International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 04 Issue: 03 | Mar -2017 www.irjet.net p-ISSN: 2395-0072

IMPLEMENTATION OF SECURITY CHIP FOR MOBILE DEVICES

Wawdane Priyanka R.[1], Chormale Sushma C. [2],**Mali Ravina G.[3]** , Prof. Meenakshi Annamalai[4]

[1] *E&TC Dept. JSPM's BSIOTR, Wagholi, Pune 412207*
[2] *E&TC Dept. JSPM's BSIOTR, Wagholi, Pune 412207*
[3] *E&TC Dept. JSPM's BSIOTR, Wagholi, Pune 412207*
[3] *Assistant Professor, E&TC Dept. JSPM's BSIOTR, Wagholi, Pune, Maharashtra, India.*

Abstract - *The purpose of this paper to secure mobile devices. Usually mobile devices are easily hacked by the hacker or any software by flashing of ROM. The main aims of paper to secure mobile devices from the software and hacker it secure the devices through the hardware. The hardware is known as MTM chip (Mobile trusted module). This chip is going to interface with the mobile devise. Through IO interfaces, UART and various IO devices. The size of chip should be as small as possible for the mobile devices .It also provides the additional functions through software. It has own software to operate and it is user friendly for the user to secure their mobile devices from any threats. In this paper we implement hardware based security devices which provides security through hardware and as well as software.*

***Key Words*: MTM chip, Hummingbird algorithm, Security chip, smart card IC.**

1. INTRODUCTION

Now a days we all uses electronics devices to store sensitive data but the data can be hacked easily by the hacker through the software and also mobile, laptops stolen cases is rises for that we implement security chip which secured the devices from the theft. In this paper we implement hardware based security devices which provides security through hardware and as well as software. It checks that is user uses their own devices or that device is of another user. It checks the password which is entered by the user through the application based on hardware security. That password is checked by the hardware and confirmed the user. If the password is correct then and only then the user can use their mobile devices or if the password is incorrect hardware tells that the password is wrong and switched off the mobile by saying that the user is not correct. The chip is as small as possible that can be fit in the mobile or other electronic devices.

2. LITERATURE SERVEY

Recently we can see the rapid growth of mobile devices almost everyone has their devices like bring your own devices [1]. BOYD's benefits are clear employees are more familiar and satisfied while using their own devices and employers save money by not having to pay for high prices devices and data planes. Companies' goals with BOYD are to increases the flexibility. Convenience and portability of devices in order to order cater to their employees work flow, which increases their productivity. But in BOYD the various threads can be occurred like spam messages, spoof caller ID, MMS sender ID. After that the survey is going to take under security for mobile devices[2] in that mobile can be secured using various communication components through GPS,GSM and the network layer only but the BOYD cannot be safe and data can be stored on cloud and is carried out only observations of data corruption and there execution but data can be corrupted using no network also for that a trusted module is executed[3].In mobile computing the data can be kept secured using hardware devices and get secured the algorithm used for the encryption of data is 3DES,AES and SHA-1 for the security operations speed for that 10 mbps and 1154 mbps. Machine cycle required for the execution of AES are the 1616 for 128 bits and also 128 key. AES and SHA-1 uses separate code for encryption and decryption. It only developed on hardware basis there is no interface of software among this [3] type of interface. Technological advancement in computing, communicational devices, as well as network connectivity is shifting the usages of conventional desktop computers to mobile devices. It is predicted that there will be a staggering amount of over 2 billion smartphones users worldwide by the year 201. The increasing reliance on these devices inevitably implies the increase in sensitive data stored on this platform, unfortunately, the portability of mobile devices also makes it vulnerable to theft [4]. As more and more capabilities are added to cell phones, the issue of mobile phone security is of increasing concern to cell phone stakeholders (Malicious code moves to mobile devices). Security concerns are intensified because these expanded capabilities boost the incentive for and multiply the opportunities for perpetrating security attacks [5]. The issue complicated by the fact that

wireless devices were not originally designed with security as a top priority. Data privacy and Digital Right Management (DRM) agents pose strict security requirements. The first step in making handheld devices and smartphones resistant to various types of attacks is therefore providing overall security architecture, security-aware design and robust software layers [6].

