Easy Glass: Implementation of Optimized Glass Technology Using Integrated Finger-Print and Touch-Screen Sensors

Sukhwant Kaur[1], Dhruv Verma[2], Trishna Thrinath[3]

[1]Assistant Professor, School of Engineering and IT, Manipal University, G-04, Dubai Academic City, PO Box: 345050, Dubai, UAE

[2]Student, School of Engineering and IT, Manipal University, G-04, Dubai Academic City, PO Box: 345050, Dubai, UAE

[3]Student, School of Engineering and IT, Manipal University, G-04, Dubai Academic City, PO Box: 345050, Dubai, UAE

Abstract: ***Currently, Innovations and inventions are on a sprint to advancements by all aspects in the field of technology. To keep up with these advancements, great improvement in hardware and software design is necessary, more specifically, a better integration of the two. In today's world, where everything works on our fingertips, laptops, mobile phones, and similars are not a rare view. As per the statistics released by Forbes, there has been a drastic increase in the statistics that approximately quantifies the usage of electronic gadgets worldwide since 2000; and since then the graph has continued to grow. From the age of push-button gadgets, the shift to touch screen technology has been widely welcomed by the users regardless of age groups and initial adaptation concerns. It is no more a luxury created for corporate needs or style statements. We create an environment where thousands of information -mere details to highly confidential documents- are sent across networks, altered on personal devices and carried around in gadgets. But are we able to say that the information is 100% secure at its spot? Have we achieved an optimal design that syncs the hardware and software to guarantee a safer technological society? Can the existing techniques help us to implement and integrate a system which not only insulates security breach but also resists high levels of damage? These questions were an inspiration to the creation of our design that poses as a possible solution. It aims to create a product which embeds a fingerprint sensor into a touchscreen enabled glass and thus, eliminate the requirement of any external hardware for security, make it easier to use and cheaper to manufacture.***

Keywords: 3D Finger-Print Technology, Capacitive sensor, Gorilla Glass, Security, Optimization

1. Introduction

The tech world has seen the rise of various devices that now implements touch and fingerprint sensors in them like mobile phones, laptops, gaming devices etc. But we still are not sure that these advanced computing machines are completely isolated from external attacks. The security measures implemented at present, has a false rate ranging from 2%-20% depending upon the device, which, in fact, is a critically high value to risk.

Nevertheless, we must oblige the progress from easily breakable passcode or pattern system to a comparatively stronger security system that uses the concept of biometrics. Fingerprint sensors have always been incorporated into special hardware, only because of technological boundaries [1]. These sensors are activated with finger touch and the electric current that flows in the then made closed loop makes an imprint of the out layer of the finger and stores it into the device for future comparisons. Here, is where we can see the restriction build by technology that explains the lack of integration of the sensors. The electric wave used in the fingerprint sensors if adjoined with a touchscreen sensor, posed a threat of introducing various bugs and functionality issues. The 3D touch technology which uses sound waves to create highly detailed 3D image of the finger serves as backbone for this paper. Not only does this technology ensure more security, but also the sound waves do not interfere with other sensory devise places along with them, hence giving a possibility to integrate the sensors of a device.

Of course, the evolution of touch screen sensors was not through a smooth graph. Differentiating human touch from others was a challenge of its own during the use of the initial resistive sensors which was duely faced by the capacitive sensors- a technology which will be widely considered in the proposed design.

The display glass that held the sensors and various electrical components over the years have always been prone to damage or crack due to various acts of human carelessness or mistakes. A boon to technology was surely the invention of a stronger glass that could survive more falls or hits and still manage to live on. Conning's Gorilla Glass runs today as the world's strongest glass. As the creators, Conning's and Sonavation rightly argue it to be. This is a hardware that is accepted and widely implemented in all the latest products that rule the electronic market today. Our design too, takes aid of this creation.

For ultimate user experience, which guarantees security and resistance to damage, our design proposes to integrate the best of the above-mentioned hardware and software technologies so that they work as a single unit eliminating the need for separate hardware sections. The proper implementation of the design is expected to increase the security of a device by multiple folds. The paper progresses to detail the abstract product model named Easy Glass.

Our paper is organized as follows: Section 2 of the paper explains the working of the various technologies suggested for making of the product and the reasons for it. Section 3

DOI: 10.21275/ART2017588

guides us through the integration of technology that gave birth to our proposed technology. Lastly, section 4 compares the product with all existing similars and concludes why it is the best design among all of it.

