**AMITY UNIVERSITY UTTAR PRADESH**

**IN HOUSE PROJECT REPORT**

**ON**

**EXPLORING AND EXPERIMENTING WITH CYBERSECURITY, AI AND IOT**

Submitted To :

AMITY INSTITUTE OF ENGINEERING AND TECHNOLOGY

Amity University, Uttar Pradesh



By

Suparna Sarkar and Palak Gupta

(A2305318102 and A2305318092)

Under the guidance of

Dr. Purushottam Sharma

**DEPARTMENT OF INFORMATION TECHNOLOGY**

**AMITY SCHOOL OF ENGINEERING & TECHNOLOGY**

**AMITY UNIVERSITY UTTAR PRADESH**

**DECLARATION**

I,Suparna Sarkar and Palak Gupta of B.Tech IT(4IT-2(Y)) hereby declare that the project titled ‘**Exploring and Experimenting with Cybersecurity, AI and IoT’** submitted by us to the Department of Information Technology, **Amity School of Engineering and Technology**, Amity University Uttar Pradesh, Noida, in partial fulfilment of requirement for the award of degree of Bachelor of Technology in Information Technology, has not been previously formed the basis for the award of any degree, diploma or other similar title or recognition.

The Authors attest that permission has been obtained for the use of any copyrighted material appearing in the report other than brief excerpts requiring only proper acknowledgement in scholarly writing and all such use is acknowledged.

**SIGNATURE:\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

Suparna Sarkar, Palak Gupta

(A2305318102, A2305318092)

4IT-2(X)

**ASET,Noida**

**Date:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**CERTIFICATE**

This is to certify that Ms Suparna Sarkar and Ms Palak Gupta , students of B.Tech in Information Technology have carried out work presented in the In house project entitled “**Exploring and Experimenting with Cybersecurity, AI and IoT”** as a part of Second year program of Bachelor of Technology in Information Technology from Amity University, Uttar Pradesh, Noida under my supervision.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Dr. Purushottam Sharma

Department of IT

ASET,Noida

**ACKNOWLEDGEMENT**

The satisfaction that accompanies that the successful completion of any task would be incomplete without the mention of people whose ceaseless cooperation made it possible,whose constant guidance and encouragement crown all efforts with success . We would like to thank Dr. A. Sai. Sabitha, HOD-IT and Amity University for giving us the opportunity to undertake this project. We would like to thank our faculty guide Dr Purushottam Sharma who is the biggest driving force behind our successful completion of project. He has always been there to solve any query of our’s and also guide us in the right direction regarding the project. Without his help, We wouldn’t have been able to complete the project. We would also like to thank our batchmates who guided us , helped us and motivated at each step.

**TABLE OF CONTENTS**

|  |  |  |
| --- | --- | --- |
| S.NO | TOPIC NAME | Page no. |
| \* | Abstract |  |
| 1 | Introduction | 7-10 |
| 2 | Cyber attacks and vulnerabilities | 11 |
| 3 | Various systems at risk | 12-13 |
| 4 | Security measures | 14 |
| 5 | Proposed design of the system | 15-16 |
| 6 | Methodology | 17-18 |
| 7 | Implementation | 19 |
| 8 | Future scope | 20-22 |
| 9 | Advantages | 23 |
| 10 | Conclusion | 24 |
| 11 | References | 25 |
| 12 | Plagiriasm report | 26 |

**ABSTRACT**

In today’s domain , a lot of data is generated each and every second. From storing small files and pictures on our mobile devices to storing greater amount of big data on much larger computers. The computer devices have become a very fundamental part of our day to day lives. The data stored in any form can be private and highly confidential to individuals/institutions/organizations, and so it needs to be properly and aptly secured. Here comes the need of Cybersecurity through Internet of Things, which is the main focus of this project. Due to the heavy reliance on our computer systems, the field of Computer Security /Cybersecurity is becoming more and more important. The growth of the ‘smart’ devices like the smartphones, laptops and televisions etc. do require constant advancements and innovations in IT security to keep pace with the everchanging technologies and tackle all possible threats to these devices . This project aims to innovate some application that can further add to the existing security systems and also make innovative and life changing advancements in the field of tech to improve and alleviate our day to day lifestyle . Since our smartphones and laptops are two of the most widely used computer devices that we use almost every day, an effort to make our laptop secure and more accessible from faraway distances for essential information and data even if its not physically present with us , with the use of the smartphone is the main idea behind this project . We as millennials are stuck to our smartphones all the times due to the ease of the access and applications it provides and how an integrated part of our life it is. So this project’s primary concern is to build an a security system that can be controlled from our smartphone to unlock other password protected devices such as the laptop.