3. DESIGN OF MTM CHIP

3.1Hardware of MTM chip

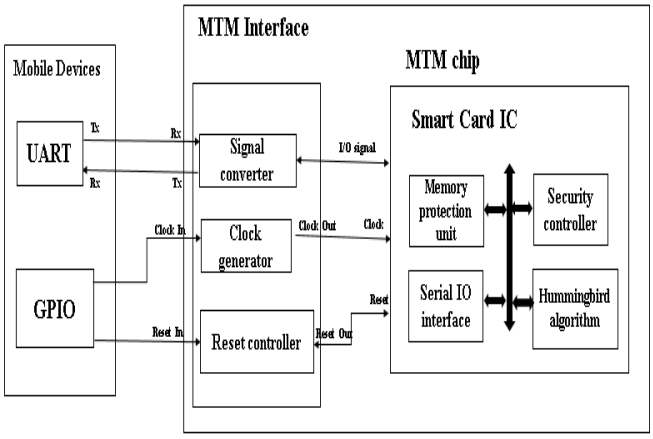

Fig-1: Hardware architecture for proposed MTM chip

The MTM [7] chip consist of an interfaces and smart card IC. The smart card IC consist of the memory protection unit to protect the memory from the external threads which can be occurred using external software. The stored password can be protected using this memory protection unit. The security controller can used to provide security using hummingbird algorithm. Hummingbird algorithm used same code for encryption and decryption [8].Serial IO interfaces are used for the serial communication between the mobile devices and the MTM chip for the proper communication. The communication between the UART that is Universal Asynchronous Receiver Transmitter and IO signal can be carried out by the half duplex communication. From the UART code is transmitted to the single converter through that it is then transferred to the smart card IC. From the General Purpose Input Output that is GPIO is transferred clock enable to the clock generator of1250 baud rate to the smart card IC. The same GPIO gives signals to the reset controller for reset the circuitry, if data or code is incorrect. When there is no use of IC the clock generator gets deactivated internally to minimize power consumption.

3.2 Software of Proposed MTM Chip

In software architecture there are three blocks are considered first one is the mobile devices second is the chip operating block and third is the command processing block. At the starting time password is user defined private keys transferred from the mobile devices that is first block through the IO interfaces of the UART to the chip operating block. The chip operating block consist of the cryptographic co-processor and IO interfaces .the cryptographic co-processor encode all the data and transferred to the chip OS. The Chip OS transferred all data to the command processing block, this encoded data accepts the message management and given to the hummingbird cryptographic engine to decode same data which is transferred by the cryptographic co-processor. If the data is matched from the secured service execution engine then message management sends message to the chip OS then chip OS sent that information data to the main processor, now the main processor start mobile devices and further processing will done.

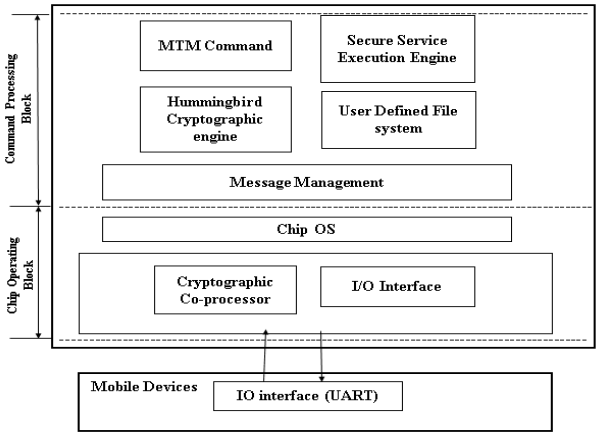

Fig-2: Software architecture for proposed MTM chip

If the data does not match from the secure service execution engine then the messenger management transfers the message to the chip OS that password is not matched hence reset the execution. If second time the password didn't match it will again reset the execution second time. We gives two times reset circuitry for the purpose of user friendly device. If all the reset execution gets failed the message management sets the message to the chip OS that the all data didn't get matched hence we stop the execution of the main processor of the mobile devices. This way the mobile devices gets switched off and we can't do further process and device is secured.

4.Proposed Implementation Work and Results

In this paper up till now we burn hummingbird cryptographic code in the Xilinx Spartan 3. For check that codes we interface mobile with Spartan 3 with the help of Bluetooth device.

