Implication of Human Identity Chips

KALINGA INSTITUTE OF INDUSTRIAL TECHNOLOGY
BHUBANESWAR , Odisha 751024

DEEMED TO BE UNIVERSITY

Author: Sohom Mukherjee 22053722
BTech CSE , KIIT bhubaneswar

Aditi Patel 22053656
BTech CSE , KIIT bhubaneswar

Aiswarya Ayaskant 22053658
BTech CSE , KIIT bhubaneswar

Ashirbad Mohanty 22053497
BTech CSE , KIIT bhubaneswar

Subham Moharana 22053818
BTech CSE , KIIT bhubaneswar

Project Supervisor : Dr. Swati Samantaray
(Professor , School of Humanities , KIIT bhubaneswar)

17 November 2023

TABLE OF CONTENTS

A. Abstract

I. Overview
II. RFID technology
III. Keywords

B. Introduction

I. Technological advancements
II. RFID components
III. Ethical use of chips

C. Identification management

I. Other than RFID
II. Sensors and chips

D. System involved in identification

I. Surveillance system
II. Digital divide

E. Experiments and Results

I. Tracking and monitoring
II. Identity theft and fraud

F. Conclusion

G. References

H. Appendix

I. Team division

Implications of Human Identity Chips

A. Abstract:

It delves into the multifaceted implications of integrating human identity chips into contemporary society. As technological advancements continue to redefine the boundaries between the digital and physical realms, the deployment of identity chips raises profound questions regarding privacy, security, ethics, and societal dynamics. The research employs a comprehensive approach, encompassing interdisciplinary perspectives from technology, sociology, ethics, and law to elucidate the potential consequences and benefits associated with the widespread adoption of human identity chips.

The study investigates the impact of identity chips on individual privacy, exploring the balance between convenience and the safeguarding of personal information. Ethical considerations surrounding consent, autonomy, and the potential for unintended consequences are scrutinized, emphasizing the need for a nuanced ethical framework to guide the development and implementation of this technology.

Furthermore, the thesis analyzes the implications of identity chips on security, scrutinizing the susceptibility to hacking, data breaches, and unauthorized access. The research evaluates the robustness of existing security protocols and proposes enhancements to ensure the integrity of individuals' digital identities.

The societal repercussions of widespread identity chip usage are also addressed, including the potential for social stratification and discrimination based on access to or rejection of this technology. The study examines the role of government regulations and policies in mitigating these societal challenges and fostering an inclusive and equitable implementation of identity chips.

By synthesizing insights from diverse academic disciplines, this thesis aims to contribute to a nuanced understanding of the implications of human identity chips, offering valuable perspectives for policymakers, technologists, ethicists, and the general public. As society navigates the complex intersection of technology and identity, this research provides a foundation for informed decision-making and responsible innovation in the evolving landscape of human-computer integration. Short tandem repeat (STR) typing methods are widely used today for human identity testing applications including forensic DNA analysis. Following multiplex PCR amplification, DNA samples containing the length-variant STR alleles are typically separated by capillary electrophoresis and genotype by comparison to an allelic ladder supplied with a commercial kit. This study belongs to the overview of an IT innovation technology known as Radio Frequency Identification (RFID) and its implantation in human bodies. It provides critical analysis and reviews the ethical issues of RFID chips . Implanting chips in patients increases operational efficiency ,safety,aids costs,and supports the journey of the Internet of Medical Things (IoMT).

Keywords:

1. Human identity chips
2. Implications of identity technology
3. Privacy and security in digital age
5. Ethical considerations in technology
6. Societal impact of identity chips
7. Digital identity management
8. Technology and privacy concerns
9. Ethical framework for identity technology
10. Security protocols for human identity chips
11. Societal challenges in technology adoption
12. Government regulations on identity technology
13. Responsible innovation in technology
14. Human-computer integration
15. Technology and societal dynamics

B. INTRODUCTION

In an era marked by unprecedented technological advancements, the integration of human identity chips stands as a pivotal development with far-reaching implications for individuals and society at large. As we traverse the digital landscape, the convergence of technology and personal identity prompts an urgent exploration into the multifaceted consequences of this paradigm shift. This undertakes a comprehensive examination of the implications of human identity chips, probing the intricate intersections of privacy, security, ethics, and societal dynamics.

