iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 12 **Issue:** IV **Month of publication:** April 2024

DOI: https://doi.org/10.22214/ijraset.2024.59940

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 12 Issue IV Apr 2024- Available at www.ijraset.com

Android Pattern Bypass using Microcontroller

Reddyvari Venkateswara Reddy[1], V Gayathri[2], P Sai Charan Reddy[3], S Raj Kumar[4]
[1]*Associate Professor,* [2,3,4]*Student, Department of CSE (Cyber Security), CMR College of Engineering & Technology, Hyderabad, Telangana, India*

Abstract: ***The goal is to exploit a potential security vulnerability in Android devices by using a microcontroller which goes by the name ATTiny85 connected via USB. The objective is to bypass the lock patterns or security measures typically in place on Android devices, which are designed to prevent unauthorized access. This could involve manipulating the USB connection to take control of the device's data or functions, potentially compromising the device's security. Such actions are unethical and illegal without proper authorization. It's really important to acknowledge the amount of loss these attacks incur. The primary aim is to capitalize on a potential security vulnerability inherent in Android devices through the utility provided by microcontroller. This strategy is devised to circumvent the established lock patterns and security protocols usually implemented on Android devices, serving as a deterrent against unauthorized access. This approach may entail manipulating the USB connection to infiltrate the device's data or functionalities, posing a significant threat. It is crucial to emphasize that engaging in such activities is not only unethical but also illegal without explicit authorization. This underscores the paramount importance of upholding robust security measures on Android devices to proactively thwart any attempts at exploitation.***
Keywords: Usage, Vulnerability, ATTiny85 Microcontroller, Bypass, USB Cable, Lockout mode.

I. INTRODUCTION

We occasionally face situations like forgetting the passcode/pattern of certain files, folders and to access the file, we can implement USB based attacks using rubber duck and trying to brute force the device to match the correct passcode using the data we provided to the device. We have to inject the program to perform brute force on the device such that t can be accessed.

The increasing ubiquity of Android devices in contemporary society has prompted a growing body of research into their security mechanisms, with particular attention paid to authentication methods such as pattern locks. There are situations where we forget our device passwords which may have useful or critical information. This project can be used to bypass device passwords using the ATtiny85 is a small 8-bit microcontroller from the AVR family and can be used for a variety of applications The ATtiny85 is commonly used in embedded systems for a wide variety of applications, including sensor interfacing, data logging, and control systems. Due to its low power consumption, the ATtiny85 is suitable for battery-powered and energy-efficient devices such as remote sensors and wearable technology. It can be used in IoT devices to connect sensors and actuators to the Internet, enabling data collection.

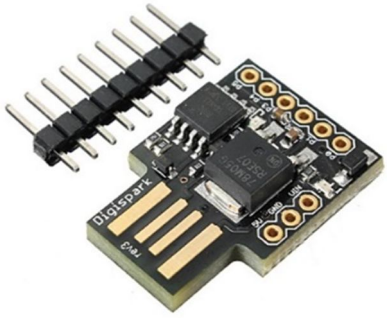


Fig.1.ATTiny85

©IJRASET: All Rights are Reserved

The ATtiny85 is part of Atmel's ATtiny series of microcontrollers, which are known for their compact size and low power consumption. With only 8 kilobytes of programmable flash memory, it might seem limited compared to larger microcontrollers, but its small form factor makes it perfect for projects where space is at a premium.

Its low power consumption makes it ideal for battery-powered devices or applications where energy efficiency is critical. This, combined with its small size, makes it popular in wearable electronics, sensor nodes, and small gadgets where minimizing power usage and physical footprint are important considerations. Despite its small size, the ATtiny85 still packs a punch with features like PWM (pulse-width modulation) for controlling motors or LEDs, multiple GPIO (general-purpose input/output) pins for interfacing with sensors or other components, and the ability to communicate with other devices using protocols like I2C or SPI. Its affordability and ease of use also contribute to its popularity among hobbyists and makers who are looking for a versatile microcontroller for their projects. Overall, the ATtiny85's combination of size, power efficiency, and features makes it a go-to choice for a wide range of applications.

