It's still magic even if you know how it's done.

-Terry Pratchett

Photo by Veronica Adrover

Science Fiction Twenty Years Ago, a Nanotechnology Reality Today: Human Microchip Implants

Neel Patel

University of California, Merced

Radio-Frequency Identification, RFID, Nanotechnology

Undergraduate Research Journal
University of California, Merced

Abstract

In recent years, Radio-Frequency Identification (RFID) technology has been on the rise with implementing new uses of the technology. This paper will start with examining the history of RFID chip and how it has evolved overtime. Afterwards, it will be going into views from scientists. Next, possible uses of the technology in different fields will be discussed. Lastly, privacy and safety issues will be addressed.

Undergraduate Research Journal
University of California, Merced

Introduction

Radio-Frequency Identification (RFID) technology first began in the twentieth century with the sole intention of identifying military aircrafts during World War II. Since then, RFID has moved away from the military sector and has enhanced into the consumer products. An RFID chip is a communication device that is capable of transmitting radio waves to a static reader, which was first patented in 1983 and first used in consumer products in 1997. Nearly twenty years later, research is being done on the same chip to make it is capable of being implemented into humans for everyday use. Specifically, microchips would be implanted in the palm of the hand, so it can be easily accessible. Microchips have already advanced medically – such as the pacemaker which is used only in patients with certain heart conditions. The current RFID microchipping research is leading in the direction to make the chips capable of making payments, authorizations, lock and unlock doors, store medical records, and act as an identification. All of these functions will be all accessible from a small unique microchip in your hand. Like any technology, some issues will arise from the public concerning the emergence of the new use of this technology.

Nanotechnology from the View of a Futurist

Michio Kaku is a well-known futurist and a popularizer of physics in the technology industry. Kaku is commonly known in mainstream media for his knowledge of complex subjects of emerging technology and science. He has received the Klopsteg Memorial Award in 2008 for one of the most notorious books, *Physics of the Impossible.* In 2011, Kaku published a sequel to

Undergraduate Research Journal
University of California, Merced

the previous book, *Physics of the Impossible,* called *Physics of the Future.* The sole intention of the *Physics of the Future,* publish the time frames of when evolving technology will emerge into everyday use of consumers. Kaku has predicted that Nanotechnology will emerge into consumers everyday use anywhere from now to 2030. Kaku stated in his book, "One goal of nanotechnology is to create molecular hunters that will zoom in on cancer cells and destroy them cleanly, leaving normal cells intact. Science fiction writers have long dreamed about molecular search-and-destroy craft floating in the blood, constantly on the lookout for cancer cells. But critics once considered this to be impossible, an idle dream of fiction writers" (Kaku). Kaku believes that Nanotechnology is going to be so small that is will be able freely flow in the bloodstream. With the newly improved microchips, he believes that they will be capable of transmitting live video of the inside organs and perform Nano surgeries. To reach that level of use, he believes the consumers must first be able to accept microchip implants in the hand. Having the microchip would be necessary because it would act as a transmitter between the Nanotechnology particle in your bloodstream and the live feed viewer, such as a monitor. Rendering from the data Kaku obtained for his book, the U.S. government has invested $1.5 billion in Nanotechnology research hoping for microchips had consumers can use in the medical, industrial, aeronautical, and commercial applications.

Evolution of RFID Chip

Radio- frequency identification technology started from the roots of the radar technology which was first developed in the 1920s. In the 1940s, the RFID was invented by Harry