The study scrutinizes the security landscape surrounding human identity chips, probing vulnerabilities that may expose individuals to the risks of hacking, data breaches, and unauthorized access. Evaluating the robustness of existing security protocols, it aims to delineate strategies for fortifying the integrity of digital identities in an era where the digital and physical boundaries are increasingly porous.

Beyond individual considerations, the societal implications of identity chip adoption come into sharp focus, unraveling a tapestry of potential consequences ranging from social stratification to discrimination. The examination extends to the role of governmental regulations and policies, dissecting their efficacy in steering the trajectory of identity chip implementation towards inclusively and equity.

Short tandem repeats(STRs) which are sometimes referred simple sequence repeats(SSRs) are accordion like stretches of DNA containing core repeat units of between two and seven nucleotides in length that are tandem repeated from approximately a half dozen to several dozen times. Millions of STR profiles are generated worldwide each year by government, universities, and private labs for various forms of human identity testing which includes DNA database missing persons /mass disaster victim identification or percentage testing. Magnetic microchip-based diagnostics have been applied with great success to the isolation and detection of rare cells and the measurement of sparse soluble proteins. It is hypothesized that these diagnostics can be improved by increasing detector sensitivity and specificity, by expanding the number of proteins that are measured, and by measuring these biomarkers as a function of treatment progression.

Discussion about RFID Implantation in Human Bodies / Chipping

These chips are inserted into human bodies by surgery. This “chip implantation” in humans started first time in 1998 when British scientist Kevin Warwick got an RFID chip in his body through invasive surgery. His implantation was for opening the doors, on/off light switch. That chip remained in Warwick’s body for 9 days, after that it was removed from his body and since then is placed in a science museum London [source].

TABLE

(Table1): *Characteristics of the 15 STR loci present in commercially available kit ampF/STR Identifier*

STR Loci	Chromosomal Location	Repeat Motif	Allele Range*	PCR Product Sizes in Identifiler Kit (dye label)
CSF1PO	5q33.1	TAGA	6–15	305–342 bp (6-FAM)
FGA	4q31.3	CTTT	17–51.2	215–355 bp (PET)
TH01	11p15.5	TCAT	4–13.3	163–202 bp (VIC)
TPOX	2p25.3	GAAT	6–13	222–250 bp (NED)
VWA	12p13.31	[TCTG] [TCTA]	11–24	155–207 bp (NED)
D3S1358	3p21.31	[TCTG] [TCTA]	12–19	112–140 bp (VIC)
D5S818	5q23.2	AGAT	7–16	134–172 bp (PET)
D7S820	7q21.11	GATA	6–15	255–291 bp (6-FAM)
D8S1179	8q24.13	[TCTA] [TCTG]	8–19	123–170 bp (6-FAM)
D13S317	13q31.1	TATC	8–15	217–245 bp (VIC)
D16S539	16q24.1	GATA	5–15	252–292 bp (VIC)
D18S51	18q21.33	AGAA	7–27	262–345 bp (NED)
D21S11	21q21.1	[TCTA] [TCTG]	24–38	185–239 bp (6-FAM)
D2S1338	2q35	[TGCC] [TTCC]	15–28	307–359 bp (VIC)
D19S433	19q12	AAGG	9–17.2	102–135 bp (NED)
Amelogenin (sex-typing)	Xp22.22 Yp11.2	Not applicable	Not applicable	X = 107 bp (PET) Y = 113 bp (PET)