2. Design

Our aim is to imbed fingerprint sensors along with touch screen sensors and attach the strongest glass to it. Such a design will ensure maximum protection and smooth usage of the device, not only eliminating the need for any additional external component, but also providing huge scopes of application in all possible technological fields.

As shown in Figure 1, the product can be observed by dividing it into three main modules: -

- Touch-Screen sensor
- Finger-Print sensor
- Glass

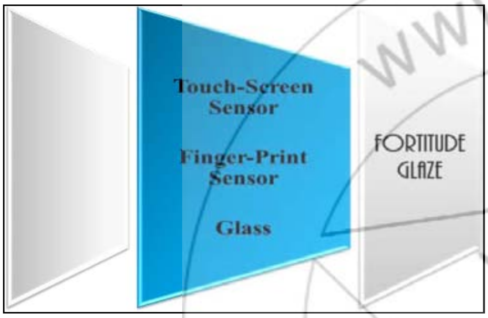

Figure 1: Design Overview

2.1 Touch-Screen Sensors

The touch-screen technology introduced two types of sensors for its working – resistive touch-screen and capacitive touch-screen. In this section, we see which one of the two would be an apt candidate for our product and introduce both.

2.1.1 Resistive Touch-Screen

Resistive touchscreen displays are composed of multiple layers that are separated by thin spaces. Pressure applied to the surface of the display by a finger or stylus causes the layers to touch one another, which completes electrical circuits and tells the device where the user is touching as shown in Figure 2 [4]. As such, resistive type touchscreens require much more pressure to activate than capacitive touchscreens. Examples of devices with resistive touchscreens are HTC Touch Diamond, Samsung SGH-i900, Omnia, etc.

Because of the continuous requirement to touch the screen with an added force, which can easily damage the screen, devices that use resistive touch-screens demand high care.

Resistive touch-screens respond to anything that touches it- it can be a pencil, a stylus or finger. This surely does not match the requirements of our product, hence we moved on to capacitive touch-screens expecting to meet requirements.

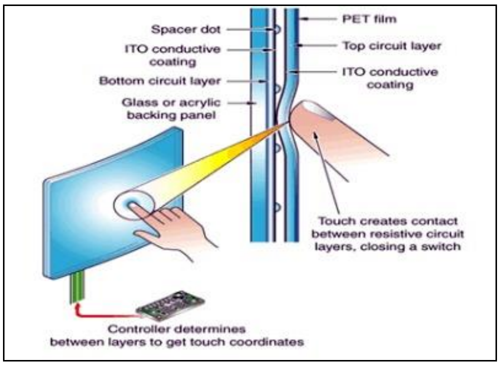
Spacer dot
ITO conductive coating
Bottom circuit layer
Glass or acrylic backing panel
PET film
Top circuit layer
ITO conductive coating
Touch creates contact between resistive circuit layers, closing a switch
Controller determines between layers to get touch coordinates

Figure 2: Working of Resistive Sensors

2.1.2 Capacitive Touch-Screen

Capacitive sensing is a technology, based on capacitive coupling, which takes human body capacitance as input. Capacitive sensors detect anything that is conductive or has a dielectric that is different from that of air. Hence capacitive touch-screens were designed based on this theory [5].

The working of these sensors relies on the electrical properties of the human body to detect when and where on a display the user touches as shown in Figure 3. This gave highly positive results, the first of them being that these displays can be controlled with very light touches of a finger. Consequently, a mechanical stylus or a gloved hand couldn’t activate the sensors. Examples of devices which implement capacitive touch-screens include Apple iPhone, T-Mobile G1, etc.

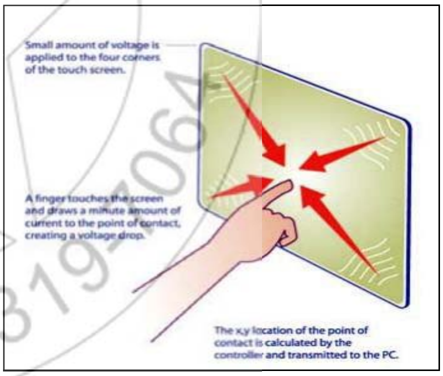
Small amount of voltage is applied to the four corners of the touch screen.
A finger touches the screen and draws a minute amount of current to the point of contact, creating a voltage drop.
The x,y location of the point of contact is calculated by the controller and transmitted to the PC.

Figure 3: Working of Capacitive Sensors

This technology completely satisfied the requirements of our product. Both types of touch-screen sensors have advantages and disadvantages: Resistive Sensors are cheaper, unstable and shock-prone whereas the latter is expensive, responsive and totally controllable.

