JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Can microchips be used in the human body?

Abhishek Gawade

Guide: Asst. Prof. Gauri Ansurkar

Keraleeya Samajam's Model College, Dombivli East, Mumbai, Maharashtra, India

abhishekgawade.model@gmail.com

***Abstract*— The purpose of this study is to analyze people's points of view regarding microchips implanted in humans. The research is focused on the effects of the use of microchips implanted, as well as how to overcome the consequences. The quantitative survey was a questionnaire in which 100 people were asked. The result showed that the people were not knowledgeable about microchip implants in humans and had a lot of different points of view about microchip technology. Some saw risk as a big threat and others saw them as less of a threat. In the end, the result shows that most of the participants were against microchip implantation in humans and would not get chipped. The conclusion showed that the people between the ages of 18-30, in general, had the same opinions regarding risks that health issues.**

***Keywords*-- Microchip, RFID chip, Active chip, Passive chip, semipassive chip, RFID reader INTRODUCTION**

People want to live an easy life where every day is smooth and simple. As technology continuously gets closer to merging with human bodies, from the smartwatches on our wrists to earbuds. Now, it's getting under our skin with a tiny microchip. It is getting more and more common for people to insert microchips into their bodies just to make their daily life easier for them. Now, more than 5000 people have inserted into their bodies. A microchip is also called an integrated circuit. A microchip has four components: Diodes, Registers, capacitors, and Transistors. The four components are integrated and are all placed on a little disk called a microchip.

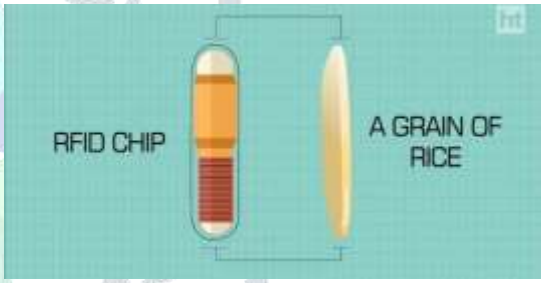
The microchip for humans is called Radio-frequency Identification (RFID). You place one RFID- a chip under the skin that can contain a lot of information and be used for many different things. The microchips have one unique identification code that connects to the system. The microchip can transmit a static identifier or serial number for a short-range distance. RFID is a passive chip which means it gets power when it connects to the reader, otherwise chip has no electronic power and therefore cannot send signals. The passive microchip makes it difficult to track the microchip implanted in the human body. This technology can be used for different kinds of payments, like on the railways, as keys and can probably develop in the future to prevent aging so that people can live longer.

The microchip has a lot of advantages but also some disadvantages. The microchip is passive which means that it needs to be active to use for more purposes. The microchip is more sensitive and there are some risks. Especially when new technology is invented and many other devices get established. The world has constantly been tested in history for risks and more risks will appear in the future. The big question is if people are ready for new evolution and the risks that come with it?

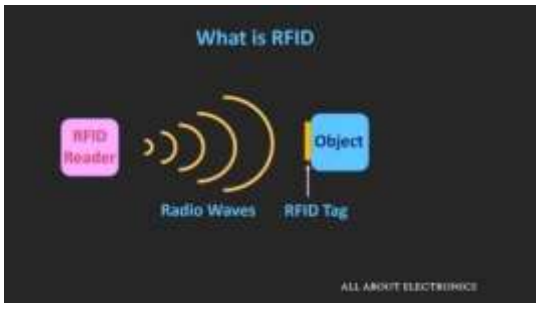
By the following questionaries of this study, the purpose is to see the opinion of people about the risk of biohacking on humans and do research on it.

What is a Microchip (RFID)?

The microchip implanted can be in form of either an IC (Integrated Circuit) or an RFID (Radio Frequency Identification) that is encapsulated in a silicone case or glass coatings with a size comparable to the rice grain. In the beginning, the chip was implanted in pets but today it is possible to implant it in humans.