1. **Introduction**

**1.1 What is Cybersecurity ?**

Computer Security/IT Security or more commonly known as Cybersecurity is the protection of computer devices/systems from the theft of data stored in it or damage to their hardware, software as well as guarding the services provided by the system from disruption or misdirection. The field of Cybersecurity is becoming important day by day due to the increased reliance on computer systems . Due to the growing complexities and various threats to the computer systems, it is also one of the major challenges in the contemporary world .Cybersecurity risk is increasing due to much better global connectivity and usage of various cloud services like Amazon web services . The chance of any organization/individual to suffer from a successful cyber-attack or any data breach is high due to poor configuration of cloud services along with increasingly sophisticated cyber criminals . Hence, the importance of cybersecurity is on the rise. Our society is technologically more reliant than ever before and there is no sign that this trend will slow down . Gone are the days of simple firewalls and antivirus software being the sole security measures . The ‘generation y’ as we call ourselves should be self-reliant enough to protect the sensitive data that is stored in the systems . Cybersecurity is often only associated with computers, however, it extends to other devices and technologies such as mobiles, televisions, cars, cameras, machinery and more . Therefore, this project will concentrate on making a simple security system using two of the most used devices in our everyday life i.e. the laptop and the smartphone .The basic idea is to take an input authentication from the user on a smartphone by the means of fingerprint/face detection or a numerical password which will control the locking-unlocking process of a laptop . In simpler words, the smartphone can be used as a handy gadget to unlock the laptop. But then what is the use of this system when we can already set passwords on our laptop , right ? The answer to this question lies in the fact that smartphones have become a very essential part of our day to day life , we almost desire to do all possible activities through our handy mobile sets, so wouldn’t it be great if we could just control our laptop with as much ease. Also , think of a hypothetical situation where somebody might have cracked a person’s laptop’s password, the data can be easily stolen from the device then. In that case, such a security system will be very useful to keep the person’s laptop secure Therefore, this project is an effort to create at least a prototype of the security system as explained above.

**1.2 What is Artificial Intelligence ?**

Only introducing the topic briefly since the system created is just the initial prototype of the advance uses of the application, we can describe AI as the ability of computer program or machine to think and act on its own and learn . It emphasises on the creation of intelligent machines that work and react like human beings.

* + 1. **Reactive machines**

The most fundamental kinds of AI frameworks are absolutely receptive, and have the capacity neither to shape recollections nor to use past encounters to educate current choices. This is the principal unmistakable hover of AI that indicated the term 'carpe diem'. All frameworks and machines depend on this sort of AI and hold an idea that the past information can anticipate what's to come. Dark Blue, the celebrated supercomputer created by IBM that won against Gary Kasparov in chess is a sweet case of this. The framework didn't have the foggiest idea what to look like at the master plan of chess piece penances nor key reasoning aptitudes. All it knew was picking the most fitting one from the rundown of accessible moves accessible relying upon the board. You could state such frameworks are once in a while like us in an eatery yet not eager.

**1.2.2 Limited memory**

This Type II class contains machines can investigate the past. Self-driving vehicles do a portion of this as of now. For instance, they watch other vehicles' speed and bearing. As the name itself proposes, the memory assigned in these frameworks is fleeting. These frameworks can return to the past for a brief timeframe and gain from it.

**1.2.3 Theory of mind**

We may stop here, and consider this point the significant gap between the machines we have and the machines we will work later on. In any case, it is smarter to be increasingly explicit to talk about the kinds of portrayals machines need to shape, and what they should be about. This sort depends on the way that best in class frameworks can see the idea of feelings and individuals and help to change their conduct separately. This idea is flawlessly consolidated in self-driving vehicles, where the sensors recognize occasions of a passer-by going across, terrible street conditions, climate, approaching vehicle, path recognition, traffic lights and more to settle on more astute driving choices. This innovation has been key in helping independent vehicles eager mishaps.