Undergraduate Research Journal
University of California, Merced

Stockman. In the 1950s, RFID chips started to be studied in military laboratories to further develop its range to enable to use in airplanes at longer ranges. It wasn't until the 1960s to 1980s that RFID chips were studied and re-engineered to be used in markets outside the military sector. The companies Checkpoint, Knogo, and Sensormatic were the first to develop anti-theft devices that are still used today, nearly forty years later, in department stores and libraries. In the late 1980s, the RFID had entirely moved away from the military sector to the commercial market. In the U.S., RFID technology was typically being used in transportation systems and animal tracking. Having the RFID chips in transportation allowed trucks to bypass weight stations by having all the information needed at the stations transmitted to RFID readers on the highway using the chip. Using the chip helped trucking companies save millions because the vehicle did not have to slow down on highway just to accelerate again and saved travel time. In the late 1990s and early 2000s, RFID chips hit the laboratories again, but this time it was not for consumer products, it was for humans. In 2004, after years of successful research, the US Food and Drug Administration approved the first implantable RFID chip in humans called VeriChip. This was a major break though in combining technology and medical research together; improving and making human lives safer. Even though the implantation was proved in 2004, it was not until 2017 that the first group of people were implanted with microchips for everyday use. A company called "Three Square Market" has begun the movement by implanting the microchip in four dozen of their employees. The current chip allows employees to pay at company vending machines, lock and unlock doors, and log into computers. The Three Square

Undergraduate Research Journal
University of California, Merced

Market was the first group to implant this emerging technology and it is a huge step forward. It took thirteen years, but the RFID microchip technology is emerging in everyday use.

Structure of the Microchip

As previously mentioned, the RFID microchips initial intention was to act as identifiers for planes and to use as a low cost anti-theft device in department stores. As the technology evolved over the years, the intention of the microchip was changed; to make payment authorizations, lock and unlock doors, store medical records, and act as an identification. Since research begin to change the use of RFID technology, a new branch of the RFID was created called the Near-field Commutation (NFC). The NFC technology was first patented in 1997 and was put into consumer products in 2007. The technology of NFC was the same was RFID. The only difference in the NFC was that it would only be used to transfer data within an approximately few centimeters between the device with NFC and the receiver while RFID range is extendable. This is the same technology found in all smartphones that use mobile payments such as Apple Pay, and Android Pay. The microchips would use both the RFID and NFC technologies. According to the research conducted by Katina Michael, having both technologies in the chip will allow far and near communication making it safer. It would be safer because the NFC technology in the microchip would be used to transfer sensitive data such as payment authorizations and non-sensitive information such identifying yourself would be routed though the RFID technology. Having the microchips with both of these technologies makes the microchip technology as a whole a lot safer and efficient in terms of cost and reliability.

Undergraduate Research Journal
University of California, Merced

Microchips for Medical Use

Technology has already been implanted in humans for medical purposes such as the pacemaker, so have technology used for the medical sector is not new. Having this technology implanted in humans will allow health care providers to store your medical history directly onto the chip. Janice Hopkins Tanne is a well-known medical journalist, researcher, and consultant for doctors, who has researched and written about microchip implant benefits for medical use. Tanne concluded that having such technology that will allow doctors to store for medical history such ones' blood type, allergies, disorders, etc. which is beneficial to the consumer in a tragic event that would require immediate medical attention (Janice Hopkins Tanne). To properly treat to patients, doctors need to know ones' medical history so if one was injured in a tragic event and rushed to a hospital and there was no one with the patient that can provide medical history to the medical staff, the implanted microchip would be able to provide it so the medical staff can accurately provide medical assistances. Another benefit of having a microchip implanted related to the medical use would be having the ability to store ones' Medical Power of Attorney. The Medical Power of Attorney states the person the patient wants to make medical decisions on their behalf if the patient is unresponsive for example, if the patient needs surgery and the option is to amputate a leg or to attempt to recover the leg with the possibility of death, the person listed on the Medical Power of Attorney stored on the microchip would make the decision. This would allow fast treatment because the medical staff would know who to contact in such situation rather than identifying the patient and calling a family member to determine who the patient had

Undergraduate Research Journal
University of California, Merced

authorized. Having a microchip implant will allow patients to be treated fast, effectively, and at their willpower.