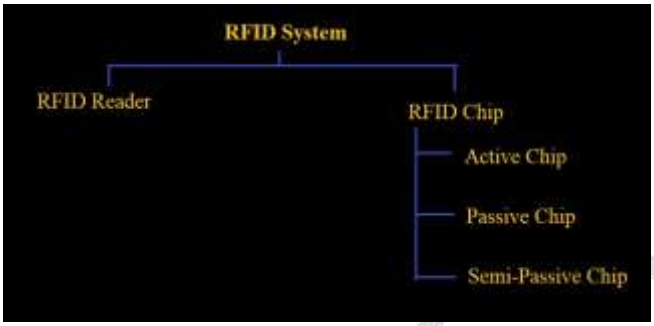


RFID microchip is the technology which is working on radio frequency or radio waves. This uses to automatically track the object. The object could be a microchip that is implanted in the human body. The RFID chip is used to track animals as well as birds.



The RFID chip contains a unique identification number that is placed on the object which we want to track. The RFID reader is continuously transmitting radio wave frequency. Whenever the object comes within a range of the RFID reader range the RFID chip transmits the feedback signal to the reader. It is similar to barcode technology it is based on a line of sides. The RFID chip technology is not based on line-of-sight technology. So as far as the object is within range of the RFID reader object with a range

reader. By using this technology, we can track multiple objects at a time.

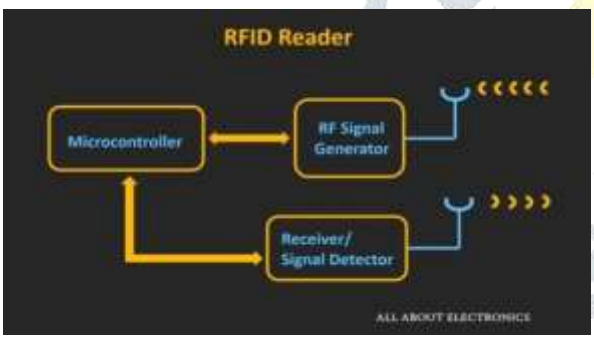


of the RFID reader object can be identified by the The active chip has its power supply. For transmitting feedback signals it uses its power supply. It has a greater range than passive and semipassive.

The passive chip does not have a power supply. So, it relies on radio waves that are coming from the RFID readers as a source of energy.it has less range than active and passive chips.

The semi-passive chip uses its power supply, but the transmitting signal relies on an RFID reader signal that transmits radio waves.

RFID Reader



RFID reader consists of three components as follows:

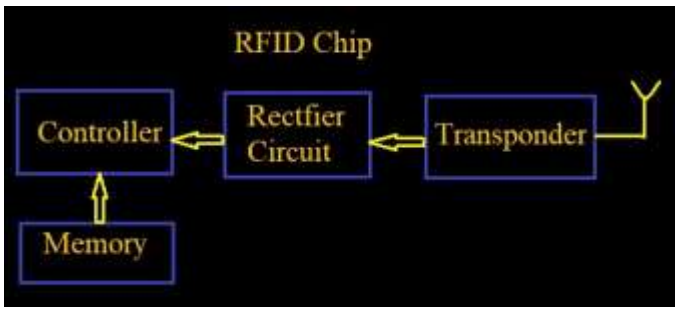
RF signal generator: This is a signal generator radio wave that is transmitted using an antenna.

Receiver signal decoder: to receive signal coming from RFID chip.

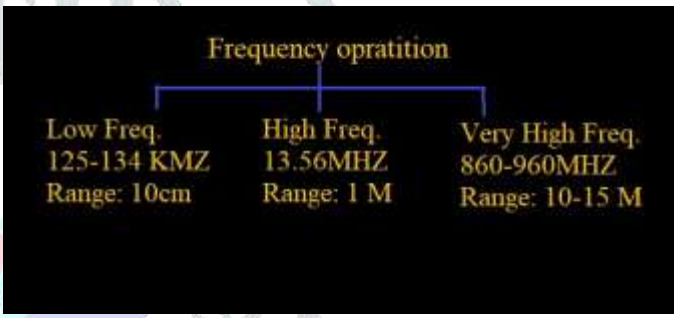
Microcontroller: To process the information sent by the RFID chip RFID reader also have a microcontroller. Several times the RFID reader is connected to the computer.