**1.2.4 Self-awareness**

The last advance of AI improvement is to manufacture frameworks that can shape portrayals about themselves. At last, we AI scientists won't just get awareness, however assemble machines that have it. While it is anything but difficult to banter on whether as people we have achieved mindfulness, this kind of man-made reasoning is as yet a likelihood and has the potential for genuine application. In this kind of computerized reasoning, machines or robots know about what their identity is, comprehend their inner qualities, states and conditions and even see human feelings. Mindful man-made consciousness is an augmentation of the Theory of Mind class of man-made reasoning. Speculatively, on the off chance that you are in a cinema and you cut the line a mindful robot is standing, you could drive the person in question mad and respond.

**1.3 What is Internet of Things ?**

"The Internet of Things (IoT) is an arrangement of interrelated registering gadgets, mechanical and advanced machines, items, creatures or individuals that are given one of a kind identifiers and the capacity to move information over a system without expecting human-to-human or human-to-PC collaboration."IoT is essentially the system of interconnected things/gadgets which are installed with sensors, programming, organize network and important hardware that empowers them to gather and trade information making them responsive.

An IoT system consists of sensors/devices which “talk” to the cloud through some kind of connectivity.

Once the data gets to the cloud, software processes it and then might decide to perform an action, such as sending an alert or automatically adjusting the sensors/devices without the need for the user.IoT gadgets can be utilized to screen and control the mechanical, electrical and electronic frameworks utilized in different kinds of structures (e.g., open and private, modern, establishments, or private) in home computerization and building robotization frameworks.

Since we have had a look at the proper definition and have a brief idea about internet of things , the system is more easy to explain . The prototype is an excellent example and infusion of all the three, since it has the technology and manifestation of internet of things , recognition and intelligence of artificial intelligence and security against many vulnerabilities of cybercrimes.

The application is most user friendly , easily accessible with a well-defined infrastructure which is easy to comprehend.

**2.Cyber attacks and vulnerabilities**

A cybersecurity system is created to tackle and protect the computer systems and networks from possible threats and vulnerabilities. A vulnerability may be defined as a weakness in design, implementation , operation or internal control of the system. To protect a computer system and make it secure , it is important to understand the attacks that can be made against it .Following are a few of such threats :

**2.1 Backdoor**

A Backdoor in a computer system/algorithm is any secret method of bypassing normal authentication/security controls . Sometimes these are added by an authorized party to allow some legitimate access or maybe by an attacker for some malicious purpose . These are generally very hard to detect.

**2.2 Eavesdropping**

It is the act of secretly listening to a private computer conversation, typically between hosts on a computer network. These systems are used by the FBI and NASA to eavesdrop on the systems of internet service providers.

**2.3 Phishing**

It is the attempt to acquire sensitive information such as usernames , passwords and credit card details directly from users by deceiving them.

**2.4 Spoofing**

It is the act of masquerading as a valid entity through falsification of data in order to gain access to information that one is otherwise unauthorized to obtain.

**2.5 Tampering**

Tampering is defined as the malicious alteration or modification of data.

**3. Various Systems at risk**

The substantial growth in the number of computer systems and also the constant reliance upon these systems by individuals, organizations, industries and governments means that there are increasing number of systems at risk.

**3.1 Personal Gadgets/Consumer Devices**

Almost everybody in the 21st century owns personal computer devices such as smart phones, smart TVs, smart watches and laptops, desktops and so on. These devices are at risk since there can be anyone out there who might try to gain some benefit by intruding into the private data stored in these computer devices.

**3.2 IOT Devices**

 IOT is a network of various physical objects comprising of many devices, vehicles, and maybe buildings sometimes which are [embedded](https://en.wikipedia.org/wiki/Embedded_system) with [electronics](https://en.wikipedia.org/wiki/Electronics), [software](https://en.wikipedia.org/wiki/Software), [sensors](https://en.wikipedia.org/wiki/Sensor), and [network connectivity](https://en.wikipedia.org/wiki/Internet_access) that enables them to collect and exchange data. This is a widely used technology in today’s world and so is prone to modern day threats.

**3.3 Financial Systems**

The computer systems of financial institutions are a prominent target for cybercriminals . The attackers maybe interested in manipulating the market or to earn some illicit gains. Web sites and apps that accept or store [credit card numbers](https://en.wikipedia.org/wiki/Credit_card_number), brokerage accounts, and [bank account](https://en.wikipedia.org/wiki/Bank_account) information are also prominent hacking targets.

