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

# Innovation Application of Microchip Technology in the 21st Century

Akshay Ghule , Hutakshini Rathod

*ASM Institute of Management and Computer Studies*

***Abstract*** **– The purpose of this study to explores the use of microchips in medical applications, specifically for the monitoring and treatment of chronic conditions such as diabetes and heart disease. The project involves the design and development of a microchip-based system that can be implanted in the body to monitor vital signs and deliver medication as needed. The system is designed to be small, biocompatible, and energy-efficient, and is intended to improve patient outcomes and reduce healthcare costs. The project also involves testing the system in animal models to evaluate its safety and efficacy, and to identify any potential issues or limitations. Overall, this project has the potential to revolutionize the way chronic conditions are managed and treated, and to improve the quality of life for millions of people around the world.**

***Keywords***-- **Microchip, RFID chip, Comm, RFID reader,**

## INTRODUCTION

People wants smooth and easy life. Today's technology has increases fastly. As technology continues to get closer to merge with our bodies, from the smartphone in our hand to smart watch on our wrist to ear buds. Now it is getting under the skin literally with a tiny microchip. The microchips which is wireless communication channel. The world first microchip has developed by body comm, the new low power wireless technology that use the human body for secure bi-directional communication. Its sounds difficult but designing with body comm is easy because you don't need antennas or crystals or a wireless transceiver. You just need in any one microchips 900 plus microcontrollers. This microchip has low power and more secure than any other wireless technologies. The microchip size is less than 1mm. It is identifying integrated device or we can say that radio frequency identification transponder. With the help of silicate glass coting microchip is implemented in human bodies.

## What is Microchips?

A microchip, also known as an integrated circuit (IC), is a small electronic device made of semiconductor material, typically silicon. It consists of a network of electronic components, such as transistors, diodes, resistors, and capacitors, fabricated on a tiny piece of silicon known as a wafer. The basic building block of a microchip is the transistor, which acts as a switch that can control the flow of electrical current. Transistors are made up of layers of different semiconductor materials, typically doped with impurities to create the desired electrical properties. The most common type of transistor used in microchips is the metal-oxide-semiconductor field-effect transistor (MOSFET).

Microchips are manufactured through a process called photolithography. This process involves applying a series of thin layers of materials onto the silicon wafer and selectively removing parts of these layers to create the desired patterns. The patterns define the components and interconnections that make up the microchip's circuitry. Once the layers are deposited and patterned, the microchip goes through several additional steps, including doping the transistors, adding metal interconnects to establish electrical connections between components, and applying passivation layers to protect the circuitry. These steps are repeated multiple times to create the complex network of components and interconnections required for the microchip's functionality.

The completed microchip is then packaged to protect it from physical damage and provide electrical connections to the outside world. The package typically includes leads or pins that allow the microchip to be connected to a circuit board or other electronic devices. Microchips can perform a wide range of functions, depending on their design and application. They can be found in almost every electronic device today, from smartphones and computers to household appliances and automobiles. They serve as the "brains" of these devices, enabling them to process data, perform calculations, store information, and control various functions. In summary, microchips are complex integrated circuits made of semiconductor materials that contain numerous electronic components and interconnections. They are manufactured through a sophisticated process that involves layering and patterning materials on a silicon wafer. Microchips are fundamental to modern electronics, enabling the functionality and automation we rely on in our daily lives.

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. It is transponder means wireless communication monitoring

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. Every microchip has unique identification number which link with.