II. LITERATURE SURVEY

Naveen Kumar T, Nikil V, Sabarish S and Ms. P. Charanya M.E has done research on bypassing Android mode, focusing on using brute force to try all possible password combinations. Brute force attacks involve a trial and error approach, trying every possible character combination until the right one is found. In the context of Android pattern lock, this means trying everything possible until the device gets unlocked. This research will involve the development of algorithms that can perform similar experiments, including features such as length, complexity, and constraints to create eight good bypasses.

This research is important in the cybersecurity industry because it shows flaws in security systems such as Android pattern lock. By showing that it is possible to bypass this process with brute force, the researchers highlight weaknesses that manufacturers and software developers need to address to improve the security of their products. Additionally, this study highlights the importance of educating users to choose strong and unique passwords or patterns.

Research conducted by Mohamed Fezari et al. on the Attiny85 microcontroller sheds light on its capabilities and applications. Here is a breakdown of the key features and functions discussed in their research:

1) *Attiny85 Microcontroller:* Attiny85 is an 8-bit AVR microcontroller manufactured by Microchip. Being an 8-bit microcontroller means that it processes data in 8-bit blocks, making it suitable for handling simpler tasks and applications. AVR is a family of microcontrollers developed by Atmel, now part of Microchip Technology.
2) *RISC CPU Architecture:* Attiny85 is based on RISC (Reduced Instruction Set Computing) architecture. RISC architectures typically simplify the instruction set to optimize performance, making them effective for tasks requiring fast execution of simple instructions.
3) *Low Power Controller:* Attiny85 is categorized as a low power controller. This designation means that it is designed to operate efficiently under low-power conditions, making it suitable for battery-powered or energy-saving applications where power consumption is a critical consideration.
4) *8-Pin Interface (PDIP):* The Attiny85 comes in an 8-pin package format known as PDIP (Plastic Dual In-line Package). This compact shape is suitable for applications with limited space or where miniaturization is required.
5) *Programmable Watchdog Timer:* The microcontroller includes a programmable watchdog timer function. A watchdog timer is a mechanism used to monitor system operation and reset it if it fails to respond within a predefined time frame.
6) *10-bit ADC converter:* The Attiny85 is equipped with a 10-bit analog-to-digital converter (ADC). This feature allows the microcontroller to convert analog signals from external sensors or devices into digital data that can then be processed or used for decision making within the microcontroller. The availability of an ADC makes the Attiny85 suitable for a wide range of sensor interface applications, allowing it to collect data from the environment and respond accordingly.
7) *Suitability for sensor interfacing and error handling:* The combination of features such as ADC and programmable watchdog timer makes the Attiny85 very suitable for sensor interface applications. It can acquire data from various sensors, process it using its computing capabilities and react accordingly. In addition, the watchdog timer provides an error handling mechanism, allowing the microcontroller to detect and recover from errors such as being stuck in an infinite loop.

Overall, the research conducted by Mohamed Fezari et al. highlights the versatility and suitability of the Attiny85 microcontroller for a wide variety of low-power embedded applications, particularly those involving sensor interfacing and error handling.

III. PROBLEM DEFINITION

USB-based attack tools like Rubber Ducky can bypass security measures in cases where someone has forgotten the password or access mode to some files or folders.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

Rubber Ducky is a versatile tool that acts as a keyboard to quickly enter commands, allowing a computer or device to operate when connected via USB.A USB-based brute force attack can extort a password or pattern, the attacker must first access the device physically. They will then connect the pre-prepared rubber duck to the device with a script designed to make different passwords or combinations. This script essentially automates the process of trying to unlock the device using brute force methods.

The success of such attacks depends on many factors, including the complexity of the password or pattern, the security measures set by the operating system, and the speed with which the rubber ducky can penetrate. order. In this case, trying to bypass security measures without legal permission would be illegal and unethical. Although USB-based attacks using tools such as Rubber Ducky could theoretically bypass passwords or patterns. Additionally, using strong, easy-to-remember passwords or patterns and using other security measures such as encryption and multi-factor authentication will help reduce the risk of unauthorized access to sensitive files and folders.

IV. OBJECTIVE

The outlined objective involves bypassing the lock patterns or security measures implemented on Android devices to gain unauthorized access to the device's data or functions. This goal implies the intention to bypass mechanisms specifically designed to protect data and device functions, such as lock screen patterns, PIN codes, or biometric authentication methods.

