ISSN XXXX XXXX © 2019 IJESC

Research Article Volume 9 Issue No.3

Smart Security System using Analog Authentication

R.Bavithra[1], G. B. Mukil[2], C. Sasikumar[3], V. Sivamani[4], I. Sutharsan[5]
Department of Electronics and Communication Engineering
Akshaya College of Engineering and Technology, India

Abstract:
Growth in technology leads the society to get better performance. On the other hand it is more complex to analyze, more vulnerable, population and other security issues. So the this is hard to secure our digital data. Already existing security methods are day by day reaches to less secured. improvement of hacking machines, Artificial intelligence algorithms and other methods are increasing the hacker performance. So the new algorithms were increasing to improve the security in the society. "Smart security system using analog authentication" is the one method to overcome all these issues in this digital world. By this method we improved the security in bit level by existing communication methods. By our project both physical and soft security system can be secured. Even though fingerprint, face recognition and high complex password like system failed in it's security level this project expected to have the more complex to provide the solution around black hats.

I. INTRODUCTION:

Embedded systems: An electronic system which integrates the hardware circuitry with the software programming techniques for providing project solutions is called as embedded systems. By using this embedded system technology the complexity of the circuits can be reduced to a great extent which further reduces the cost and size. Embedded system was primarily developed by Charles Stark for reducing the size and weight of the project circuitry.

Characteristics of hardware: Our analog authentication method should need following specifications to give better throughput.

- making the SOC [system on-chip] hardware will be reduces digital data capturing in system.
- Reducing channel noise and SQNR [Signal to Quantization Noise Ratio] will improve the performance of the system.

Existing systems: Currently using webAuthn and windows USB password recovery are the examples of USB keys. User can’t remember large number of password to secure their account information. so this types of recovery method will help them to recover or unlock their account with correct authentication. in these systems previously the digital data is recorded by the USB, when we need to activate our account this will be helpful at the time of authentication.

Proposed system: The analog System [USB like key device] compare the analog values from the already stored value in lock system. It contain n bit ADC/DAC data stored as digital signal with the sequence of array (Length N). If the analog value is valid then the locker will open otherwise it will not open. This system is more secure than other system because sampling rate can increase with certain level of security. The implementation of this project in any sector the cost wise very low and the security level is very high. Making it as SOC hardware with the size of pen drive will not be affected by MITM type attack. because it can be made with half-duplex communication channel. A majority of consumers are interested in new features and functionality that are enabled by connected home technology. Looking forward, the arrival of new smart home features is likely to both expand the reach of home security and provide consumers with new ways to manage their busy lives.

Working principle: Analog authentication working by the concept of bit level encryption of data. if we use n bit resolution ADC and DAC n bit digital data combines to make a single sample data of analog signal. Lock system and key system have two ADC and DAC circuit inside the SOC hardware. Lock device is integrated with the digital device which needs to be unlocked or login. Initially digital device generates random number array of length N and the random data interval of 0 - (2^n)-1. For example array for n=10 & N=10 will be like [184, 48, 1023, 12, 673, 376, 272, 878, 583, 944]. This same data is stored in key device while creating the key device in the simplex system. but the need of key-lock authentication we taken the concept of two SOC (key and lock) hardware with half-duplex. half-duplex uses different two analog array of data to transmit and receive analog signal from the ADC/DAC. In real-time we can increase this N value to 1000 or more. for this application we need sampling rate of 1000 or more depend upon the samples and delay to unlock.

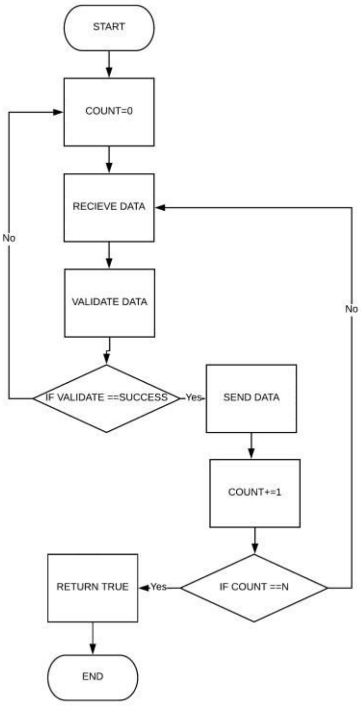

Figure.1. caption. Flowchart of steps in authentication in the Key or Lock system.