## Can microchips works in human body??

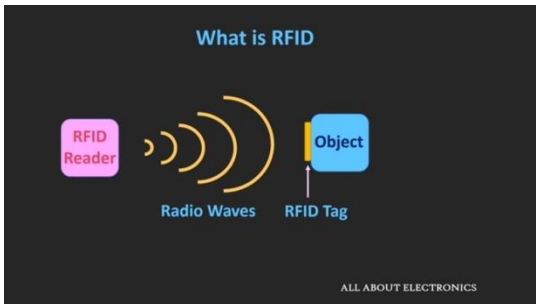
Microchips can work in human bodies. These chips are called implantable medical devices, and they are used to monitor and treat various medical conditions. For example, pacemakers are implantable devices that use microchips to regulate the heartbeat, while cochlear implants use microchips to help people with hearing loss. The most common type of microchip that is implanted in the human body is the implantable medical device (IMD). These devices are used to monitor and treat various medical conditions. Some examples of IMDs include pacemakers, which regulate the heartbeat, cochlear implants, which help people with hearing loss, and deep brain stimulators, which treat Parkinson's disease and other neurological conditions.

### Types of technology to implement microchips:

There are different types of technology used to implement microchips in the human body. One of the most common types is radio-frequency identification (RFID) technology. RFID chips are small, passive devices that can be implanted in the body and used to store and transmit data wirelessly. Another type of technology is wireless telemetry, which uses radio waves to transmit data from an implanted device to an external receiver. This technology is commonly used in medical devices like pacemakers and neuro stimulators. Yet another type of technology is biocompatible materials, which are materials that are safe to use in the human body. These materials can be used to create implantable devices that are safe and effective for long-term use.

## About RFID chip

RFID (Radio Frequency Identification) chips are small electronic devices that can be used to store and transmit data wirelessly. They consist of a tiny microchip that is attached to an antenna, which allows the chip to communicate with a reader device. RFID chips are commonly used in applications like inventory management, access control, and payment systems. In the medical field, RFID chips can be used to track medical equipment and supplies, as well as to monitor patients. Some people have even chosen to have RFID chips implanted in their bodies for various reasons, such as to store medical information or to use as a form of identification.




RFID chips have several advantages, such as:

- They can be used to track inventory and assets in real-time, which can help businesses save time and money.

- They can be used to improve supply chain management and logistics, which can help businesses operate more efficiently.

- They can be used to improve access control and security, which can help prevent theft and unauthorized access.

- They can be used to monitor patients in hospitals and other healthcare facilities, which can help improve patient care.

However, there are also some disadvantages to RFID chips, such as:

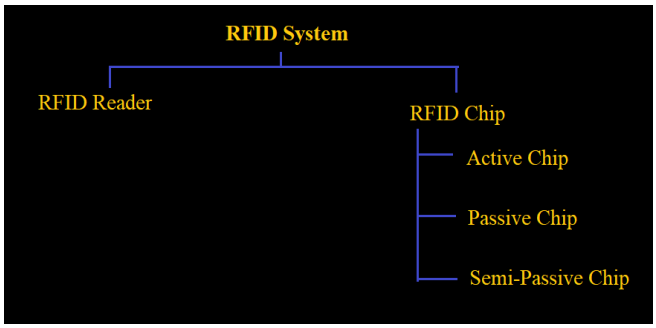
- They can be expensive to implement, which can be a barrier for some businesses.

- They can be vulnerable to hacking and other security threats, which can put sensitive data at risk.

- They can raise privacy concerns, as some people may feel uncomfortable with the idea of being tracked or monitored.

- They can be difficult to remove once they have been implanted, which can be a concern for some people.

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 of the RFID reader object can be identified by the reader. By using this technology, we can track multiple objects at a time.




.

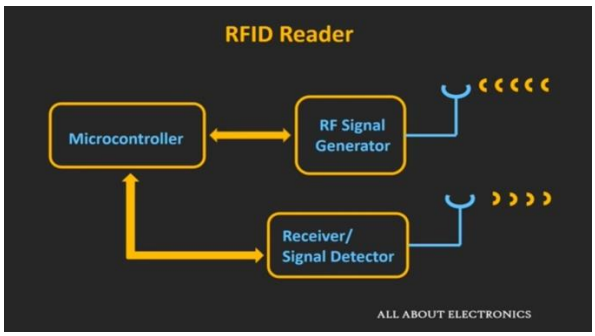
There are two main types of RFID chips: passive and active.