Consumer Safety using Microchips

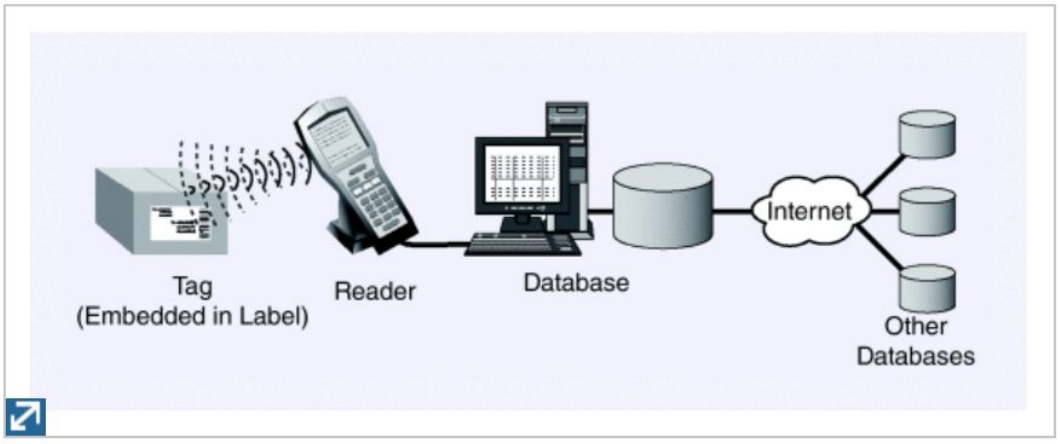
As technology has prevailed, consumers and businesses are starting to move away from paper currency to digital cryptocurrency. This may be a good thing we are advancing technology in our finances, but it is also creating a huge market for thieves. Every day we carry a piece of plastic card ultimately has your address, birthday, phone number, social security number, and account number. If that one plastic card is lost by a consumer, they basically gave up their whole identity to the person who found the card eventually resulting in identity theft. With technology prevailing, the threat of identity theft has always increased and never decreased.

Having payments made and authorized using the implanted microchip will drastically decrease identity theft (Katina Michael). When a consumer swipes their card at a local supermarket and enters their Personal Identification Number (PIN), there is always a set of wandering eyes around you that might have had a look at your PIN when you had entered it making your identity and finances vulnerable if the card had been lost. Being able to just place your hand on a payment terminal would significantly reduce the consumers of unauthorized payments because they would not be needing to carry a physical card and do not need to enter a PIN. The microchip would have a digital card stored so when the hand is placed on the terminal, the microchip would use the NFC technology inside the microchip to transmit the payment authorization to the terminal.

Undergraduate Research Journal
University of California, Merced

Having a microchip implantation would give the consumer a unique identification which would help reduce identity theft. When a consumer goes to a bank to apply for a loan, the only thing that they currently ask for is two forms of ID cards to provide that you the person with the name and social security number that is written on the application. It is not hard to make fake ID cards to prove an identity. Having a microchip implanted will allow lenders to verify the consumer's identity by being able to scan the consumer's hand. The microchip would have a unique identification code that would be cross-referenced with a government database to verify the identity which would help prevent identity theft making it safer for consumers (fig. 1). The database with used to verify an identity would only be given to authorized companies and trained personal to use the database. The personal would need to be trained to use the database due to safety precautions and because the system would be encrypted (fig. 2). Most identity theft starts off your credit card is lost or stolen. Having a microchip implanted will allow identity theft to be reduced.

(fig.1)



Components of an rfid system. (image courtesy of the u.s. government accountability office.)

Undergraduate Research Journal
University of California, Merced

(fig. 2)

RFID Tag	New Profile / Old Profile as stored in database for a sample of RFID tags
FD7EE477	305B6F0D35DA7739DFF78FFDE3092F737CE94E335FEF6454C7F26A6E694AD79B7FD0A470
	2E5B6F0D35DA7739DFF78FFDE3492F737CE94E335FEF64FFC7F26A6E694AD79B7FD03232
FDC1DB77	49076644BDF82762785A3B0E73C65B9F2653BEEE88991D5311B1AFA4BA332D3CFB36CEF1
	1007E644EDF82762785A3B0E73C65BFF2653BEEE88991D531131AFA4BA532D3CFB3635DD
FDCB5377	4B1BA2A1DB9379B837B0C7B1964B8524B1BB2B28BFD9B05679FD8CC516FDB80D4F34AC47
	BD1BA221DB9379B837B0C7B1964B8524B14B2B28BFD9B05679FD8CC516FDB80D4F34EE21
FDBD3177	• 5FOBF32149704E08630F248425FFAF6E86D8A41DFEB43E6A862832AC964EBBBC25BE8EF2
	AFOBF321AC704E08630F248425FFAF6E86D8A41D6EB43E6A862832AC964E6BBC25BE9C1C

Microchips implants will allow humans to make payment authorizations, lock and unlock doors, store medical records, and act as an identification from the wave of ones' hand. The RFID technology has evolved drastically over many decades. Recently with the new research, RFID chips are able to be implanted in humans. Having the microchip implanted makes it safer for consumer medically and finically. Microchip implants have also been predicted by the futurist Michio Kaku. Having this technology implanted in our hands will allow us the move away from plastic cards, keys, and identity theft.

