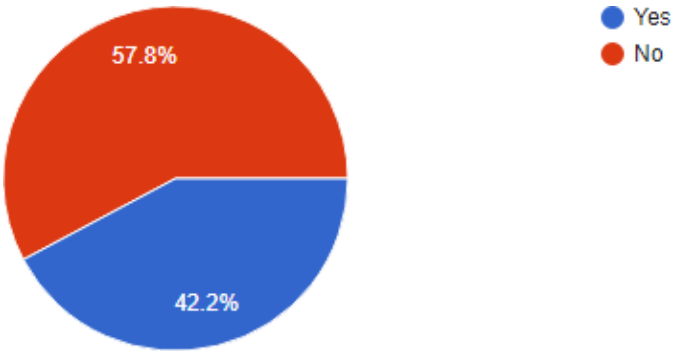


When asked if they were concerned that smart devices could have security vulnerabilities that could compromise their network and

steal their personal information, about 84% were very concerned, while the remaining 16% were not.



When asked if an indication that most smart devices do not meet basic safety standards would prevent them from buying one in the future, 58% of respondents said they would still buy a smart device, while the remaining 42% said they would not.



8. HYPOTHESIS TESTING

Hypothesis testing is a sort of statistical reasoning that includes analyzing data from a sample to derive inferences about a population parameter or probability distribution. First, a hypothesis is created regarding the parameter or distribution.

This is known as the null hypothesis, abbreviated as H0.

After that, an alternative hypothesis (denoted Ha) is defined, which is the polar opposite of the null hypothesis. Using sample data, the hypothesis-testing technique

For this paper,

Null hypothesis (H0): Smart devices are very secure and can be trusted with our privacy.

Alternative hypothesis (Ha): Smart devices are not secure and cannot be trusted with our privacy.

TEST (STATISTICS)

There are 3 tests available to determine if the null hypothesis is to be rejected or not. They are:

1. Chi-squared test
2. T-student test (T-test)
3. Fisher's Z test.

For this paper, we will be using a 2 tailed T-student test.

A t-test is an inferential statistic that determines if there is a significant difference in the means of two groups that are related in some manner.

- **Level of significance**

Level of significance = 0.05

The chance of rejecting the null hypothesis when it is true is the significnace level

I.e 5% Level of confidence = 95%

determines whether or not H0 may be rejected. The statistical conclusion is that the alternative hypothesis Ha is true if H0 is rejected.

Level of confidence

The confidence level indicates the probability that the location of a statistical parameter (such as the arithmetic mean) measured in a sample survey is also true for the entire population.

Sr. No.	Data
1	88.1
2	85.3
3	58.7
4	37.6
5	67.9
6	71.6
7	66.1
8	84.4
9	57.8
Mean (x)	68.61111111
Standard Deviation (s)	16.20250324

A t-score (t-value) is the number of standard deviations away from the t-mean. distribution's.

The formula to find t-score is: $t = (x-\mu) / (s/\sqrt{n})$

where x is the sample mean,

μ is the hypothesized mean,

s is the sample standard deviation, and n is the sample size.

The p-value, also known as the probability value, indicates how probable your data is to have happened under the null hypothesis. Once we know the value of t, we can find the corresponding p-value. If the p-value is less than some alpha level (common choices are .01, .05, and .10) then we can reject the null hypothesis and conclude that smart devices are not secure and cannot be trusted with our privacy.

Calculating t-value:

Step 1: Determine what the null and alternative hypotheses are.

Null hypothesis (H0): Smart devices are very secure and can be trusted with our privacy.

Alternative hypothesis (Ha): Smart devices are not secure and cannot be trusted with our privacy.

Step 2: Find the test statistic.

In this case, the hypothesized mean value is considered 0.

$t = (x-\mu) / (s/\sqrt{n}) = (68.61-0) / (16.202/\sqrt{9})$

$= 12.704$

t-value = 12.704

Calculating p-value:

Step 3: Calculate the test statistic's p-value.

The t-Distribution table with n-1 degrees of freedom is used to calculate the p-value. In this paper, the sample size is n = 9, so n- 1 = 8.

By plugging the observed value in the calculator, it returns a p-value. In this case, the p-value returned is less than 0.00001.

Since this p-value is less than our chosen alpha level of 0.05, we can reject the null hypothesis. Thus, we have sufficient evidence to say that smart devices are not secure and cannot be trusted with our privacy.

9. FINDINGS

1. People who are aware of the threats in smart devices think twice before buying them, while some people buy smart devices just because they are trendy or because there is a sudden hype about the devices, regardless of the security threats
2. People believe just because they spend a large amount of money on the smart devices they buy that they are safe, and do not take any additional measures to ensure the safety of their devices.
3. It is very important that you keep your devices updated to receive the latest security patches that the company issues, which greatly improve the security of your network. They may not be applied automatically. Therefore, it is important to manually check for updates every few months.
4. Disable the features you don't use. It may sound paranoid, but if the hacker gains access to your smart devices like Siri, Alexa, etc., the active microphone can be used to eavesdrop on your conversations. Disabling features is all about blocking as many of these different access points as possible.
5. A separate Wi-Fi network can be set up for smart devices. Many modern routers offer the ability to set up a guest (or secondary) network. You can protect your primary network from IoT

1. risks by setting up a secondary network specifically for your IoT devices.
2. Create a strong and unique password. The longer it is, the more secure it is. Change it frequently. Set up two-factor authentication.

10. CONCLUSION

New devices are constantly being developed to bring the power of the Internet to

home appliances and systems. By 2021, there could be 25 billion smart IoT devices in use, such as smart light bulbs, air quality monitors, doorbells, washing machines and refrigerators. Your IoT home will have the ability to provide great control, but it's up to you to make sure it also provides smart home security. You can buy the most expensive IoT devices from the most reputable companies, but the security of your smart home is ultimately in your hands. Therefore, before you choose a device, do your homework. Check if it's still receiving manufacturer updates or if any vulnerabilities have been identified by users. Yes, it costs money and time, but better safe than sorry.

11. BIBLOGRAPHY

1. https://www.techopedia.com/definition/31 463/smart-device
2. https://internetofthingsagenda.techtarget.co m/definition/Internet-of-Things-IoT
3. https://builtin.com/iot-internet-things/smart-device
4. https://towardsdatascience.com/what-is-a-smart-device-the-key-concept-of-the- internet-of-things-52da69f6f91b
5. http://smarthomes-technology.blogspot.com/p/conclusion-and-additional-work.html
6. https://www.kaspersky.co.in/resource-center/threats/how-safe-is-your-smart- home
7. https://us.norton.com/internetsecurity-iot-smart-home-security-core.html