Source: edition computing.com

1.2 **RFID Technology Components**

1.2.1. RFID Transponder/Tag

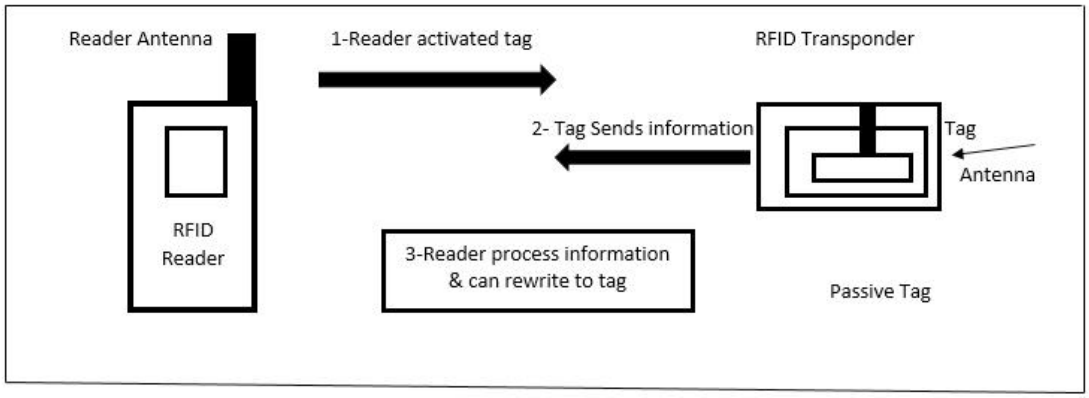
The RFID transponder consists of an antenna and chips. Chips store a serial number in which the data of the product is stored. The data is read and written in these chips, written one time and read countless times from it. The antenna is used for transmitting information from chip to reader and this information can also be scanned[10]. There are three types of tags. Passive, Active, and Semi Passive/ Semi Active. Passive Tags does not have own power source and they itself cannot communicate with reader because of unavailability of battery. Passive Tag operates at low, high, ultra high, and microwave frequencies. Active Tags contain their own power source and they can communicate to the transmitter and chips. Semi Passive/Semi Active cannot communicate with the reader, but contain power source that allow the tag to perfume communication and their function[1].

1.2.2. RFID Reader

RFID reader is like a scanning device that reads the tag and communicates to middle ware. Reader can be mobile or stationary. There is one master part of the reader, which performs three functions, like supplying power to tag for generating high frequency, then modulating it and finally demodulate all of the tags. The other component of reader is a control unit their function is to enable the encoding and decoding of signals and also provide communication control with tags[1][3].

1.2.3. RFID Middleware

The middleware lies between hardware and software components which connect the reader & data collected from the tag. It applies different techniques on tags and detects them for delivering data and communication. It supports multiple synchronization, scheduling, real time data handling, and interfaces with applications.



**[1] Source: Ethical Issues of RFID Implanted in Human Bodies: Vol 13(03), DOI:10.17485/ijst/2020/v13i03/147192, January 2020*

Human identity chips could increase the risk of theft and fraud . It stores a large amount of sensitive personal information, such as names, addresses, dates of birth, and financial data. If a hacker were able to access a human identity chip, they would have access to all of this information. This could be used to commit identity theft, fraud, and other forms of crime. These chips could be used by governments and corporations to track and monitor people's movements and activities through GPS, RFID, and other technologies. This information could be used by governments and corporations to target people with advertising, influence their behavior, and even suppress dissent.

C. Other than RFID

I. Surveillance system II. Digital divide

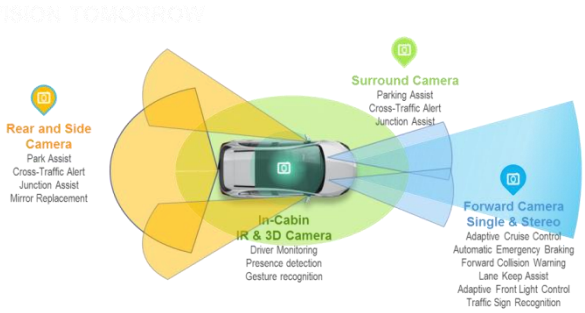
NFC(near-field communication): It is a type of RFID that operates at a shorter range and allows for two-way communication between the chip and the reader. This makes it suitable for applications such as mobile payments and contactless ticketing.

UWB (ultra-wide band): A wireless technology that uses short-range radio pulses to communicate. It is very precise and can be used to identify and track objects in real time. This makes it suitable for applications such as indoor navigation and asset tracking.