Ethical and Unethically Issues of Microchipping Humans

The idea of having a microchip implanted in your hand means the consumer will have a unique number to act as an identification and will have the ability to store personal information while being able to process that information when commanded to do so. As good it may sound, there will always be concerns that arise from new upcoming technology. The implantable microchip technology has been a controversial topic since the first microchip, VeriChip, was approved by the FDA in 2004. Since the birth of this technology, controversy for this technology

Undergraduate Research Journal
University of California, Merced

whether its safety design, tracking capabilities, and privacy of consumers has become a concern for many potential consumers. There have been many studies conducted to expose the potential issues and to find a way to correct the issues so it is safe and reliable for the public to use.

Safety of the Technology

When a case is sent to the Federal Drug Administration (FDA) for an approval, a group of highly trained professional, in their respected field of study, reviews the item in question to determine if it is safe for the public to use and if it is ethically appropriate to use. The implantable microchip went through the same process before it was approved by the FDA. Even though the FDA that approved the microchip, many scientists still had concerns about how safe the microchip is so many conducted research studies. According to Perakslis, a study was conducted a study in 2010: "Between 2005 and 2010, the unwillingness ("Strongly unwilling" and "Somewhat unwilling") of college students to implant an RFID chip into their bodies decreased by 22.4% when considering RFID implants as method to reduce identity theft, decreased by 19.9% when considering RFID implants as a potential lifesaving device, and decreased by 16.3% when considering RFID implants to increase national security (Perakslis pg.1)". This an example of a study that proved that more consumers are worried about the safety of the technology. Even though it had been six years since the technology was approved and research was continued, the number of people that felt the microchip was safe decreased by nearly 22%. Because of the declining approval ratings of technology, researchers are conducting studies so the technology can be further developed to be safe for consumers to use.

Undergraduate Research Journal
University of California, Merced

Every piece of technology ever invented to this day has required a power source. When the microchip technology was approved, one of the biggest concerns expressed by the consumers was how the chip was going to be powered and whether or not it required a battery to also be stored implanted along the microchip. According to the research conducted by Janice Tanne, implantable microchips use a specific type of tag called passive. Passive tags are designed so that it does not require a battery to be attached in order to run the microchip. This specific design enables the microchip to run on the power of the incoming radio signals, which also enables the microchip to last a lifetime without needing to replace the power source. The research conducted on the power source for technology showing that due to the fact that there is no battery attached to the microchip, surveys have shown technological issues about the safety of this technology had been reduced to only 28% (Perakslis). Consumers surveys reporting that the out of all the possible issues, the technological aspect it rated the lowest proves that the consumers trust the safety of this technology.

Secure Payment Processing

One of the major aspects of the microchip is the ability to authorize payments with the wave of your hand. Many concerns regarding the safety of the payment transaction can be brought up by potential consumers of the microchip. Having the NFC technology embedded in the microchip allows transactions to be processed only in close proximity. Currently, NFC technology is used in smartphones to allow safer payment processing because a physical card is

Undergraduate Research Journal
University of California, Merced

not needed because a digital card is stored within the smartphone but leaving the possibility of the phone to be hacked and financial data to be stolen. Having the microchip use the NFC technology instead of a smartphone to process payments will take away the issue that has concerned nearly every consumer, payment fraud because microchips are not hackable (Katina Michael). The microchip is not connected to the internet, and, therefore, is not vulnerable to hacks. As the number of consumers starts using the microchip increases, the number of financial thieves will decrease only helping the consumers.