RFID Chip

Most RFID chip used today is a passive chips they are quite cheaper than other as well as they do not require any power supply. This chip is quite compact. The transponder receives a radio wave that is coming from the RFID reader and sends a feedback signal back to the RFID reader. As the passive chip does not have a power supply that relies on radio waves that are coming from the RFID reader. They will get energy from radio waves that come



from the reader using this rectifier circuit energy from radio wave across the capacitor. This energy is used as a supply for the controller as well as the memory of the RFID chip.



The majority of the company uses a Very High-Frequency level in RFID chip. As low-frequency signal travel from a short distance the range of the RFID chip is up to 10 cm. high-frequency signal travel greater than low frequency the range of the RFID chip is up to 1M.
very high-frequency ravel longer than both frequency 10-15 M.

How microchip (RFID) works?

It depends on the frequency of operation LF and HF working principles are based on inductive coupling while in the case of UHF operation working principles are based on electromagnetic coupling.

Inductive coupling (near field coupling)

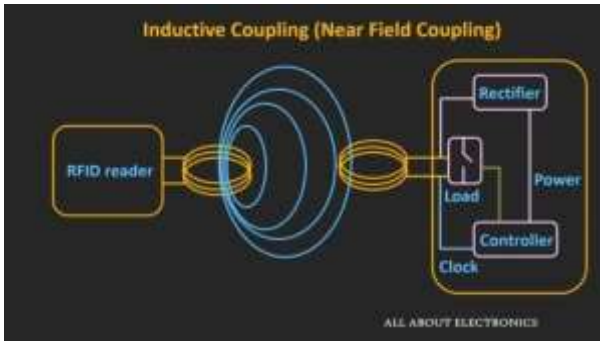
RFID readers continuously send radio waves with a particular frequency. Radio waves sent by RFID readers used for three purposes:

It induces enough power into the RFID chip.

It provides a synchronization clock for the passive chip.

It acts as a carrier for the data which is coming back to the RFID chip.

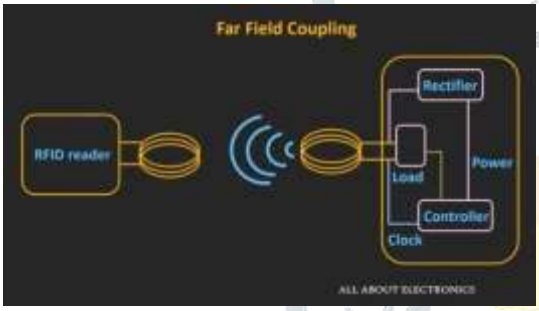
In this case, the RFID reader and RFID chip are very close to each other. The field generated by the RFID reader is used to get a couple with an antenna of the RFID chip because of this mutual coupling the voltage gets induced across the RFID chip some portion of the voltage gets rectified and use as a power supply for the controller as well as memory elements. The RFID reader is sending radio waves of a particular frequency the voltage gets induced across the coil is also of a particular frequency. This induced voltage is used to drive a synchronization clock of the controller.



Suppose we connect load across this coil current will start flowing through this load. If we change the impedance of the load the current that is flowing through this load also changes how to support switch is on or off this load then the current also switches on and off. This switches off current or rate of change of current also generates a voltage in the RFID reader. So, this switch is on or off this load known as load modulation. Now suppose switch on and offload according to data stored inside the database of RFID chip. Then that data can be read by the RFID reader in form of voltage.

Electromagnetic coupling (far-field coupling)

In this case very high-frequency RFID reader and RFID chip up to a few meters so coupling between the reader and chip is far-field coupling. RFID reader continuously sends electromagnetic wave toward the chip in response to this chip sends a weak signal to send back to the RFID reader this signal is called backscatter signal intensity of this signal depends on the load



matching across the coil if the load is matching exactly the inbackscatter signal will be more. If the load is not matched exactly the intensity of the backscatter signal is less if we change the condition of the load according to the data that is stored in a database across the RFID chip the data can send back to the RFID reader initial signal sent by the reader is strong.

Background

From the beginning, humans are taken the technology evolution to next level. Integrated circuits have been placed in almost all electronic devices and after that device is implanted into animals.