From our observations, capacitive touch-screens would prove to be beneficial if included in the product design. Hence, capacitive sensors were selected.

2.2 Finger-Print Sensors

Fingerprint scanners earlier used to be large, but as the technology progressed, the size of the fingerprint scanners reduced to that much of a home button on a phone

DOI: 10.21275/ART2017588

Over the years, not only has the hardware improved, but the software and technology being used has also been improved on a huge scale. An evaluation conducted by National Research Council of Canada in 2008, stated that earlier fingerprint scanners had a false acceptance rate of up to 5% (which is very bad) [6].

Having finalized the touch screen sensors, the next task was to identify the perfect fingerprint sensor which will not affect the functioning of the touch screen sensors. While focusing on that point, we also had to make sure that the fingerprint sensors prove to be the most secure sensors ever since alongside functionality, security was a top priority.

Basic finger-print security systems functioned as depicted in Figure 4.

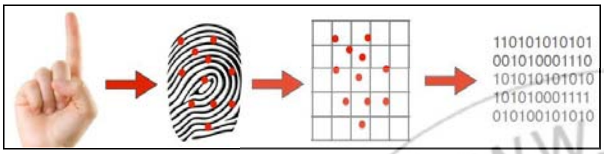

Figure 4: Functioning of basic finger-print security system

A finger-print scanner system has two basic jobs. Firstly, it needs to get an image of the user's finger, and secondly, it needs to determine whether the pattern of ridges and valleys in this image matches the pattern of ridges and valleys in pre-scanned images.

Only specific characteristics, which are unique to every finger-print, are filtered and saved as an encrypted biometric key or mathematical representation. The image of the finger-print is not saved, instead only a series of numbers (a binary code), which is used for verification is stored for future references. The algorithm cannot be reconverted to an image, so no one can duplicate your fingerprints.

During enrolment or verification, each print is analysed for very specific features called minutiae, where the lines in our fingerprint terminate or split in two. The computer measures the distances and angles between these features—a bit like drawing lines between them—and then uses an algorithm (mathematical process) to turn this information into a unique numeric code as shown in Figure 5. Comparing fingerprints is then simply a matter of comparing their unique codes. If the codes match, the prints match, and the person gains access.

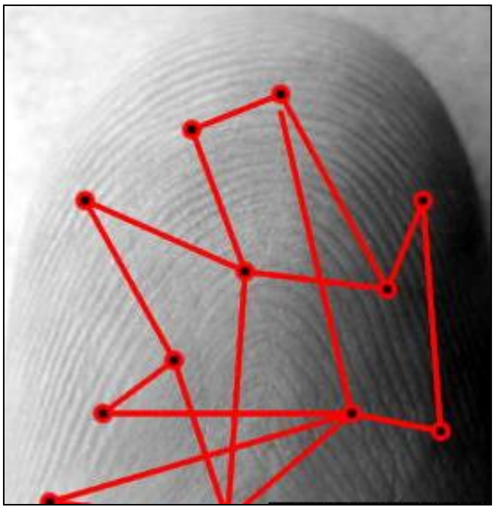

Figure 5: Pattern matching

We discuss three types of finger-print technology in our paper, namely, optical, capacitive and ultrasound finger-print technology in order to select the best technology for our product.

2.2.1 Optical Finger-Print Technology

The scanning process starts when we place our finger on a glass plate, and a charge-coupled device (CCD) camera takes a picture. The scanner has its own light source, typically an array of light-emitting diodes, to illuminate the ridges of the finger as shown in Figure 6. The CCD system generates an inverted image of the finger, with darker areas representing more reflected light (the ridges of the finger) and lighter areas representing less reflected light (the valleys between the ridges).Before comparing the print to stored data, the scanner processor makes sure the CCD has captured a clear image [7]. It checks the average pixel darkness, or the overall values in a small sample, and rejects the scan if the overall image is too dark or too light. If the image is rejected, the scanner adjusts the exposure time to let in light, and then tries the scan again. If the darkness level is adequate, the scanner system goes on to check the image definition (how sharp the fingerprint scan is). The processor looks at several straight lines moving horizontally and vertically across the image. If the fingerprint image has good definition, a line running perpendicular to the ridges will be made up of alternating sections of very dark pixels and very light pixels. If the processor finds that the image is crisp and properly exposed, it proceeds to comparing the captured fingerprint with fingerprints on file.