**3.4 Large Corporations**

Large corporations are common targets. In many cases attacks are aimed at financial gains through identity theft involving [data breaches](https://en.wikipedia.org/wiki/Data_breach).

**3.5 Government**

Government and [military](https://en.wikipedia.org/wiki/Military) computer systems are often attacked by activists and foreign powers. Local and regional government infrastructure such as [traffic light](https://en.wikipedia.org/wiki/Traffic_light) controls, police and intelligence agency communications, [personnel records](https://en.wikipedia.org/wiki/Office_of_Personnel_Management_data_breach), student records and financial systems are also potential targets as they are now all largely computerized and digitized.

**3.6 Medical Systems**

These days even the medical systems are being attacked and hacked to gain crucial information for example maybe a patient’s medical history or data breaches of sensitive data stored in hospital servers.

**3.7 Aviation**

The [aviation](https://en.wikipedia.org/wiki/Aviation) industry is much reliant on a series of complex systems that are prone to get attacked.. .Maybe asimple power outage at one airport might cause worldwide repercussions. There is also some potential for attack from within an aircraft.

**4. Security Measures**

Following are some of the security controls and measures:

4.1.Access control

4.2.Antivirus software

4.3.Anti-spyware

4.4.Anti-malware

4.5.Anti-theft

4.6.Firewall

4.7.Parental Control

4.8.Security information management

4.9.Anti tamper software

4.10.Intrusion prevention system

4.11.Intrusion detection system

**5.Proposed design of the system**

This project aims on creating an application which primarily focuses on accessing and unlocking various devices through the security of smartphones. The main idea of the application is to unlock devices and gadgets via mobile phones , which means to install a created application which is capable of providing numerous security unlock options to choose from , such as face identification unlock , fingerprint unlock and moving onto the evergreen and most versatile for any lower end to higher end models with passcode unlock and pattern unlock. The user would be able to choose from these above mentioned options and also has the liberty to apply more than two security locks. The application will further open up to a listings of the devices or places or things they respectively want to unlock and extract information. The similar application or hardware setup will be installed on the devices chosen to be unlocked , which will indeed help the operator to unlock the selected device even from a far distance , without accessing it physically, operator can retrieve information and data without touching the desired device with full security within the operators hands . The proposed system shall make use of this feature to take authorization from the user on the smartphone to unlock the other computer device, which is the laptop .Wi-fi technology is supposed to be used here to connect the devices in a LAN.

A picture containing drawing

Description automatically generated

Figure 1 wi-fi

A close up of a cell phone

Description automatically generatedA person taking a selfie

Description automatically generated

Fig.2 Passcode unlocking Fig. 3 Face recognition

A close up of a logo

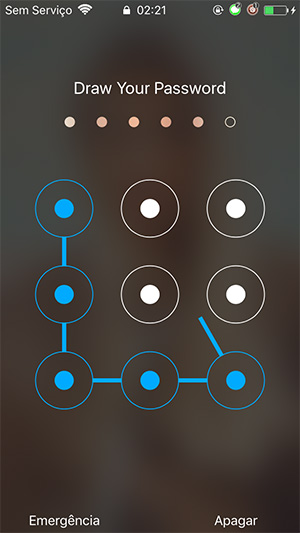
Description automatically generated

Fig.4 Fingerprint detection Fig.5 Pattern unlock

**6.Methodology**

**6.1 Android Studio**

Android studio a powerful, yet easy to use software for android application development. This tool can manage and create almost every type of feature you want to implement in your project/App and the software also packs GitHub support which is used to implement different types of API’s available on the GitHub library by the different developers. Also android studio packs the support of firebase in it, which is used to implement a real-time database in your project according to your requirements. You can always use short lines of codes to implement something in your application. Also you can see the real-time errors on writing the code side by side. For example: - if you make a mistake while writing a code in XML then it will show you the error of different types.