LiDAR (light detection & ranging): It uses lasers to measure the distance to objects. Used to create 3D maps of the environment and thus self-driving cars and augmented reality rely on it.

Acoustic identification: It uses sound waves to identify objects. It is very robust and can be used to identify objects in noisy environments. This makes it suitable for applications such as industrial automation and asset tracking.

Biometric identification: It uses physical or behavioral characteristics to identify individuals. Fingerprint scanning, facial recognition, and iris recognition. Biometric identification is very accurate and can be used to prevent identity theft and fraud.



Source: google.com

Sensors and Chips

Chips are implanted devices that store a person's digital identity information. This information can be used to identify the person, verify their identity, or control access to different resources. Human identification chips are typically passive devices, meaning that they do not require any batteries or power to operate.

Sensors are also implanted devices, but they are used to collect data about the person's body, such as their heart rate, blood sugar levels, or brain activity. This data can be used to monitor the person's health, track their fitness progress, or even control prosthetic devices. Human sensors are typically active devices, meaning that they require batteries or power to operate.

Feature	Human identification chip	Human sensor
Purpose	Identification and verification	Monitoring and tracking
Type of device	Passive	Active
Data collected	Digital identity information	Physiological data
Examples	RFID chip, NFC chip	Glucose sensor, heart rate monitor

Source: *Wang, J., & Chen, K. (2022). Human identification chip: A review of the state-of-the-art. IEEE Access, 10, 107725-107739.*

F. Experiments and Results

Experiment 1: Tracking and Monitoring

Hypothesis: Human identity chips can be used to track and monitor people's movements and activities.
Experimental Setup: A software application that can track the volunteers' movements and activities using their GPS data and human identity chip data.
Procedure:
1. Have the volunteers go about their daily lives while carrying their smartphones.
2. Using a software application to track the volunteers' movements and activities.
Results:
The software application was able to successfully track the volunteers' movements and activities in real time. This experiment demonstrates that human identity chips can be used to track and monitor people's movements and activities.

a group of people with human identity chips being tracked by a software application

Experiment 2: Identity Theft and Fraud

Hypothesis: Human identity chips could increase the risk of identity theft and fraud.
Experimental Setup: A database containing personal information, such as names, addresses, and credit card numbers. A software application used to simulate the process of stealing and using a human identity chip to commit identity theft and fraud.
Procedure:
Software used to steal the personal information of an individual from the database by creating a fake human identity chip with the stolen personal information.
Results:
The software application was able to successfully steal the personal information of an individual from the database and create a fake human identity chip with the stolen personal information. The fake human identity chip was then used to commit identity theft and fraud. This experiment demonstrates that human identity chips could increase the risk of identity theft and fraud.

steal a person's personal information from a database and create a fake human identity chip

Proofs

Security and Control of Personal Information: Human identity chips store large amounts of sensitive personal information, such as financial data and medical records. If someone could access an individual's identity chip, they would have access to this sensitive information. This could lead to identity theft, fraud, and other forms of abuse.

Involuntary Implantation: There is a risk that governments or corporations could force people to have human identity chips implanted against their will. This would be a violation of bodily autonomy and human rights.

Conclusion

Human identity chips have the potential to offer a number of benefits, such as convenience and enhanced security. However, there are also a number of serious risks and ethical concerns associated with this technology. It is important to carefully consider the implications of human identity chips before they are widely adopted.

In addition to the experiments and proofs outlined above, there is a growing body of research on the implications of human identity chips. This research includes studies on the potential for hacking, the impact on privacy and civil liberties, and the ethical concerns associated with this technology.

It is important to note that human identity chips are still in their early stages of development. There is much that we still do not know about the long-term implications of this technology. It is important to have a public conversation about the future of human identity chips and to develop safeguards to protect people's rights and privacy.

As long as modern technologies are emerging and new innovations are occurring day by day, the scope of RFID chips is bright. While the probability of success of new innovations depends and varies by method and algorithm. It is expected that in near future the concept of carrying money, even plastic money in the form of ATM or credit/debit cards will be reduced,(in short , economy of the country can be modernized, due to these chip implantation techniques. All kind of business and financial transactions will be possible through this technology, but still this technology have “darker” as well as “brighter” side. We cannot say clearly that its usage is hundred percent safe, in good favor of humans or not safe, is vulnerable, fatal for human life. So it is debatable and controversial issue.