Passive RFID chips do not have their own power source, but instead rely on the energy from the reader to power the chip and transmit data. They are typically smaller and less expensive than active RFID chips, and are often used for applications such as inventory tracking and access control.

Active RFID chips, on the other hand, have their own power source and can transmit data over longer distances than passive RFID chips. They are often used for applications such as vehicle tracking and asset management.

There are also semi-passive RFID chips, which have their own power source but only transmit data when they are within range of a reader. These chips are often used for applications such as temperature monitoring and asset tracking.

**RFID Reader**




RFID readers are used to wirelessly read and transmit data from RFID tags or labels. They use radio waves to communicate with the tags and can read multiple tags at on once. RFID readers can be used in various industries such as retail, healthcare, and logistics. They come in different form factors and can be handheld, fixed, or integrated into other devices. They can read tags from a few centimetres to several meters away, depending on the type of reader and tag**.** There are several types of RFID readers, including:

- Fixed RFID readers, which are stationary and can be used for applications such as inventory management and access control.

- Mobile RFID readers, which are handheld and can be used for applications such as asset tracking and field service.

- Integrated RFID readers, which are built into other devices such as smartphones and tablets.

RFID readers have several advantages, such as:- They can be used to read multiple tags at once, which can save time and improve efficiency. They can be used to read tags from a distance, which can be useful in applications such as access control and asset tracking. They can be used in harsh environments, such as warehouses and manufacturing plants. However, there are also some disadvantages to RFID readers, such as they can be expensive to purchase and maintain. They can be vulnerable to hacking and other security threats, which can put sensitive data at risk. They can raise privacy concerns, as some people may feel uncomfortable with the idea of being tracked or monitored**.** An RFID reader consists of three main components: an antenna, a transceiver, and a decoder.

The antenna is used to transmit radio waves to the RFID tag and receive the response from the tag. The antenna can be either internal or external, and the size and shape of the antenna can vary depending on the specific application.

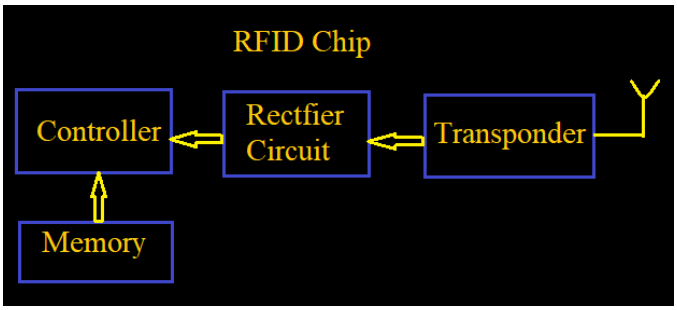
The transceiver is responsible for sending and receiving radio signals to and from the antenna. It also modulates the signal received from the antenna and demodulates the signal that is sent to the tag.

The decoder is responsible for decoding the signal received from the transceiver and converting it into a format that can be read by a computer. The decoder can also perform additional functions such as filtering and data manipulation.

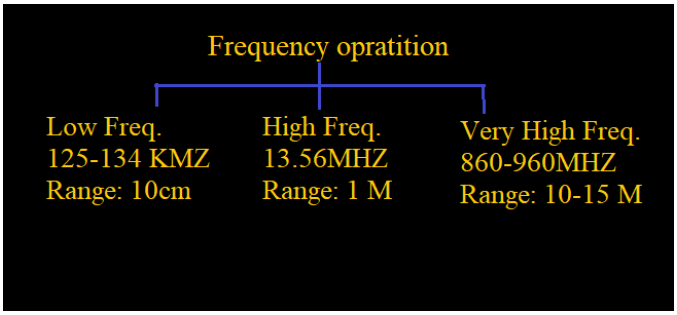
In addition to these components, some RFID readers may also include additional features such as a power source, memory, and a user interface.