Practical Analytics of Security:

security level: It is a simplest method to build very complex type password to take security to another level. Practically increasing the possible chances and reducing number of correct outputs in system will improves security. We know that choosing correct Entry (unlocking event) in total possible entries will be calculated by below equation,

$$probability = \frac{number\ of\ correct\ entries}{total\ entries}$$

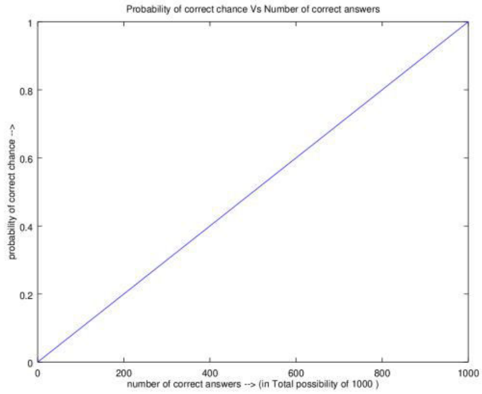

Figure.2. number of correct answers vs total probability

we should maintain only one correct key to unlock device to increase its complexity, and for the wrong entry the probability equation will be,

$$probability = 1 - \left(\frac{2}{10}\right) \quad \text{(or)}$$

$$= \frac{8}{10}\frac{(wrong\ prob.)}{(total\ prob.)}$$

when the correct chance will (Actual answers probability) reduces it will increases the security at higher range.

Effect of probability in security

Every pin, password, mobile pattern, picture have particular probability to provide complexity.

If the system have very low probability value for the unlocking event it is very difficult to unlock that device.

$$Complexity = \frac{1}{probability\ of\ unlocking\ event}$$

using single analog data with ADC/DAC of n bit resolution will be provides,

$$probability(unlocking) = \frac{1}{2^n} = 2^{-n}$$

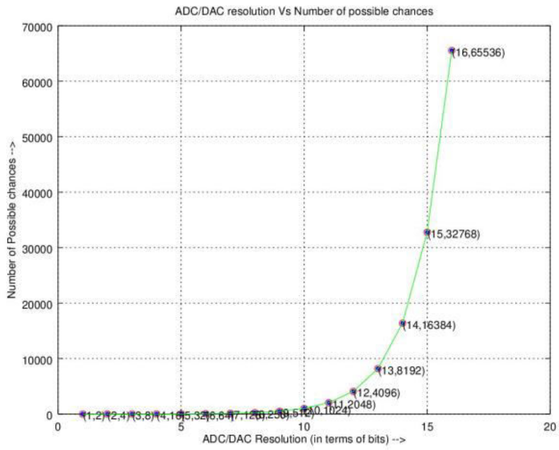

Figure.3. ADC/DAC resolution Vs probability

Bit level security:

The sequence of n analog values will be increases its complexity. For the N analog values the complexity can be calculated by,

$$probability(unlock) = \left(\frac{1}{2^n}\right)^N = 2^{-n \times N}$$

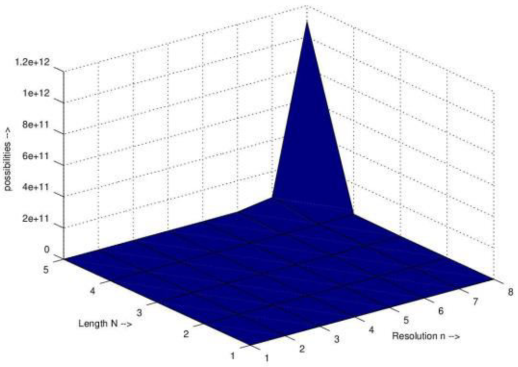

Figure.4. effect of sequence length and resolution on probability

every bits of ADC/DAC data affects its complexity. So the encryptions in the '**bit level**'.

II. LITERATURE SURVEY:

In networking ipv4 and ipv6 protocols are based on this encryption. IPV4 have 4 segments of 8 bit data (in sequence) one followed by another. This complexity refers the total number of devices can be connected in one large network.