DOI: 10.21275/ART2017588

Figure 6: Optical Scanner

2.2.2 Capacitance Finger-Print Scanners or 2D Finger-Print Technology

Like optical scanners, capacitance fingerprint scanners generate an image of the ridges and valleys that make up a fingerprint. But instead of sensing the print using light, the capacitors use electrical current. Figure 7 shows the circuit design for a simple capacitance sensor. The sensor is made up of one or more semiconductor containing an array of tiny cells. Each cell includes two conductor plates, covered with an insulating layer. The cells are tiny -- smaller than the width of one ridge on a finger.

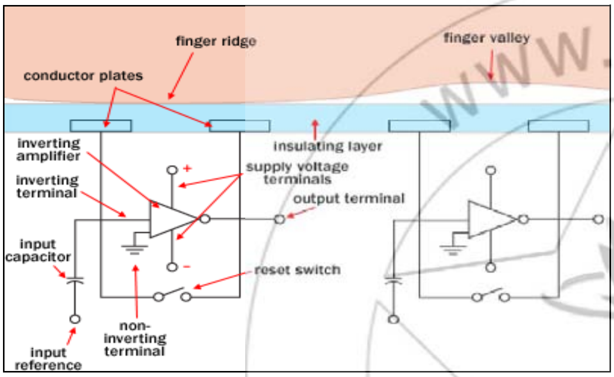

Figure 7: Capacitance Finger-Print Scanner

The sensor is connected to an ritegrator, an electrical circuit built around an nverting operational amplifier. The inverting amplifier is a complex semiconductor device, made up of several transistors, resistors and capacitors [9].

The two conductor plates form a basic capacitor, an electrical component that can store up charge. The surface of the finger acts as a third capacitor plate, separated by the insulating layers in the cell structure and, in the case of the fingerprint valleys, a pocket of air. Varying the distance between the capacitor plates (by moving the finger closer or farther away from the conducting plates) changes the total capacitance (ability to store charge) of the capacitor. Because of this quality, the capacitor in a cell under a ridge will have a greater capacitance than the capacitor in a cell under a valley.

To scan the finger, the processor first closes the reset switch for each cell, which shorts each amplifier's input and output to "balance" the integrator circuit. When the switch is opened again, and the processor applies a fixed charge to the integrator circuit, the capacitors charge up. The capacitance of the feedback loop's capacitor affects the voltage at the amplifier's input, which affects the amplifier's output. Since the distance to the finger alters capacitance, a finger ridge will result in a different voltage output than a finger valley.

The scanner processor reads this voltage output and determines whether it is characteristic of a ridge or a valley. By reading every cell in the sensor array, the processor can put together an overall picture of the fingerprint, like the image captured by an optical scanner.

The main advantage of a capacitance scanner is that it requires a real fingerprint-type shape, rather than the pattern of light and dark that makes up the visual impression of a fingerprint. This makes the system harder to trick. Additionally, since they use a semiconductor chip rather than a CCD unit, capacitive scanners tend to be more compact that optical devices. The pros of the scanner explain why most of the devices at present use the capacitance sensors at present.

2.2.3 Ultra-Sound Finger-Print Scanners or 3D Finger-Print Technology

This is a comparatively new technology that scans a fingerprint by releasing pulses of ultrasound that bounce off the fingertip's skin, creating an echo. It takes more time for sound waves to reflect off the valleys of a fingerprint versus its ridges, allowing the device to pinpoint and paint a picture of the crevices. However, some of the ultrasound waves also penetrate through the outer skin layer — the epidermis — reaching the inner layer called the dermis as shown in Figure 8.

When a user places his or her finger to the print-reading chip, an ultrasonic pulse bounces against it. The chip is coated with a layer of aluminium nitride, which can convert mechanical stress to electric energy or vice versa. When the ultrasonic pulse bounces back off the fingerprint, ridges and valleys return different patterns of stress, which can then be converted into electrical signals. By measuring the bounce from the ultrasound for longer period, the scanner can also sense the depth of the ridges and valleys [10].

As per scientist Dr Horsley, "It turns out that you have the same fingerprint on your dermis that you have on your epidermis". Hence, this deeper scanning mechanism can detect physical landmarks like sweat pores and blood vessels buried in that inner skin layer. The ultrasound sensor penetrates the outer layers of your skin to see inside the ridges and specific characteristics that make up your fingerprint as shown in Figure 9. It can even see the sides of the ridges as well as your skin's sweat pores in intimate detail [8].