**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)

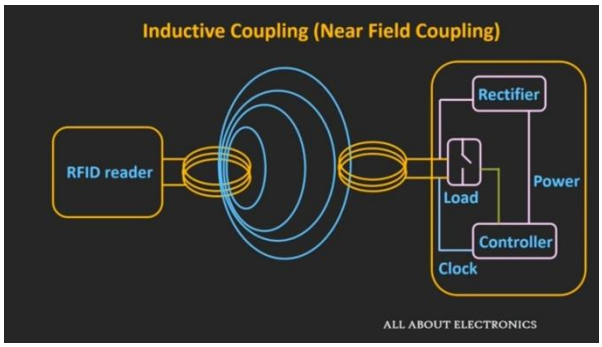
RFID readers continuously send radio waves with a particular frequency. Radio waves sent by RFID readers used for three purposes:

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.

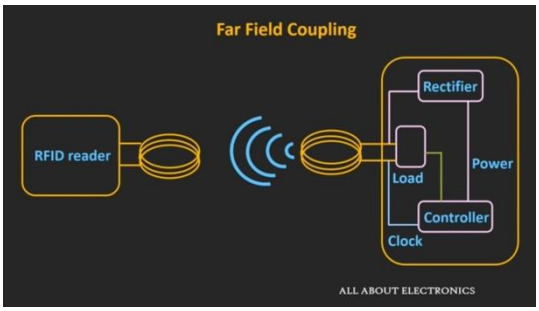
In this case, the RFID reader and RFID chip are very close to each other. The field generated by the RFID reader is used to get a couple with an antenna of the RFID chip because of this mutual coupling the voltage gets induced across the RFID chip some portion of the voltage gets rectified and use as 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 in-backscatter 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:**

The idea of implanting microchips in humans has been a topic of debate and controversy. While there are some potential benefits to using microchips for medical purposes, such as tracking patient data and monitoring vital signs, there are also concerns about privacy, security, and personal autonomy. Some people worry that the use of microchips could lead to a loss of privacy, as the data collected by the chips could be used for surveillance or other purposes without the individual's consent. Others worry that the use of microchips could be used to track or control individuals, or that the technology could be hacked or used for nefarious purposes. It's important to note that the use of microchips in humans is currently very limited, and there are strict regulations in place to ensure that the technology is used safely and ethically. However, it's also important to continue to have conversations about the potential risks and benefits of emerging technologies, and to work to ensure that they are developed and used in ways that are safe, ethical, and responsible.

**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. RFID technology is generally considered to be safe and non-harmful to the body. RFID tags and readers use radio waves to communicate, which are a type of electromagnetic radiation. However, the radio waves used in RFID technology are generally low-frequency and low-power, and are not considered to be harmful to the body. In addition, RFID tags are typically very small and are designed to be implanted or attached to the body in a way that minimizes the risk of injury or harm. RFID tags used for medical purposes, for example, are designed to be biocompatible and safe for use in the body. That being said, it's always important to follow proper safety procedures when using any type of technology, and to be aware of any potential risks or hazards associated with its use. If you have any concerns about the safety of RFID technology, you should consult with a qualified healthcare professional or technology expert.

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.

**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 micro+2/chipping 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**

- https://www.researchgate.net/publication/221787702_RFID_Technology_Security_Vulnerabilities_and_Countermeasure
- https://lhsepic.com/1232/opinion/microchips-invade-employees-privacy/
- https://www.bbvaopenmind.com/en/technology/innovation/technology-under-your-skin/
- https://www.divaportal.org/smash/get/diva2:1572358
- https://www.youtube.com/watch?v=Ukfpq71BoMo&t=346s
- https://www.youtube.com/watch?v=Zy7a6W8OG5s
- https://www.youtube.com/watch?v=Gs0bVs8QuWE&t=16s