Technology is moving futuristic way, nowadays microchips are implanted in humans. The microchip is around 1cm in size, meaning that you can easily have it under your skin without noticing it. The microchip is used for simplifying your life and it is widely used in different areas. Currently, there is limited accessibility from some devices like id-cards, keycards, door-entry, unlock lockers, payments, etc. microchips are already inserted into humans but are still a new technology to our society. The next step is to upgrade the chip and make it more effective and powerful.

Problem definition

With the new innovation, that microchips are embedded into people there are various issues that happen. The hazardous region is privacy, hacking, monitoring, hacking, and harmfulness to the human body. Microchip technology today uses passive chips, but in the future active chips can be used. The active chip can have more data and a bigger range of usage. But active chips are easier to obtain sensitive data.

While the chip is getting developed, the hacker can develop their hacking abilities to have the sensitive information stored in the microchip of their victim. By developing their skills while, following the development of the chip, there might be a possibility of the hackers learning how to get their hands on the sensitive data in an easier way. This can be an issue as a result of things to come probability of when users are using their microchip there may be a huge risk in having all information gathered in a similar spot. This can lead to the wrong people having the ability to reach all of your data instead of just parts of it.

tracking is one more angle that also can be obtained from various social factors which makes it a much more delicate subject considering it is under the skin and has the chance of surveillance consistently. Irritation under the skin can be a problem because the chip may move around while irritating the skin and to get away and fix the problem, professional surgery might be necessary. People can be hurt both physically and mentally which makes people more doubtful to get a microchip.

Threats of use of microchips:

Data collected by microchips are stored in external databases that help it convenient to not carry your id-cards and remember your password every time.

But you are at risk if all the data saved on the database falls into wrong hands, due to the increased sophistication of hacking, this is a logistic cause of danger. The various damage depends on what is at stake when it comes to security breaches in microchip devices. The following are some of the most common security risks against microchips

Privacy

When it comes to privacy for each person, a lot of people see microchip implementation as a really bad thing since their privacy can be threatened with the risks of constantly being tracked. These small chips make it easier to get information about one person and can easily get personal information through just one scan. Today there are privacy concerns issues and debates mostly when it comes to RFID microchip implementations. Applied advanced arrangements, that were developed by Verichip, have been involved all around the world in getting VIP status at bars to patients at emergency clinics for getting data rapidly and have once said that their system has stored all information regarding Verichip.

- That the tags can hide information and documents against the individuals without their knowledge.
- That it is possible to mass identify objects which means it is possible to track items to persons afterward when a product has been transferred or has been sold. This makes the privacy decreases.
- The possibility to collect a lot of data and especially if it can connect to personal data makes privacy decrease.
- With personal identity numbers connected to the personal microchip can private persons be profiled and tracked without their knowledge and consent.
- Privacy concerns have been created since it is possible to read a microchip from distance in many different environments which decreases privacy and integrity.

Tracking and Monitoring

Tracking is when you try to figure out who has left traces behind or to see what a person has done by following. The digitalizing society is developed in a way that reduces the cost of monitoring and tracking. Society has become more interconnected through most of all electronic devices and is highly developed and connected to computer software.

Data from electronic devices collect and get analyzed. The individual does not know who obtains the RFID chips data. Hackers can get unauthorized access to the data stored in microchips. This allows them to keep track of

everything you do and say and the potential to use it against you. A tracking system that uses the Global positioning system (GPS) to automatically detect your home location where ever you go, saves data into the database, making it vulnerable to us.

Hacking

The use of the internet increases similarly criminals commit different crimes over the internet. Cybersecurity is protection for organizations and individuals from threats, still, that can damage the user's information. Risks that may occur are viruses, phishing, spyware, trojans, and many more.

In the same way, computers can be hacked by different kinds of threats like other people and different kinds of viruses the RFID microchip can be hacked. RFID has to be read from a specially designed reader that is based on regulations and standards and for a hacker to hack into an RFID chip is all that they need, just more power to have the opportunity to read and identify information. Hackers that can reach those chips can also deploy harmful content that is almost impossible to find. RFID chips are on and off because of changing information which can concern people getting it since they feel it is not worth it.

Harmful to the body

According to WHO health is defined as social, mental, and physical wellness. RFID implantation is a pretty new technology; therefore, the knowledge is limited to what are side effects and the risks it brings to the body. Chip implantation is approved but there is nothing that the chip implant is completely safe.