**6.2 Firebase**

Firebase is also the service provided by the google to implement the backend support to your application. It helps to you with the different types of features available on it which are very much useful in modern day application. For example: -

**6.2.1. Firebase Authentication**: It is a feature of firebase which takes care of that client is only using the code which is meant for them not the server side code. It also allows user to login through different famous platforms available out there. It also ensures that user registers with and email and UID provided randomly through authentication

**6.2.2**. **Firebase Real-Time Database:** It gives a database to your application to keep a track of all your users and what they do in that application. It also provides all kind of codes to imply in your application of all there features available on their documentation page. It also packs the support of all kind of languages available out there. It provides the real-time updates to the user. For example: - you can provide the online and typing status to the user. Also the database works in backend and you don’t have to worry about the rules as they are defined in the full protection of the code, so that no one can access the other user’s data, just by finding a loop hole. You can also access this database anywhere you want as you can create this just by logging into yours google account.

**6.2.3 Firebase Storage: -** It is used to store all kind of images and files that are used in your application. It also provides secure downloads of every type of file present on the application to the user.

For example: - if user uploads a profile picture in the social media application, then it will directly stores in the storage folder which is provided by you in the code.

**6.3 Java**

This language is mostly used in application building which packs a lot of features includes click listener and action listener as well, it is also preferred by many of the companies.