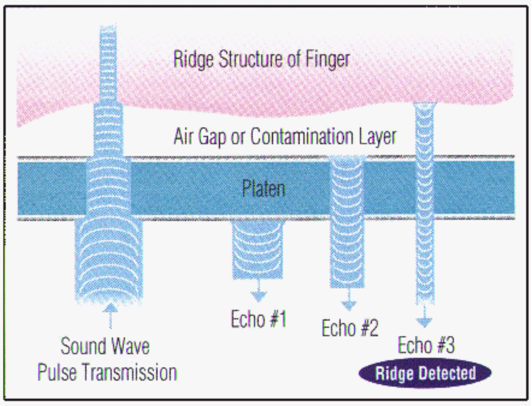

Figure 8: Working of Ultra-Sound Finger-Print Scanner

Since the ultrasound detects from deep into the skin, it can sense whether the fingerprint in use is attached to a living person. This is because it's possible that an attacker or hacker tries to gain access by placing the fingerprint that is caught on a tape or similars. The technology detects the motion of blood flow under the skin, alerting the software that the fingerprint is indeed real and a part of a living person. Neither glue molds nor hacked-off thumbs from gangster movies can fool this innovative sensor.

2.2.4 Consideration of Finger-Print Technology for our product

While choosing an apt finger-print scanner for our proposed design, the optical sensor was ruled out because of its high hardware requirement. Though the capacitance sensor was considered, on running tests of these sensors combined with the touch screen sensors, showed that, the electric pulses being passed by the capacitance fingerprint sensor were disrupting the functioning of the touchscreen sensors. Hence the capacitance sensors were also rejected.

Finally, we were left with the 3D or the ultrasound fingerprint sensors. These sensors turned out to be a complete and perfect package. The ultrasound technology did not disrupt or interrupt the functioning of the touch screen sensors. Alongside this fact, optical and capacitance sensors had failed to function properly in case of sweaty, dirty and oily fingertips. But, the ultrasound technology works perfectly in this condition as it penetrates the finger deeper. Also, the false acceptance rate of the Ultrasound fingerprint sensors is proved to be extremely low compared to the other technologies, which meant a significant rise in the security aspect. Hence, we decided to incorporate Ultrasound fingerprint sensors into Easy Glass.

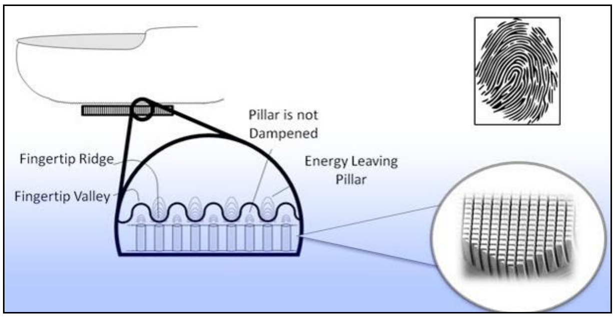

Figure 9: Ultra-Sound Finger-Print Scanner

2.3 Glass

After the touchscreen and fingerprint scanners were decided, we had to select the main hardware component - the glass. Mobile phones and other devices using a screen of some sort at present, have two options: a sapphire glass or a gorilla glass.

2.3.1 Sapphire Glass

Synthetic sapphire is generally made by applying incredibly high heat and pressure to aluminium oxide powder (sapphire is, after all, just a compound of aluminium and oxygen) [2]. Heat-treated to remove its internal stresses, which can cause weakness, and processed into sheets, this synthetic sapphire is referred to as sapphire glass similar to the model shown in Figure 10. And that's what is widely used on phones and other electronic devices.

Sapphire glass is highly transparent to wavelengths of light between 150 nanometres and 5500 nanometres. For context, the human eye can only discern wavelengths from about 380 nanometres to 750 nanometres. So it passes the first and most and important screen test i.e., you can see through it.

But the real charm of sapphire glass is its hardness. It's nearly twice as hard as standard glass, and nearly as hard as diamond. In practical terms, that means it's almost impossible to scratch, unless we happen to carry a bunch of diamonds in our pockets. It's not just hard, though, but strong, too: sapphire crystals have a compressive strength of 2,000 MPa, about ten times that of stainless steel.

Figure 10: Sapphire Glass

Sapphire glasses are used frequently for applications where optical transparency, high strength, and scratch-resistance are required. Shatter-resistant windows in armoured vehicles, bullet-proof glass, or screens and visors in military body armour suits are few places where these glasses are used besides in electronic devices.. But there are more mundane applications too: it's used in scientific experiments that need an optical window into harsh environments, and even at checkouts for the little glass windows that cover barcode readers to ensure the optics of the device aren't rendered useless by heavy scratching of normal glass.

2.3.2 Gorilla Glass

The manufacturing company Corning has developed a product called the Gorilla Glass. The company designed the glass for the new-gen electronic lifestyles.