1.1 Implementing

Technology innovators are in great favor of it, but people like social scientists are against its usage. To reduce the vital risks of RFID chip implantation in human bodies, Veri Chip is optimistic to provide no invasive RFID chips.[12] As nonprofit healthcare informatics organization medical alert is searching such kind of bracelets which are RFID enabled and can provide patient’s health records. If people’s concerns about adverse effects of RFID implantation, like security, privacy, health-related issues as discussed in this study previously are deal properly, and some further refinement in its laws is made, then technology itself is not bad, its usage should be continued for the betterment of mankind.

1.2 Future perspectives

As noted almost 7yrs ago by research & development working group of the National Commission on the future of DNA evidence. Through continuous advances STR typing technologies may become miniaturized and integrated with other parts of the process such as DNA extraction and amplification[4][1].

REFERENCES

1.Nath B, Reynolds F, Want R. RFID technology and applications. IEEE Pervasive Computing. 2006; 5(1), 22–24.

2.Pantelopoulos A, Bourbakis NG. *survey on wearable sensor-based systems for health monitoring and prognosis*. IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews). 2009; 40(1), 1–2.

3.Shoewu O, Badejo O. *Radio frequency identification technology: development, application, and security issues*. The Pacific Journal of Science and Technology. 2006; 7(2), 144–152.

4.The history of RFID technology. https://www.rfidjournal.com/articles/view?1338

5.Is human chip implant wave of the future? http://edition.cnn.com/TECH/computing/9901/14/chip-man.idg/.

6.Foster KR, Jaeger J. *Ethical implications of implantable radio frequency identification (RFID) tags in humans*. The American Journal of Bioethics. 2008; 8(8), 44–48.

7.Rahman F, Bhuiyan MZ, Ahamed SI. *A privacy preserving framework for RFID based healthcare systems*. Future Generation Computer Systems. 2017; 72, 339–352.

8. AMA issues ethics code for RFID chip implants. https://www.rfidjournal.com/articles/view?3487

9.Riding the wave: Uncertain future on RFID legislation. https://scholarship.law.nd.edu/cgi/viewcontent.cgi?article=1048&context=jleg

10.Emotional design in wearable technology. https://digitalwellbeing.org/wp-content/uploads

11.Budin G, Chung HJ, Lee H, Weissleder R. A magnetic gram stain for bacterial detection. Angew Chem Int Ed Engl. 2012;51:7752–7755.

12.Nagrath S, Sequist LV, Maheswaran S, Bell DW, Irimia D, Ulkus L, Smith MR, Kwak EL, Digumarthy S, Muzikansky A, Ryan P, Basil UJ, Tompkins RG, Haber DA, Toner M. Isolation of rare circulating tumour cells in cancer patients by microchip technology. Nature. 2007;450:1235.

13.Issadore D, Chung J, Shao H, Liong M, Ghazani AA, Castro CM, Weissleder R, Lee H. Ultrasensitive clinical enumeration of rare cells ex vivo using a micro-Hall detector. *Sci Transl Med.* 2012;4:141ra92.

14.Gao, W., Emaminejad, S., Nyein, H. Y. L., Challa, S., Chen, K., Peck, A., ... & Rogers, J. A. (2016). Fully integrated wearable sensors on soft contact lenses for continuous tear glucose monitoring. Nature medicine, 22(4), 386-392.

15.Wang, J., & Chen, K. (2022). Human identification chip: A review of the state-of-the-art. IEEE Access, 10, 107725-107739.

GROUP AND DIVISIONS

Sohom Mukherjee 22053722

I. Cover page
II. Introduction
III. Editing
IV. Highlighting points from sources
V. Keywords

Aditi Patel 22053656

I. Sensors and chips
II. Citations

Ashirbad Mohanty 22053497

I. Table of contents
II. RFID components

Subham Moharana 22053818

I. Experiments & results
II. References

Aiswarya Ayaskant 22053658

I. Conclusion
II. References