One common method used to achieve this is to manipulate the USB connection using an ATTiny85 microcontroller. The ATTiny85 microcontroller is a small, programmable device that can be used to emulate human input, such as keystrokes or touch screen gestures, when connected to a device via USB.

V. METHODOLOGY

A. Arduino Software Installation

Arduino IDE can be downloaded from Arduino website. Follow the on-screen instructions and download the software and complete the installer. After installation, connect the Arduino board to your computer using a USB cable. Open the Arduino IDE, select your specific board under Devices, and then select the correct port from the same menu. After connecting and installing the Arduino board, open the drawing example from the menu in the Arduino IDE. Click "Upload" to transfer the sketch to your Arduino board.

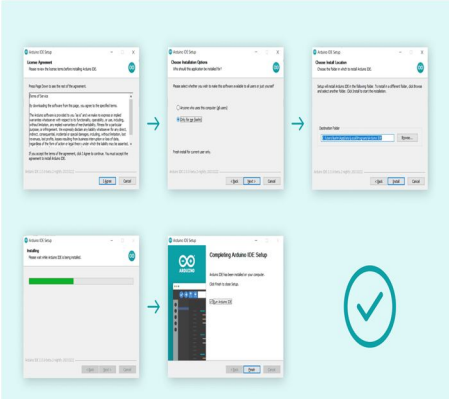


Fig.2.Arduino IDE

B. Digi Spark installation

To install the DigiSpark board, first make sure that Arduino IDE is installed on your computer. Download from Arduino's official website. Once installed, open the Arduino IDE and go to Profile->Preferences. In the Preferences window, enter the URL of the DigiSpark dashboard in the Plugin Dashboard Manager URL field: http://digistump.com/package_digistump_index.json. Click OK to close the Preferences window. Next, install the DigiSpark development board manager from "Tools" -> "Development Boards" -> "Development Board Manager" in the Arduino IDE. Search for “DigiSpark” in the Board Manager and install the DigiSpark board package. After installation go to Tools->Cards and select DigiSpark from the list. Finally, connect the DigiSpark card to the computer via USB.

Open the drawing template and click "Upload" to upload it to your DigiSpark dashboard. Now that your Arduino IDE is configured for DigiSpark you can start programming and uploading diagrams.

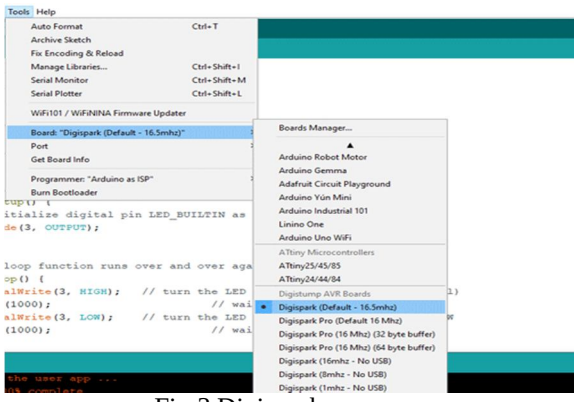


Fig.3.Digispark

C. Code Injection

To inject the code, first add the ATtiny board to the Arduino IDE from File -> Preferences and add the URL to the Plugin Board Manager URL. Next, go to "Tools" -> "Cards" -> "Card Manager", find "ATTinyCore" by Spence Konde and install it. Set the Arduino Uno to ISP mode by connecting it to your computer, open the Arduino IDE, load the "ArduinoISP" sketch, select the Uno board and the correct COM port, and upload the sketch to the Uno. Learn about ATtiny85 pin maps. Then, remove Uno from computer and connect Uno to ATtiny85, 5V to VCC and GND to G.

D. Connect AtTiny 85 to the mobile device

We connect the AtTiny 85 microcontroller device via USB. The target phone number can be easily called using the code given before this step. After this process, we will complete Android using Arduino IDE and AtTiny 85 USB bypass mode. This solution provides solutions to deficiencies in Google account sign-in, factory reset and security applications.