Possibility of Tracking

Every change comes with risks. Without taking risks, nothing would ever change nor improve. Having a microchip with GPS capability obviously raises the concern of the others misusing the technology, including the government, to track our movements. We already have the issue with the government already spying on citizens using their cameras on cell phones and laptops tracking next thing we want is government tracking our movements. The study conducted by Liz McIntyre shows that they are mostly concerned about the government having the ability to track every movement of the consumer. Microchip comes with GPS technology allowing it to be tracked. In recent years, evidence has shown that the government has used their resources watch and track citizens using their smartphones and computers.

Many consumers currently use company provided cell phones. A concern that many have is whether or not their employers have the ability to track the movements of their employees

Undergraduate Research Journal
University of California, Merced

according to the study conducted by Karma Allen. Currently, employers like hospitals provide cell phones to their doctors with the condition to track them so they know which doctor is closer in proximity to the hospital in case of an emergency. So, the question that will remain unanswered is, will employers track their employees besides work purposes because the microchip will always be with you, unlike smartphones which can be left behind? Like every device with the GPS technology, there will always be a possibility of someone misusing their authority and there is nothing consumers can do to prevent it.

Having the GPS technology in the microchip will help solve crimes, put away the guilty, and even prove innocence. When law enforcement is investigating a person to solve a crime, detectives will ask the person of interest for their location when the crime took place. Many times, people are not able to prove where they were so are found guilty because they couldn't prove where they were. Sometimes criminals may make a fake alibi which eventually leading the case to be dismissed because of lack of evidence. Having the GPS in the microchip would allow law enforcement to get a warrant and search the history to either prove or disprove the alibi of the person of interest. Having a microchip implant will help prove and guiltiness and innocence.

Medical Privacy

According to the current medical laws, doctors cannot release medical information of their patients without the consent. The microchip would have technology that would allow doctors to store medical information about the consumer directly into the microchip. During a

Undergraduate Research Journal
University of California, Merced

visit, the medical staff would have access to all the medical information stored on the microchip. The medical staff could potentially unethically violate the law by accessing the medical information without being caught. According to Janice Tanne, the research conducted on the microchip has already identified the issue with unauthorized access to medical information. To help prevent unauthorized access, the software would be developed and implemented to allow only doctors with different tiers of credentials to access the information stored in the different tiers.

The information stored on the microchip would only be able to be read using special RFID enable reading devices. Like previously stated, the microchips will be equipped with the NFC technology which only allows signals to extend only to a few centimeters. In a study conducted by Janice Tanne, the procedure to use the technology for patients is explained; “A handheld scanner passed near the injection site activates the chip and displays the number on the scanner (pg. 1)”. Because the data would be transmitted via the NFC technology, the medical scanners would only be able to gather patient information by placing the scanner on top of the microchip’s location. Having data transmitted using the NFC technology onboard the chip takes away the possibility of others being able to intercept the signal and violating the medical privacy of others. The special scanner that will allow hospitals to view information would only be exclusively sold to health care providers so others with bad intentions are not supplied with tools to violate patient’s privacy, adding another layer of security directly from the manufacturer. Having this special reader exclusively for health care providers will help protect the privacy of

Undergraduate Research Journal
University of California, Merced

the consumers. The reader will cost about $650 and individuals that can provide evidence that they work for a health care provider will be allowed to buy the reader only from the manufacturer (Janice Tanne). Have these protocols internally and externally of the microchip will allow consumers to utilize the technology without having to worry about medical privacy.

Laws on Microchips

As new technology emerges, laws also have to be updated to accommodate the new technology to keep the consumers and public safety for the use of the technology. There are many ethical and unethical issues that come along with the use implantation of microchips in the human body. On the major issues with the microchip is the use of RFID reader to access information stored on the consumer's microchips. Having laws in place that require proper authorization and permits to buy a reader would protect consumers from unauthorized personal gaining confidential information.