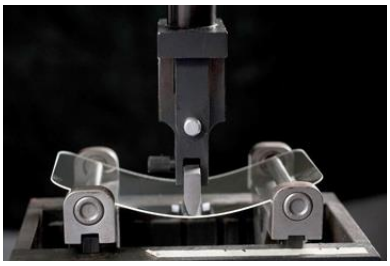

Figure 11: Flexibility test of Gorilla Glass

Corning takes the silicon dioxide (SiO2) and combines it with other chemicals before melting it down into a glass melt. The resulting glass is alum inosilicate -- that means the glass contains aluminium, silicon and oxygen [11]. The glass also contains sodium (Na) ions, which become important in the next phase of manufacturing.

Corning pours the molten glass into a V-shaped trough but doesn't stop at filling the trough to the top. The company continues to add molten glass until the glass begins to overflow the sides of the trough. Automated robotic arms draw the sheets of glass from the edge of the trough. Each sheet is just over half a millimetre thick.

If you were to use this glass for a screen on your electronic devices, you'd end up with a very clear covering. But it's not damage-resistant like Gorilla Glass -- it's just alum inosilicate glass. To give Gorilla Glass its ability to withstand scratches and cracks, Corning gives these sheets of glass a little bath, making the Gorilla Glass strong, flexible and scratch proof as shown in Figure11. Corning has already spoken about its newer Gorilla Glass 4. They argue that the newer glass 4 shall be 80% stronger than the glass 3, along with proportional increase in the flexible and scratch proof criteria. In an experiment, it was proven that the Gorilla Glass 4 is much stronger than the latest Sapphire Glass. The results are shown in Figure 12.

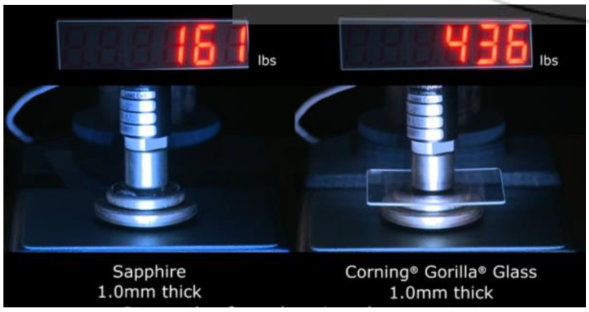

Figure 12: Strength test

Besides the strength test, we also looked at the fact that sapphire glass weighs 67% heavier than Gorilla Glass—with a density of 3.98 grams/cm^3 compared to the 2.54 g/cm^3. That means that to match it gram-for-gram, a screen made of sapphire would need to be rather thinner. That's great for our pockets, but just because it's hard and strong doesn't mean that it's unbreakable, and making it thinner makes it more vulnerable [13].

Hence, after complete analysis of both the type of glasses available in the market today and also on the basis of the above facts, we decided to propose the Corning Gorilla Glass 4 for our design.

3. Integrating Technology

Till date each device having a fingerprint scanner has been in the need of a special hardware component. Example: Fingerprint port in laptops, Home button in Apple, Return button in Samsung, Back button in LG etc. Our product is the embedding of fingerprint sensors and touch screen sensors working seamlessly together within a glass.

Figure 13: Sample Product that uses Easy Glass

Figure 13 shows us a probably Easy Glass product. This is a simulated iPhone without a home button fingerprint sensor, but with an embedded touch screen fingerprint sensor.

The following technologies have been finalized after a comprehensive literature review.

- Touch Screen sensors: Capacitive sensors
- Fingerprint sensors: 3D fingerprint technology or ultrasound fingerprint technology
- Glass: Corning Gorilla Glass 4

For these sensors to work together lag free, the product will require good processing power alongside with good RAM. Per calculations done by experts, processing chip should be dual core 64-bit architecture, clocking up to 1.8 GHz to run this technology perfectly and RAM should be of minimum 1 GB.

This sort of hardware specifications is seen in almost all devices in the market today. But the challenge here, was figuring out how to adjoin fingerprint sensors and touch screen sensors together so they don't interfere with each other's work so that our objective to create a product where both would work seamlessly together is achieved.

Figure 14 shows how the architecture that was designed by a leading firm, Sonavation, of the probable hardware assembly of Easy Glass can be imagined to be [12].

This could be implemented as an integrated circuit connected to a bottom surface of a cover sheet, near the bottom surface of the cover sheet, or connected to a top surface of a display as shown in Figure 15.