There are some health risks of implantation of a microchip as follows:

- The potential problem with this chip is that they don't always stay in their place. They sometimes migrate to a different location inside the body, making it hard to find them. Which would be particularly problematic in medical emergencies.
- Electrically hazards, with medical equipment such as MRI machine. In an emergency during an MRI scan, the patient cannot wear metal ornament as well as cannot take metal, including microchips.
- Research studies in 2007 have indicated that microchips caused cancer in between one and ten percent of lab animals implanted with the chips. Even though these causes are too rare to be distinguished from the cancer risk associated with the implanted device.
- There is risk associated with certain pharmaceutical issues of electrosurgical and electromagnetic interference with devices and defibrillators.
- various potential RFID chip-related health issues that are currently not adequately studied.
- Infection and other medical reactions are a risk that could emerge when an RFID implant has been performed.

How to overcome threats:

Privacy

Countermeasures against eavesdropping include establishing a secure channel and/or encrypting the communication between chip and reader. Another approach is to only write the tag with enough information to identify the object. The identity is used to look up relevant information about the object in a back-end database, thus requiring the attacker to have access to both the tag and the database to succeed in the attack.

Monitoring and Tracking

- Microchips are specially used for monitoring, and tracking purposes. Microchips track people continuously; this is why all those people believe that microchips are not necessary for everyday life. Due to privacy and ethical issues, microchips should only use for those people who need them. The common people do not need a microchip, as the risk of being hacked is too great.
- Microchips are also vulnerable to hacking and lead to privacy issues even in the workplace, this is too many problems that are not worth the benefit of the use of the microchip.

Hacking

- The FIPS standard refers to chip coating as an anti-reverse engineering method to prevent attacks. Various' temporary protecting technique has been developed to defend against reverse engineering attacks. For example, by adding a tamper release to the microchip, operations can be a modification in the microchip that has been tampered with.
- The most common methods used to defect power analysis attacks are to filter or add random elements. Filtering the power signal or randomly delaying the count can increase the attacker's difficulty identifying patterns of energy consumption. Another method implemented in some smart card designs is to add a component that consumes only a random amount of energy. Unfortunately, this approach can create problems for microchip systems where reducing power consumption is a priority.
- A common way to defeat a spoofing attack is to implement an RFID authentication protocol and data encryption, which increases the cost and technology complexity needed for a successful attack.

Harmful for health

Migration of the microchip is very rare. A major BSAVA microchip study examining found that true migration occurs in less than 1 out of 10000 cases, to find out a migrated chip in the side body we need to use good quality scanners. also found that the failure of the microchips is even less common.

Methodology

This research contains a qualitative and quantitively analysis where the purpose is to see people's opinions and understanding about getting a microchip implanted into the human body. We can examine and a conclusion can be drawn to reason about the system. We first conducted a poll of the people utilizing an online form creator and data collection services to acquire information regarding people awareness.

Analysis and discussion Data collection

The data is collected through the survey. The result will be analyzed and also how the result has been reached. in this case, 100 individuals what they believe and what they think about questions regarding the topic, microchip implants in humans. The survey is a must for getting good data that later on can be analyzed and give a result of the survey. By using the survey research method, the study would give good data by asking the right individuals that were within ages 18-30 years old the right kind of questions to go forward in the survey.

Questionnaire

- Are you heard about microchips implanted in humans before?
- Are you comfortable with having a microchip implanted in the human body?
- Are you aware of the application of microchips implanted in the human body?
- Are you aware of threats concerning microchip implantation?
- Which of this harm the use of microchips in the human body?

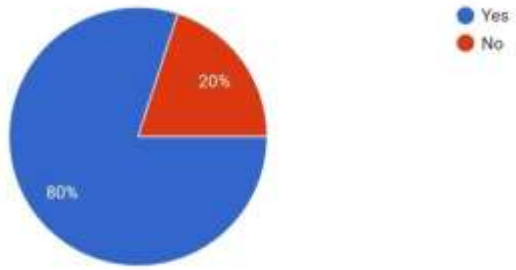
- Privacy
- Monitoring and tracking
- Hacking

Harmful to health

- Do you think that it is physically or medically good practice to use a microchip?
- Do you feel that microchip devices implanted in your body are monitoring and tracking you secretly?
- Do you think that microchip implantation has some loopholes that will allow hackers access to your data and steal your important information?
- Is that much essential to use the microchip in the human body?
- Would it prohibit you from implantation of a microchip if I told you, a microchip is harmful to our health?