VI. IMPLEMENTATION

A. Arduino Software

It relates to the development environment concerned with brute force attacks. Arduino Software or Arduino IDE is a platform for writing, writing and shipping code for Arduino microcontrollers.

B. Attiny85 USB

Attiny85 is a small, low-cost microcontroller capable of several tasks. It works as a hardware component responsible for performing brute force attacks. Attiny85 is connected to the device via USB, allowing it to send commands and data to the device.

C. Plug USB into Android

This step involves physically connecting the Attiny85 microcontroller to the Android device using a USB connector. When installed, Attiny85 can interact with Android devices and launch brute force attacks.

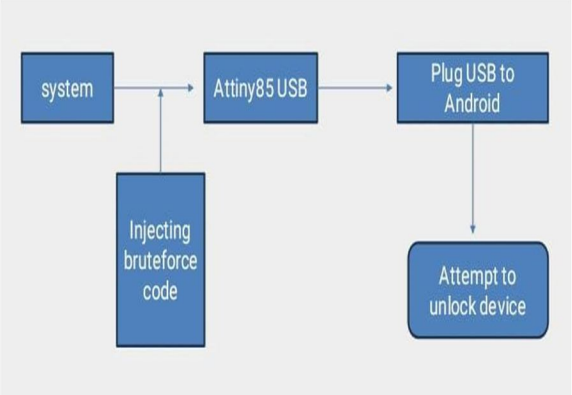


Fig.4.Block Diagram

VII. RESULT

A. *Injecting Brute Force Code*

The Attiny85 microcontroller sends commands to the device to execute brute force attacks. The code programmed into Attiny85 is designed to try different models to unlock the device. This technique involves sending commands to simulate user input, such as swiping the screen to create a pattern.

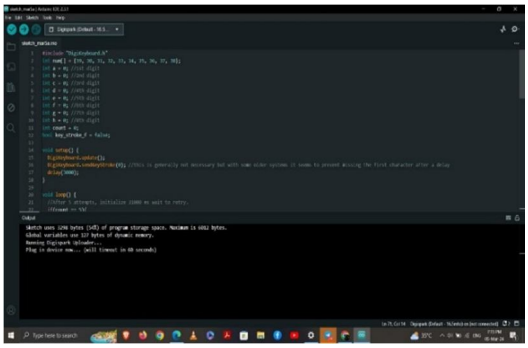


Fig.5.Uploding code

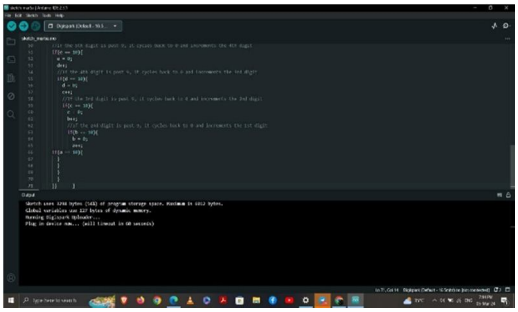


Fig.6.Running code

B. *Attempting To Unlock The Device*

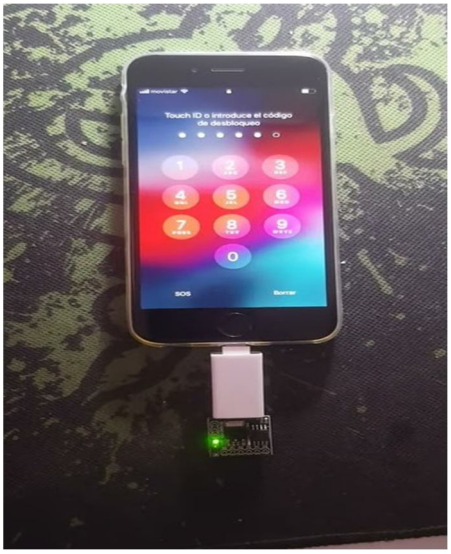


Fig.7.Connecting ATtiny 85 to mobile

The Attiny85 microcontroller, which is designed to mimic human input in order to unlock the smartphone's lock screen, sends orders to the Android device. In an effort to unlock the device, the Attiny85 microcontroller launches a brute force attack by methodically attempting various lock screen patterns. During this process, several patterns, like swipe movements, are generated and sent to the device.