The same technology could be used to allow for a larger device like an iPad to scan multiple fingerprints at once, or even your palm print. This is possible because while the sensor technology can capture a specific point on the screen (such as an unlock button on the lock screen), it can also read fingerprints from any point on the touchscreen's surface.

Having the capability to read fingerprints from any point on the touch screen surface, this product has a huge scope.

Let's take a simple example to understand this. Like how root accounts work in Linux, imagine your phone would instantly get root privileges on your touch, and loose these privileges on someone else's touch.

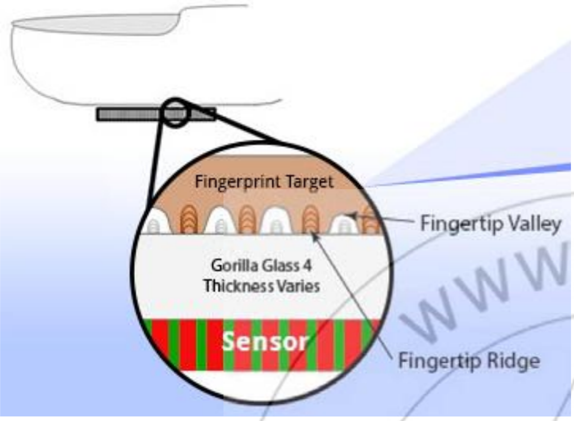

Figure 14: Proposed Architecture by Sonavation

This idea has unlimited applications. We would no longer need passwords or 3rd party apps to hide our content.

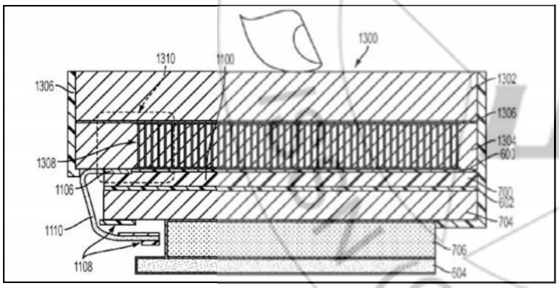

Figure 15: Working of integrated fingerprint and touchscreen sensor

4. Comparative Analysis

Table I: Comparison of the technologies

Technology	*Advantages*	*Disadvantages*
3D-Fingerprint	•Popular •Cheapest •Very accurate	• Unfamiliar
Voice	•Non invasive	• Least Accurate
Iris	•Very accurate	• Invasive • Expensive • Sensitive
Palm Vein	•Non-invasive •Relatively Cheap •Accurate	• Unfamiliar

In the earlier sections, we have explained the technologies selected for this product and about how we can integrate them all together. In this section, we compare the 3D Fingerprinting technology we have selected with other authentication technologies that is available in the market today. Table I shows us the comparison that is necessary to conclude that our selection of authentication method is accurate. It gives us a clear idea about the advantages and disadvantages of the various authentication methods. Clearly, we can conclude that 3D Fingerprint technology that we have chosen aces the comparison chart.

Table II: Comparison of the misidentification rates of the technologies

Technology	*Misidentification Rate*
3D-Fingerprint	1/12000000
Voice	1/30
Iris	1/1,200,000
Palm Vein	1/800000

To go ahead with the 3D Fingerprint technology we needed to be sure about one more very important attribute: misidentification rate [3]. Because the lesser is the misidentification rate of the selected technology, the higher is the security of the device. In Table II, we compare the misidentification rates of all the authentication technologies and conclude that 3D Fingerprint Technology has the least misidentification rate.

From the tables above, it's clear that 3D fingerprinting technology is not only the cheapest in the market, but also the most secure. This comparison becomes our trump card to conclude that Easy Glass promises to be the most secure product ever made.

5. Conclusions

The advancements in technology demand the creation of an improved security mechanism and hence we present this paper as a superior solution. Our aim is to create a technology that imbibes touch-screen and finger-print sensors within a glass that can withstand tough circumstances so that this component can be directly accommodated in any electronic device. Our design eliminates the need for any external device, chip or component while attaching to a device.

With a rigorous study, we could select the best component from each category. A comparative analysis of the proposed design and all the similar security mechanisms proved why Easy Glass stands out as a unique security device.

Upon implementation, this product would become the most secure, easy to use and physically-reliable. Along with a huge improvement in fail rates, Easy Glass promises to reduce production space and cost by almost half. Even while guaranteeing simplicity of use, Easy Glass shall bring the most advanced security protocols to electronic devices.

What Easy Glass after production is expected to give us is a perfectly responsive touch screen in the front, which has embedded touch and fingerprint sensors in its background, all working together as one piece of hardware, that is perfectly synced. This hardware will be unbreakable and will act as an insulator to security breach.