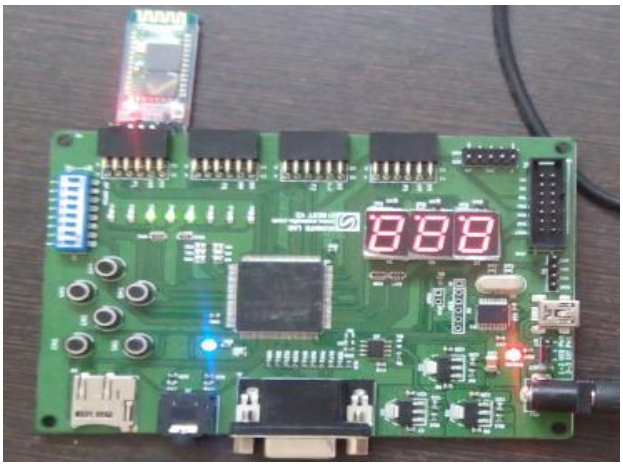

Fig-3: Screenshot of hardware implementation

Spartan 3 kit has 622+ Mbps data transfer rate per IO. Also has low cost high performance logic solution for high volume consumer oriented applications. It uses USB for burning the logic codes to the kit. When LED blinking is ON then kit and Bluetooth device is ready for use. We check that code by using the BT Simple Terminal software. When mobile's Bluetooth and the Bluetooth device get paired with each other. Then operation get started. We gives the user defined private key password of 4 different digits as A, B, C, D. When we entered these 4 different code then the signals sends from the Bluetooth devices to the Spartan 3kit as per the hummingbird cryptographic process the codes get verified and output is transferred to the mobile through the Bluetooth. If the code is right then it displays "Y" and if the code is wrong then it display "N".

Fig-(a): Screenshot password 'A' entered

Fig-(b): Screenshot password 'B' entered

Fig-(c): Screenshot password 'C' entered

Fig-(d): Screenshot password 'D' entered

Fig-4: a, b, c, d correct passwords entered

Figure (A), (B), (C), (D) if we type correct password then it shows the letter "Y" that is password is correct and verified by the cryptographic algorithm

Fig-(e): Screenshot password '1' entered

Fig-(f): Screenshot password 'K' entered

Fig-5: Any other wrong password entered

Figure (E), (F) if we type wrong password then it shows the letter "N" that is password is incorrect and verified by the cryptographic algorithm.

CONCLUSION

Thus this paper provides security for various hand held and mobile devices. Hummingbird algorithm is efficient for the encryption and decryption of the user defined private keys.

REFERENCES

[1] Y. Wang, J. Wei, and K. Vangury, "Bring Your Own Device Security Issues and Challenges," in Proc. The 11th Annual IEEE Consumer Communications and Networking Conference (CCNC), Las Vegas, USA, pp. 80-85, Jan. 2014.

[2] M. L. Polla, F. Martinelli, and D. Sgandurra, "A Survey on Security for Mobile Devices," IEEE Communications surveys & tutorials, vol. 15, no. 1, pp. 446-471, Mar. 2013.

[3] M. Kim, H. Ju, Y. Kim, J. Park, and Y. Park, "Design and implementation of mobile trusted module for trusted mobile computing, "IEEE Trans. Consumer Electron., vol. 56, no. 1, pp. 134-140, Feb. 2010.

[4] Pin Shen Teh, Ning Zhang, Andrew Beng Jin Teoh, Ke Chen "A Survey on touch dynamics authentication in mobile devices," ELSEVIER Science Direct, computer & security, vol.59, pp.210-235, 18 Mar.2016.

[5] Carlin Covey, Mark Redman, Thomas Tkacik "An Advanced Trusted Platform for Mobile Phone Devices," ELSEVIER, Science Direct, Information Security Technical Report, vol. 10, pp.96-104, 2005

[6] A. Ashkenazi, D. Akselrod "Platform Independent Overall Security Architecture In Multi-processor System-on-chip Integrated Circuits For Use In Mobile Phones and Handheld Devices," ELSEVER, Science Direct, Computer and Electrical Engineering, vol.33, pp.407-424, 23 July 2007

[7] M. Rabbani, R. Ramprakash, M. tech Students, "Design of Hummingbird Algorithm for Advanced Crypto Systems," IJEDR, vol.2, Issue 1, ISSN 2321-9939, 2014

[8] Hongil Ju, Youngsae Kim, Yongsung Jeon, and Jeongnyeo Kim, "Implementation of a Hardware Security Chip for Mobile Devices," IEEE Consumer Electronics, vol. 61, no.4, pp305-700, 4 Nov 2015