©IJRASET: All Rights are Reserved

The Android device receives a command from the Attiny85 microcontroller and attempts to unlock itself using a pattern provided by the brute force attack. The tool acts as a guide and compares all models together to keep the model locked until a match is found or all combinations are exhausted. The Android device matches each pattern it receives with the user-configured lock screen pattern. The gadget unlocks and allows access to its contents and functions if a match is found. But if there's no match, the device stays locked and the brute force attack carries on.



Fig.8.Unlocking mobile

VIII. CONCLUSION & FUTURE SCOPE

Hardware Master Key uses Digispark Attiny85 to solve the issues related to passwords. The main advantage of the hardware master key is its user-friendliness. Unlike online solutions that may require an internet connection and rely on third-party servers, hardware keys operate independently and connect directly to the device they want to unlock. This flexibility improves user experience and eliminates the possibility of interference with online platforms such as server corruption or network outage. But despite their advantages, it is important for users to recognize and mitigate the risks associated with hardware keys. One of these risks is physical security. Since a key is a physical device, it can easily be lost, stolen, or accessed without permission if not properly protected.

Users must take of things such as storing keys in a safe location and using additional security measures such as login or biometric authentication (if supported by the device). Also, although the hardware key can be operated offline, that's not all. Protect yourself against malware threats. Malware can infect devices in a variety of ways, compromising the security of the switch or the device it is connected to. To reduce this risk, druggies should regularly modernize the switch's firmware, use estimable antivirus software on their bias, and be careful when connecting the switch to unauthorized bias. In conclusion, Hardware Key powered by the Digispark Attiny85 board provides an offline result for managing Legs and watchwords. Its stoner-friendly design and bettered security controls make it an seductive result for online problems. still, druggies should be apprehensive of the pitfalls, including physical security issues and malware pitfalls, and take applicable measures to alleviate these pitfalls.

IX. FUTURE SCOPE

The potential for Attiny85 to be used for a variety of nefarious purposes on Android devices in the future raises a number of alarming issues and highlights the necessity of strong security protocols and constant monitoring in the field of cybersecurity. Here's a more detailed explanation of each:

A. Reducing Time Intervals for Pattern Bypass

Because Attiny85 can perform pattern bypass in brute force assaults without time intervals, Android device security may be seriously jeopardised. The possibility of successfully evading lock screenpatterns in a shorter amount of time increases when time intervals are absent since the brute force attack becomes faster and more effective. Increased unauthorized access to Android devices may arise from this, raising the possibility of data breaches, privacy violations, and other security concerns.

B. Gathering Data from a Device

Because Attiny85 can collect data from Android devices, there are significant security and privacy risks. Attackers might use this feature to obtain private or confidential data that is saved on the device, including login credentials, financial information, and proprietary business information. The information that has been obtained may be exploited for nefarious activities such as financial fraud, corporate espionage, identity theft, or focused assaults on specific people or institutions.