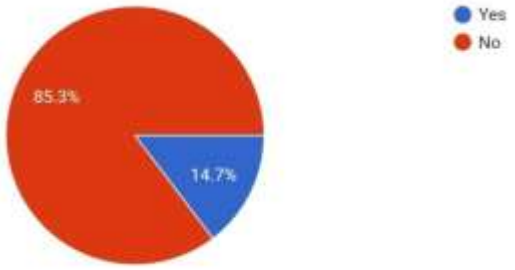
Results

1.



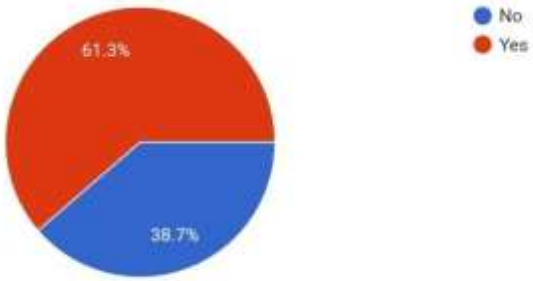
When people were asked if they were any knowledge regarding microchip implantation,80% about we are knowledgeable, and the rest 20% of people does not have any knowledge of microchips.

2.



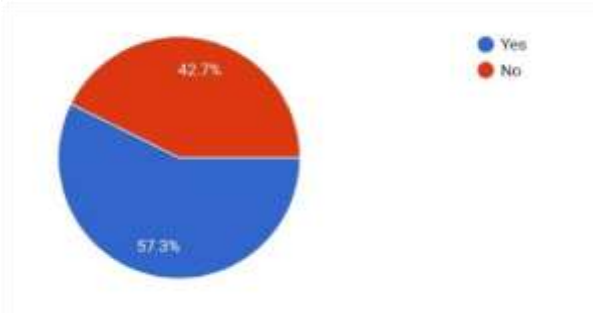
When they were asked if they were comfortable having implanted in their body, 14.7% of people are comfortable and the rest 85.3% of the people were not so comfortable with the implementation of microchips.

3.



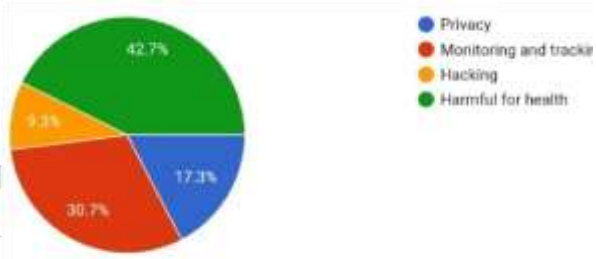
When they were if they knew any application of microchips, 61.3% about knew the application and 38% did not.

4.



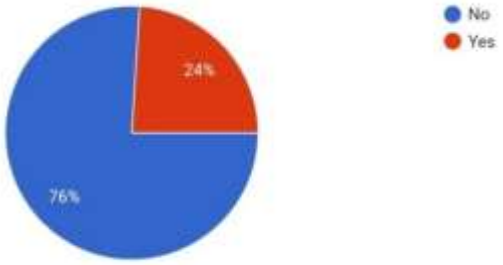
When they were asked about, they are knowing the threats and effects concerning microchips, 42.7% were aware of threats and effects, and were 42.3% not.

5.



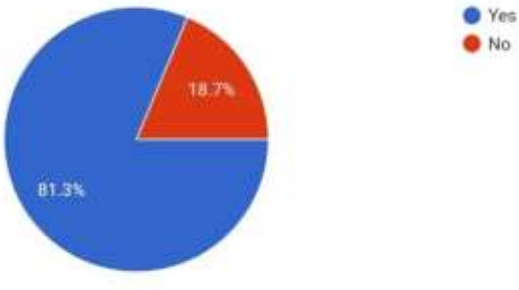
When asked which of these threats are adverse effects on humans they were away, 42.7% of people said that it was harmful to health, 17.3% people said that it has privacy issues, 30.7% people said that it has monitoring and tracking issues, 9.3% people said that it has hacking issues.