Currently, people that work in high profile jobs such as a banker, have to go through a deep background to make sure they are involved in illegal activities, having a law in place that only allows people had passed a deep background check be able to read consumer microchips and handle their material. Another huge concern that consumers will have, it the possibility of their employers tracking their movements outside of work. To prevent that, the government should implement a law that requires consumers to authorize employers to tracking their movement in the time frame entered into the system. The system would be designed that once

Undergraduate Research Journal
University of California, Merced

the window of time is up, the employer would not have access to view the employees' movements. There also should be an article within that law that states the tracking law is not just limited to employers but also all citizens to prevent people from stalking each other. Having such laws will help protect the consumers from anyone that tries to use the technology unethically and hold those individuals who do accountable for their actions.

The emergence of this human implantable microchip will revolutionize the how health providers provide service to patients, how payments are processed and authorized, and most importantly how it will make consumers safer with a unique identity. This piece of technology that can potentially improve lives which only costs between $150 to $200 to implant (Tanne pg. 1). The technology is so small, size of a grain of rice (fig. 3), that it can be implanted in the palm of your hand without any complications (Michael pg.1). Like any technology, the microchip has its pros and cons but still has the potential to re-shape the world making it a safer place for consumers.

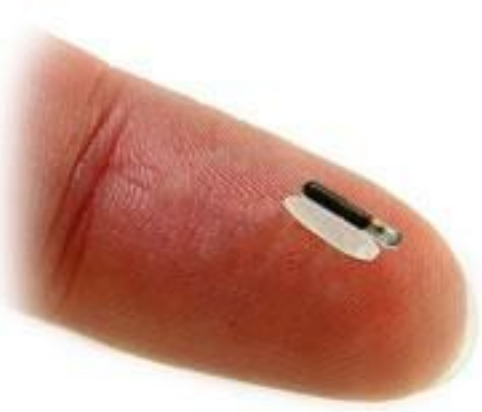


Fig. 3: A figure of the Implantable Microchip technology (Kelly Nash, 2016)

Undergraduate Research Journal
University of California, Merced

References

Gadzheva, Maya. “Getting Chipped: To Ban or Not to Ban.” Information & Communications Technology Law, vol. 16, no. 3, 4 Dec. 2007, pp. 217–231., doi:10.1080/13600830701680537. n.d.

Gasson, Mark N. “Human Enhancement: Could You Become Infected with a Computer Virus?” IEEE International Symposium on Technology and Society, 2010, pp. 61–68., doi:10.1109/istas.2010.5514651. n.d.

Mazanov, Jason. “Intersecting Performance Enhancing Smart Technologies, Health and Social Science.” Performance Enhancement & Health, vol. 5, no. 3, May 2017, pp. 87–88., doi:10.1016/j.peh.2017.04.001. n.d.

Mcintyre, Liz, et al. “RFID: Helpful New Technology or Threat to Privacy and Civil Liberties?” IEEE Potentials, vol. 34, no. 5, 4 Sept. 2015, pp. 13–18., doi:10.1109/mpot.2015.2410392. n.d.

Michael, Katina, and Mg Michael. “The future prospects of embedded microchips in humans as unique identifiers: the risks versus the rewards.” Media, Culture & Society, vol. 35, no. 1, 2013, pp. 78–86., doi:10.1177/0163443712464561. n.d.

Michael, Katina. “RFID/NFC Implants for Bitcoin Transactions.” Media, Culture & Society, IEEE Consumer Electronics Magazine, vol. 5, no. 3, 2016, pp. 103–106., doi:10.1109/mce.2016.2556900. n.d.

Undergraduate Research Journal
University of California, Merced

Perakslis, Christine, et al. “Perceived Barriers for Implanting Microchips in Humans: A Transnational Study.” 2014 IEEE Conference on Norbert Wiener in the 21st Century (21CW), 2014, doi:10.1109/norbert.2014.6893929. n.d.

Pettersson, Mona. Microchip Implants and You : A Study of the Public Perceptions of Microchip Implants. 2017, http://urn.kb.se/resolve?urn=urn:nbn:se:umu:diva-133890. n.d.

Undergraduate Research Journal
University of California, Merced

Neel Patel is a first year pursing his Bachelors' of Science Computer Science and Engineering. Patel is passionate about nanotechnology and artificial intelligence and plans on work with it for his career. Currently, Patel in involved with Engineering Service Learning working part of Project Protect where is using his knowledge in software development to make a difference in the medical field and aid underserved community.