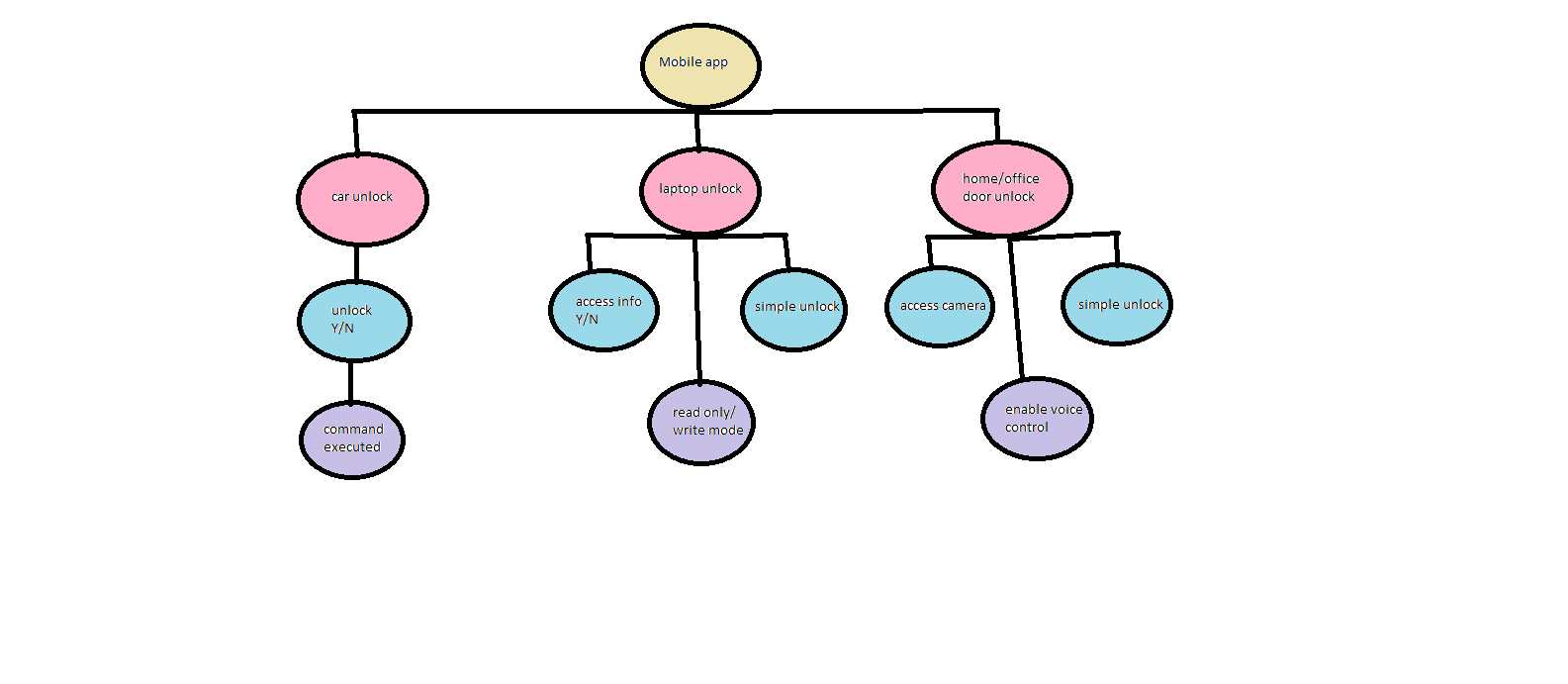
A screenshot of a cell phone

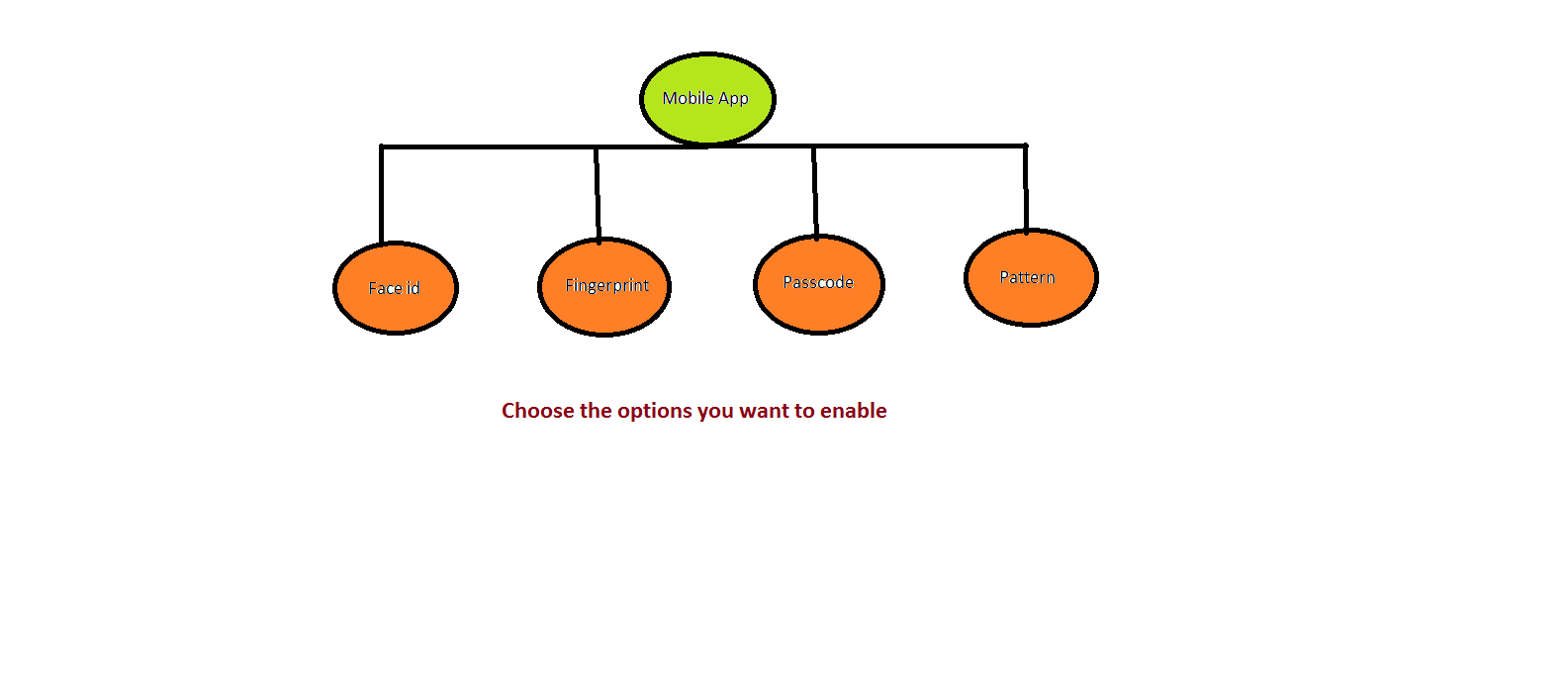
Description automatically generated

Android Operating system which is part of our phones is also written in this language. And because of that this language has the power to create android level applications which also support phone physical components, such as camera and finger print scanner.

This language can not only work in android but also to program any kind of applications for any type of machine others than IOS applications.

**7.IMPLEMENTATION**

****

****

**8.Future Scope**

The future scope of the project includes amplifying the security aspect of the application and making it more user friendly and providing many more advantages within one application such as:

**8.1.For home locks** : If we choose the option of unlocking the home doors , specially the entrance gate , a future application allows us to look at the person who has arrived outside the door, without his/her prior knowledge. This feature is so advanced and useful as the culprit wouldn’t be aware of being watched and the victim can keep their eye within the safe boundaries of their home.