From 0.0.0.0 to 255.255.255.255 totally,

$$2^8 \times 2^8 \times 2^8 \times 2^8 = 4{,}294{,}967{,}296$$

number of devices can be connected in one network. Choosing of one correct device among all devices in that network will have the probability of

$$= 1/4{,}294{,}967{,}296 \approx 2.3283064365e^{-10}$$

Similar way in our analog authentication method uses the policy to our security. when we used 12 bit ADC/DAC with the sequence of 10 analog data with one analog key, the possible causes raised to $= 4096^{10} \approx 1.32922799578e^{+36}$ just only from 10 analog sequence data we can get this amount of possible combinations.

Output:

Output of the system is unlocking the lock system which is integrated with with pc/mobile hardware. using the secondary authentication leads to recover this lock when you lose analog key [usb like key] otherwise it can't be recovered.

III. CONCLUSION:

By this method we can increase probability and the possibilities nearly to zero and infinite respectively. achieving high security with cheap price of hardware is succeeded by this algorithms and probability theorems. User can modify the N and n values depend upon their needs. Making optical channel between key and lock device can take it to another level.

IV. REFERENCES

[1]. W. Tan, J. R. Cruz, "Signal-to-noise ratio mismatch for low-density parity-check coded magnetic recording channels", IEEE Trans. Magn., vol. 40, no. 2, pp. 498-506, Mar. 2004.

[2]. W. Tan, private communication, 2004.

[3]. T. J. Richardson, R. L. Urbanke, "The capacity of low-density parity check codes under message-passing decoding", IEEE Trans. Inf. Theory, vol. 47, no. 2, pp. 599-618, Feb. 2001.

[4]. T. Schwarzer, J. Falk, M. Glaß, J. Teich, C. Zebelein, C. Haubelt, "Throughput-optimizing compilation of dataflow applications for multi-cores using quasi-static scheduling", Proceedings of the 18th International Workshop on Software and Compilers for Embedded Systems, pp. 68-75, 2015.
Show Context Access at ACM

[5]. K. Bertels, V. M. Sima, Y. Yankova, G. Kuzmanov, W. Luk, G. Coutinho, F. Ferrandi, C. Pilato, M. Lattuada, D. Sciuto, A. Michelotti, "Hartes: Hardware-software codesign for heterogeneous multicore platforms", IEEE Micro, vol. 30, no. 5, pp. 88-97, Sept 2010.

[6]. B. Carrion Schafer, K. Wakabayashi, Computers Digital Techniques IET, vol. 6, no. 3, pp. 153-159, 2012.

[7]. B. Carrion, A. Mahapatra, IEEE Embedded Systems Letters, vol. 6, no. 3, pp. 53-56, 2014.

[8]. NEC CyberWorkBench, 2017.

[9]. J. Huang, F. Qian, Y. Guo, Y. Zhou, Q. Xu, Z. M. Mao, S. Sen, O. Spatscheck, "An in-depth study of lte: Effect of network protocol and application behavior on performance", Proceedings of the SIGCOMM 2013, pp. 363-374, 2013.
Show Context Access at ACM

[10]. Y. Ohara, K. Nishizuka, K. Chinen, K. Akashi, M. Kohrin, E. Mu-ramoto, S. Miyakawa, "On the impact of mobile network delays on connection establishment performance of a carrier grade nat device", Proceedings of the AINTEC 2014, pp. 1-8, 2014.
Show Context Access at ACM

[11]. V. Bajpai, J. Schonwalder, "Measuring tcp connection establishment times of dual-stacked web services", Network and Service Management (CNSM) 2013 9th International Conference on, pp. 130-133, Oct 2013.

[12]. H. Alzoubi, M. Rabinovich, O. Spatscheck, "Performance implications of unilateral enabling of ipv6", Passive and Active Measurement, vol. 7799, pp. 115-124, 2013.

[13]. S. Zander, L. L. Andrew, G. Armitage, G. Huston, G. Michael-son, "Mitigating sampling error when measuring internet client IPV6 capabilities", Proceedings of the 2012 ACM Conference on Internet Measurement Conference ser. IMC '12, pp. 87-100, 2012.

[14]. M. Bagnulo, M. Sullivan, P. Matthews, I. van Beijnum, "Rfc 6147: Dns64: Dns extensions for network address translation from IPV6 clients to ipv4 servers", IETF Tech. Rep., 2011, [online] Available: www.ietf.org/rfc/rfc6147.txt.