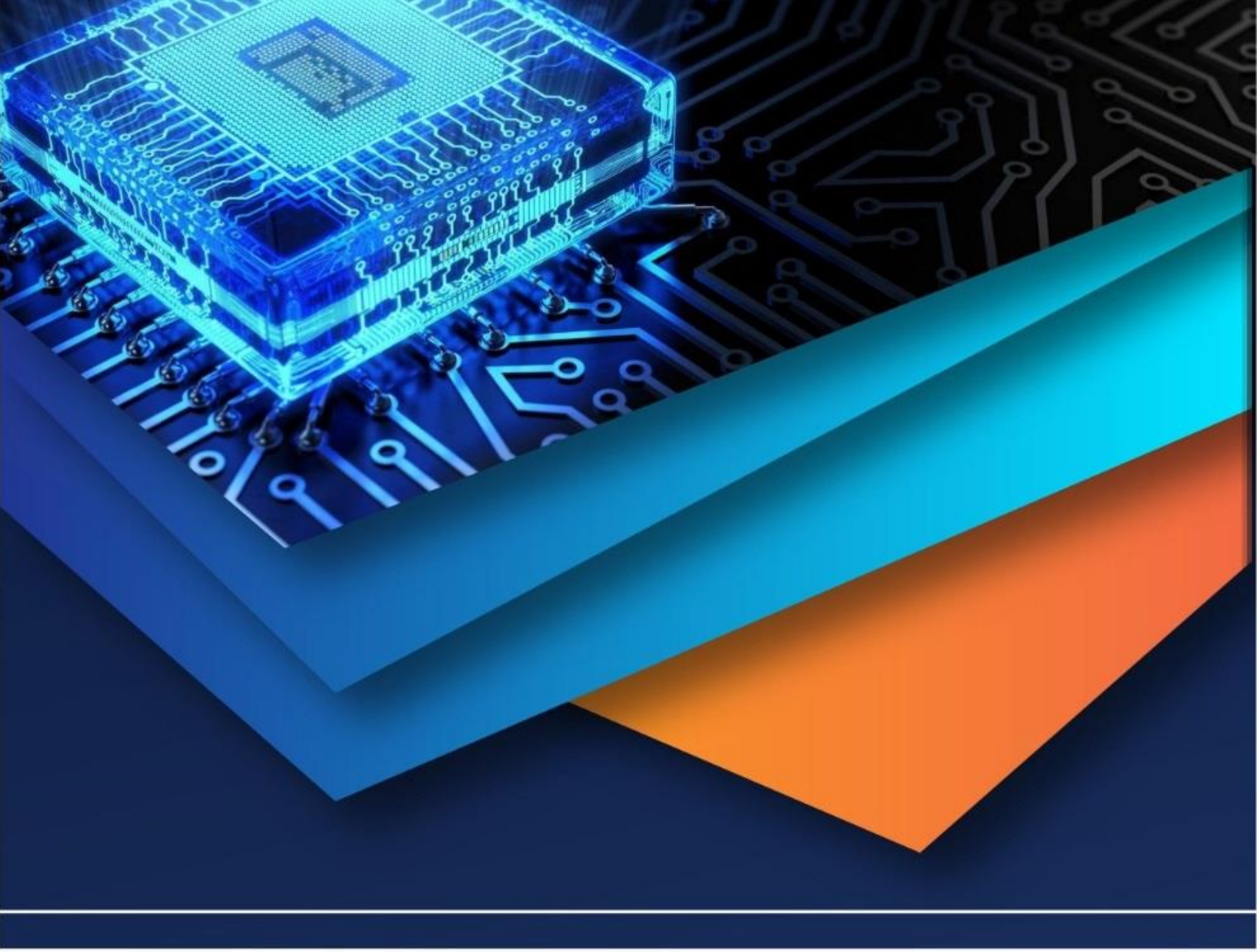
C. Virus or Malicious Code Injection

Android devices' security and integrity are seriously threatened by Attiny85's capacity to introduce viruses or other malicious programming into them. This feature could be used by attackers to infect the device with spyware, malware, ransomware, or other harmful programmes. Once installed, the malware might steal data, track user activity, and impair device operation.

REFERENCES

[1] K. Barmpatsalou,D. Damopoulos,G. Kambourakis, andV. Katos, " A critical review of 7 times of mobile phone exploration, " Digital Investigation,vol. 10.No. 4,p. 323- 349, 2013.
[2] CCL Group Ltd, the UK's leading exploration and consultancy company, 2016.
[3] E. Onyejegbu,A. Dorzhigulov,A.P. James, " Biometric Pixel Fusion Crossbar, " 2021 IEEE International Symposium on Circuits and Systems(ISCAS),p. 1- 5, 2020.
[4] Yeun Ku, Leo Hyun Park, Soyeon Shin, Tekyoung Kwon, " As reported Behavioral enrollment for mobile stoner authentication, " IEEE Access, Volume 7, runners 69363- 69378, 2019
[5] Puninder Kaur, Geeta, Vidhu Kiran Sharma, "Analysis of Secure Locking Techniques on Smart Phones", 2022 5th International Conference on Contemporary Computing and Informatics (IC3I), pp.1807-1811, 2022.
[6] Altaf Khan, Alexander G. Chefranov, "Captcha-based graphical encryption with strong password space and usability study," 2020 International Conference on Electrical, Communications and Computer Engineering (ICECCE), p. 1-6, 2020.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)