A plant in a glass door

Description automatically generated

Figure 6 Home door unlocking

**8.2 For physically challenged** : If the operator is physically challenged he/she has the benefits of not only unlocking the device , but also accessing only the most critical and confidential information from their personal computers, just with the touch of a button in their handsets, they don’t have to move anywhere or grant access to others of their passwords and other information .

A picture containing toy, man

Description automatically generated

Figure 7 Physically Challenged

**8.3 Car door unlocking** : In the near upcoming , this application will also be competent for unlocking and locking the cars doors without touching them. As we are aware of the infamous COVID-19 pandemic, it would be a great feature to have sinceit would exempt the use of touching the door handles , and also would have the same camera feature as mention in point (2).

A car parked on the side of a road

Description automatically generated

Figure 8 Car door unlocking

The application now designed is just a future prototype for many such applications. Which covers the grounds of cyber security , artificial intelligence and internet of things. This application is quite vast in the fields of its expandability and can be diversified into may more such expedient features .

Its one of a kind initiative hasn’t been found or made anywhere yet.

**9.ADVANTAGES**

The advantages of the proposed system are as follows :

9.1.The security system provides the ease of controlling various devices from our smartphones.

9.2.No physical contact is required by the operator to give authorization to the other device.

9.3.It is versatile system and can be further modified agaianst high security breeches.

9.4.It has multiple unlocking and security options to choose from.

9.5.Two or more unlocking options are available to the operator at the same time.

9.6..The system can be further improvised to accommodate more features beyond locking/unlocking like to control other devices such as a home safe used to keep valuables.

**10.CONCLUSION**

The aim of this project was to innovate a security system using the smartphone and the laptop.Our project is majorly an application of three main technologies : AI, IoT and Cybersecurity.A protopype of the proposed system has been achieved wherein the smartphone is the handheld device to control the other device,which is the laptop. The world today is heavily suffering from the Covid-19 pandemic; and in this age this no touch device is an effort to innovate something for the betterment of the society.The system we have accomplished here is just a small part of the cake. It can be further extended to achieve many meaningful purposes such as the locking/unlocking of car doors,everyday security appliaces,helping the physically challenged and so on.

**11.References**

1.Singer, Peter W., and Allan Friedman. *Cybersecurity: What everyone needs to know*. oup usa, 2014.

2.Geers, Kenneth. *Strategic cyber security*. Kenneth Geers, 2011.

3.Nilsson, Nils J. *Principles of artificial intelligence*. Morgan Kaufmann, 2014.

4.Russell, Stuart, and Peter Norvig. "Artificial intelligence: a modern approach." (2002).

5.Tan, Lu, and Neng Wang. "Future internet: The internet of things." In *2010 3rd international conference on advanced computer theory and engineering (ICACTE)*, vol. 5, pp. V5-376. IEEE, 2010.

6.Stojkoska, Biljana L. Risteska, and Kire V. Trivodaliev. "A review of Internet of Things for smart home: Challenges and solutions." *Journal of Cleaner Production* 140 (2017): 1454-1464.

7.Liu, Yehui. "Study on smart home system based on internet of things technology." In *Informatics and Management Science IV*, pp. 73-81. Springer, London, 2013.

8.Lu, Yang, and Li Da Xu. "Internet of things (iot) cybersecurity research: A review of current research topics." *IEEE Internet of Things Journal* 6, no. 2 (2018): 2103-2115.

9.Boeckl, Katie, Katie Boeckl, Michael Fagan, William Fisher, Naomi Lefkovitz, Katerina N. Megas, Ellen Nadeau, Danna Gabel O'Rourke, Ben Piccarreta, and Karen Scarfone. *Considerations for managing Internet of Things (IoT) cybersecurity and privacy risks*. US Department of Commerce, National Institute of Standards and Technology, 2019.

10.<https://en.wikipedia.org/wiki/Computer_security>

11.<https://en.wikipedia.org/wiki/Artificial_intelligence>

12.<https://en.wikipedia.org/wiki/Internet_of_things>

**12.PLAGIARISM REPORT**