This idea of Easy Glass can be implemented in almost every area of our daily life. Cars, doors and so on the list would be long and its best to say, not just in mobile phones but Easy Glass can be used to add maximum security and protection in almost all IOT devices.

6. Acknowledgment

The creation of our design and this paper would have been impossible without the help and support of few. We would like to express our profound gratitude and deep regards to Prof Sukhwant Kaur for her unwavering encouragement, exemplary guidance, and constant support throughout the course of this thesis. We thank our dear family and friends for believing in us and supporting our ventures. Our achievements would be incomplete without their inspiring suggestions and advices. Last but not the least; we bow in gratitude to Him, who makes it all possible.

References

[1] Le Hoang Thai, Ha Nhat Tam, "Fingerprint recognition using standardized fingerprint model", International Journal of Computer Science, 7(3), 1694-0784.

[2] Andrew Wereszczak, Advances In Ceramic Armor II, John Wiley & Sons Inc, 2009.

[3] Desong Wang, Jianping Li, Gokhan Memik, "User identification based on finger-vein patterns for consumer electronics devices", IEEE Transactions on Consumer Electronics, 56(2), 0098-3063.

[4] Fia Stenmark, "Design of a touch screen interface for a mobile position aware instant messaging client", Master's thesis, Umea University, Sweden, 2008.

[5] Philip Irri, Julian Lindblad, "A Study of Ambient Light-Independent Multi-Touch Acquisition and Interaction Methods for In-Cell Optical Touchscreens", Master's Thesis, Chalmers University of Technology, Sweden, 2014.

[6] Gaurav Kalia, Gurshaan Sandhu, Aseem Kaushal, "Touch Screens: Technology for Better Tomorrow", International Journal of Electronic and Communication Technology,4(5), 2230-7109.

[7] Mudit Ratana Bhalla, Anand Vardhan Bhalla, "Comparative Study of Various Touchscreen Technologies, International Journal of Computer Applications", 6(8), 0975-8887.

[8] Kaoru Uchida, "Detection and Recognition Technologies-Fingerprint Identification", NEC Journal of Advanced Technology, 2(1), 2015.

[9] Seung Min Jung, "Design of Low Power and High Speed CMOS Fingerprint Sensor", International Journal of Bio-science and Bio-technology, 5(2), 2013.

[10] John. K. Schneider, Advances In Biometrics, Springer, London, 2008.

[11] Gorilla Glass, [Online]. Available: http://www.digitaltrends.com/mobile/sapphire-vs-gorilla-glass/

[12] Sonavation, [Online]. Available: http:// http://www.sonavation.com/

[13] Comparison of Glass, [Online]. Available: http://www.nature.com/news/ultrasound-fingerprint-security-1.17904

Author Profile

Ms. Sukhwant Kaur Sagar had her Bachelors in Computer Science and Engineering from Punjab Technical University, Jalandhar, Punjab in 1999. She completed her Master of Science in Software Systems from Birla Institute of Technology, Pilani, Rajasthan, in the year 2001. Currently, she is pursuing Ph.D at Salford Univeristy at Manchester, UK. She has 13 years of teaching experience. During her tenure of teaching, she was the coordinator of various Technical and Non-Technical events of the college. Ms. Sukhwant Kaur Sagar published 25 research papers in International Journals and International and National Conferences. She is the life member of Indian Society of Technical Education (ISTE, New Delhi) and International Association of Computer Science and Informational Technology (IACSIT, Singapore). She is also the life member of Computer Society of India (CSI, India). Currently Ms. Sukhwant Kaur Sagar is working as an Assistant Professor in the School of Engineering and IT, Manipal University, Dubai Campus. Her area of interest includes Image processing, Operating Systems, Computer Networks, Software Engineering and Data Structures and Algorithms.

Dhruv Verma completed BTech in Computer Science from Manipal University, Dubai. Currently, he is pursuing MS in Cybersecurity from Syracuse University, New York. His strength includes problem solving along with project management and software developing. Work experience includes internship at Torrid Networks as Cyber Security Analyst and On-Campus Job as Information Security Consultant at Syracuse University. Active member in IEEE and SAE

Trishna Thrinath is currently pursuing her MS in Cybersecurity at Syracuse University, New York. She is an active member in IEEE and SAE. Work experience includes internship at Torrid Networks as Cyber Security Analyst. Designing interface and problem solving along with software development includes her list of strengths. She completed her undergraduate in computer science from Manipal University, Dubai.