6.



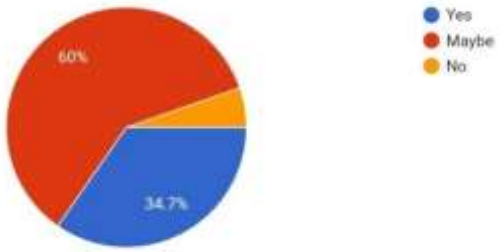
When asked how is it physically or medically a good practice to use a microchip,24% agreed with implementation, and 76% are not.

7.



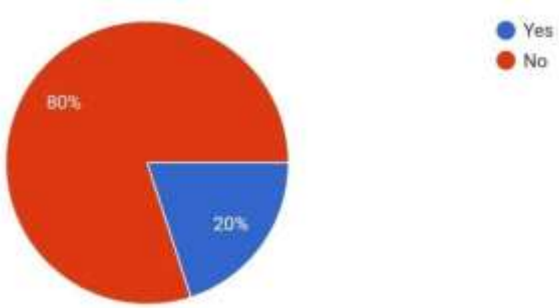
When asked if they were using microchip professional spy can monitor and track (24*7), 81.3% about were agreed with that and 18.7% were not.

8.



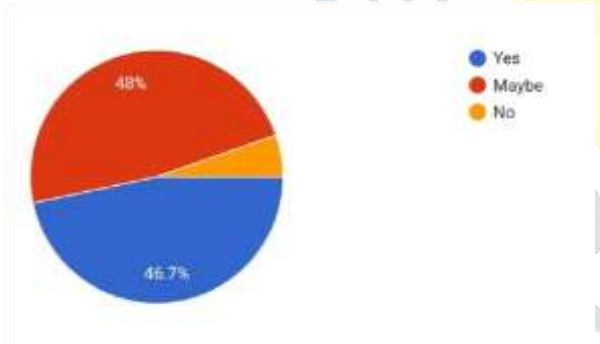
When they were asked if microchips have some loopholes and through that, they were stealing their important information, 34.7% of people said that it is possible to have some loophole and hackers can access our data, and 60% were considering the possibility of data can be hacked. Were 5.3% not.

9.



When they were asked is essential to implement in their body,80% of people are not ready for microchip implementation, and were 20% ready for microchip implementation.

10.



When they were microchips are harmful to health, 46.7% of people think it is harmful to health and 48% of people think they may be harmful to health, 5.3% were not.

Hypothesis testing

Hypothesis testing is a way of statistical reasoning that includes analyzing the data from the samples to drive statistical inferences to conclude population parameters or probability distribution. First, the hypothesis or assumption is a claim regarding the population parameter or probability distribution, which is known as the null hypothesis. Its id was donated by H_0. After that alternate hypothesis is defined. It is donated by H_a. the alternate hypothesis is defined, as the opposite of the null hypothesis. By using sample data, the hypothesis testing technique which determines whether or not H_0 may be rejected. If H_0 is rejected, the statistical conclusion is that the alternate hypothesis H_a is true.

For this paper,

Null hypothesis (H_0): μ = Microchips can't be used in the human body. It is harmful to human health as well as it does not protect data from hacking monitoring and tracking.

The alternate hypothesis ($H_{a)}$: $\mu \neq$ Microchips can be used in the human body. It is not harmful to human health as well as it protects our data from hacking, monitoring, and tracking.

TEST (Statistics)

There are three types of tests available to determine the given assumption the null hypothesis is rejected or accepted.

The type of test is as follows:

- Chi-squared test T-student test
- Fisher's Z-test.

For this paper, we are using 2two tailed T-student tests.

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

The chance of rejecting the null hypothesis when it is true is the significance level (also known as alpha or α). A significance level is

0.05 for the example, which means there is a 5% of probability of discovering a difference when there is not one. Lower significance levels indicate that more evidence is required to reject the null hypothesis.