[15]. C. Huitema, "Rfc 4380: Teredo: Tunneling IPV6 over udp through network address translations (nats)", IETF Tech. Rep., 2006, [online] Available: www.ietf.org/rfc/rfc4380.txt.

[16]. D. Wing, A. Yourtchenko, "Rfc 6555: Happy eyeballs: Success with dual-stack hosts", IETF Tech. Rep., 2012, [online] Available: www.ietf.org/rfc/rfc6555.txt.

[17]. Android CLAT, [online] Available: https:// android. Google source.com/platformlexternal/android-clat.

[18]. C. Bao, C. Huitema, M. Bagnulo, M. Boucadair, X. Li, "Rfc 6052: IPV6 addressing of ipv4/ipv6 translators", IETF Tech. Rep., 2010, [online] Available: www.ietf.org/ rfc/ rfc6052.txt.

[19]. T. Savolainen, J. Korhonen, D. Wing, "Rfc 7050: Discovery of the IPV6 prefix used for IPV6 address synthesis", IETF Tech. Rep., 2013, [online] Available: www. ietf. org/ rfc/rfc7050.txt.

[20]. R. Draves, "Rfc 3484: Default address selection for internet protocol version 6 (ipv6)", IETF Tech. Rep., 2003, [online] Available: www.iettorg/rfc/rfc3484.txt.

[21]. Global IPV6 Deployment Progress Report, [online] Available: http://bgp.he.net/ipv6-progress-report.cgi.

[22]. Cisco 6lab The place to monitor IPv6, [online] Available:http://6lab.cisco.com/stats/cible.php?country= world = network.

[23]. Mustafa Kilic, Yusuf Leblebici, "A DAC Assisted Speed Enhancement Technique for High Resolution SAR ADC" in PRIME 2017, Giardini Naxos-Taormina, Italy.

[24]. B. Murmann, P. Nikaeen, D. J. Connelly, R. W. Dutton, "Impact of Scaling on Analog Performance and Associated Modeling Needs", IEEETransactions on Electron Devices, vol. 53, no. 9, Sept. 2006.

[25]. Maoqiang Liu, Arthur van Roermund, Pieter Harpe, A 7. 1fJ/conv.-step 88dBSFDR12b SAR ADC with Energy-Efficient Swap-to-Reset, IEEE, 2016.

[26]. T. Jiang, W. Liu, F. Y. Zhong, C. Zhong, K. Hu, P. Y. Chiang, "A Single-Channel 1. 25-GS/s 6-bit 6. 08-mW Asynch ronous Successive Approximation ADC With Improved Feedback Delay in-nm CMOS", IEEE J. Solid-State Circuits, vol. 47, pp. 2444 to 2453, Oct. 2012.

[27]. L. Kull, T. Toifl, M. Schmatz, P. A. Francese, C. Menolfi, M. Braendli, M. Kossel, T. Morf, T. K. Andersen, Y. Leblebici,"A3.1mW 8b1. 2GS/s Single-Channel Asynchronous SAR ADC with Alternate Comparators for Enhanced Speed in 32nm Digital SOI CMOS" in ISSCC 2013, San-Fransisco USA.

[28]. Y.-K. Chang, C.-S. Wang, C.-K. Wang, "A 8-bit 500 kS/s low power SAR ADCfor bio-medical application" in ASSCC Dig. Tech. Papers, pp. 228-231, Nov. 2007.

[29]. C.-C. Liu, S.-J. Chang, G.-Y. Huang, Y.-Z. Lin, "A 10-bit 50-MS/s SAR ADCwith a monotonic capacitor switching procedure", IEEE J. Solid-State Circuits, vol. 45, no. 4, pp. 731-740, Apr. 2010.

[30]. V. Hariprasath, J. Guerber, S.-H. Lee, U.-K. Moon, "Merged capacitor switching based SAR ADC with highest switching energy-efficiency", Electron. Lett., vol. 46, no. 9, pp. 620-621, Apr. 2010.

[31]. P. Harpe, C. Zhou, N. P. van der Meijs, X. Wang, K. Philips, G. Dolmans, H. deGroot, "A 26 W 8-bit 10 MS/s asynchronous SAR ADC for low energy radios", IEEE J. Solid-State Circuits, vol. 46, no. 7, pp. 1585-1595, Jul. 2011.