Level of confidence

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

index	Data(m)	(m – X)	$(m – X)^2$
1	80	-32.67	1067.33
2	14.7	32.63	1064.72
3	61.3	-13.97	195.16
4	57.3	-9.97	99.40
5	42.7	4.63	21.43
6	76	-23.67	560.27
7	81.3	-33.97	1153.96
8	34.7	12.63	159.52
9	20	27.33	746.93
10	5.3	42.03	1766.52
∑X	**473.3**		$\sum (m- X)^2$
			7135.24

$\sum X = m/n = 473.3/10 = 47.33$

$S.D\ (S) = \sqrt{\sum (m - X)^2/n – 1} = \sqrt{7135.24/9} = 729.80$

Level of significance = 0.05 i.e.,5%

Level of confidence =95%

A t-score (t-value) is the number of standard deviations away from the t-mean.

The formula to find a t-score is:

$T = (X-\mu) /(S/\sqrt{n})$

Where X: is the sample mean,

μ: is the hypothesized mean, S:

sample standard deviation, n:

sample total population.

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 of t, we can find the corresponding p-value. If the p-value is less than some alpha level (common choices are 0.01, 0.05, 0.10) then we can reject the null hypothesis and conclude that microchip is not implanted in human that is harmful to health as well as they can be hacked, tracked, and monitored by accessing the data stored on the microchip.

Calculation of T-value:

Step 1: Determine the null hypothesis and alternate hypothesis are.

Null hypothesis (H_0): Microchips can't be used in the human body. It is harmful to human health as well as it does not protect data from hacking monitoring and tracking.

The alternate hypothesis (H_a): Microchips can be used in the human body. It is not harmful to human health as well as it protects our data from hacking, monitoring, and tracking.

Step 2: find the test statistic.

In this case, the hypothesis mean value is

$|t| = (X-\mu) / (S/\sqrt{n})$

$= (47.33 - 75)/ (729.80/\sqrt{10})$

$|t| = 0.11$

t-value = 0.11 calculating p-value:

step 3: calculate the test statistic's p-value.

The t-Distribution table with n-1 degree of freedom is used to calculate the p-value. In this paper, the sample size is n=10, so n-1 = 9.

Level of significance(α) =0.05

Tabulated t at 10 degrees of freedom and $\alpha = 0.05$

Level of significance for two-tailed test t=2.228

Since the t-value is less than our chosen alpha level of 0.05, we can accept the null hypothesis. Thus, we have sufficient to say that Microchips can't be used in the human body. It is harmful to human health as well as it does not protect data from hacking monitoring and tracking.

Findings

- People who are aware of the threat of microchip usage think before being implanted in their bodies. While some people are microchips implanted in their body only because it's in trend or there are suddenly used without considering the safety threats and health effects.
- Some people believe that just because they are spending a large amount of money on the chip implantation, it will be secured and do not take any extra measures over health and security.
- In case of a medical emergency during an MRI scan, we cannot carry metal elements. so, in this case, we need to remove that chip time taken for the removal of the chip effects on a person's life
- Two-step verification is a good idea to prevent hacking if any unauthorized device reader scans the microchip, it immediately asks us for permission to access that reader.
- It is important to keep up-to-date security patches in microchips that greatly enhance your network security.

Conclusion

A microchip is continuously being developed to simplify human life. Microchips implanted in the body are identification, club membership, access control, medical history, control devices, criminal record, monitoring, and tracking might be used. Your microchip will have the ability to provide great control, but it will be up to you to ensure that it provides security. You can implant microchips from well know firms, but the security of microchipping in is your hand. As a result, before you implant any microchip inside your body do your homework. Check if it is any vulnerabilities identified by the user. Its costs money and time, but it's better to be safe.

References

1. https://www.researchgate.net/publication/221787702_RFID_Technol ogy_Security_Vulnerabilities_and_Countermeasure

2. https://lhsepic.com/1232/opinion/microchips-invade-employeesprivacy/

3. https://www.bbvaopenmind.com/en/technology/innovation/technolog y-under-your-skin/

4. https://www.divaportal.org/smash/get/diva2:1572358

5. https://www.youtube.com/watch?v=Ukfpq71BoMo&t=346s

6. https://www.youtube.com/watch?v=Zy7a6W8OG5s

7. https://www.youtube.com/watch?v=Gs0bVs8QuWE&t=16s