IJCSE International Journal of Computer Sciences and Engineering Open Access

Technical Paper Vol.-6, Issue-6, June 2018 E-ISSN: 2347-2693

Towards Performance Analysis of Symmetric Key Algorithm on n-Core Systems: An IOT Perspective

Manju Suchdeo[1], Deepak Mawane[2], Mahek Negandhi[3], Shipra Sarkar[4], Shaligram Prajapat[5]

[1,2,3,4,5] International Institute of Professional Studies, Devi Ahilya University Indore, India

Available online at: www.ijcseonline.org

Accepted: 09/Jun/2018, Published: 30/Jun/2018

Abstract- Several Symmetric Key based algorithms exist for securing data of big size. In Order to investigate the efficient one , performance analysis is often desirable activity over variety of parameters including number of cores or processors. In present work one symmetric key algorithm has been considered for analysis for n=1(Serially) and (n =2) for Parallel analysis, (where n is number of core). The relative gain of serial implementation and tested for efficiency indicates that encryption of data chunks in parallel is the for blowfish algorithm. The findings in this study provides a useful direction to users and designers of low power handheld devices and IOT to exploit faster encryption and decryption of data with more number of cores.

Keywords- Symmetric Key Cryptography, Blowfish , parallel implementation

I. INTRODUCTION

For exponential growth of digital data various active systems are generating data on computing and storage, cloud and IOT based computing services. Moreover, conventional IOT is enabled with set of connected things { Parts of computers, Networks, Monitors, Controllers, technologies}able to share information using Communication Technologies = { device to device, device to gateway, device to cloud, back-end,data sharing components} is generating information [1].

Further, most recent Consumer electronics (IoT enabled products) and home automation(smart home), use of Internet and energy efficient data sending and receiving devices [2] .The increased connectivity of devices, results into the growth of security and privacy vulnerabilities due to the poorly secured applications, services, and devices [3]. Less Processing power requirement of critical applications of digital and embedded devices leads to vulnerable system, to common malwares of personal computers. In other words restricted computing power of the devices, device cost, completion in the market etc [4]. Making exponential usage rate of everyday applications , trusted computing, and applied cryptography have not been integrated on them.

During analysis of algorithm for security of information the consideration of analysis of the applied suites and parameters like processing power, memory resources, and power availability are considered. During this analysis cryptographic models and security schemes are unclear, so detailed analysis is needed, in order to be ensured, for applicability in the specified resources of IoT [5]. specialized investigation is also required for hand held ,portable devices[6] together with key management is issue in future designs of these devices.[7]

In order to ensure secure end-to-end N/W data exchange for M2M and IoT devices with its Lightweight Stream Encryption Technology [10] has been demonstrated in Figure 1.0. The symmetric key generated by the model of figure 1.0 will produce secure encrypted data for IOT enabled system.

Figure 1: Application of Symmetric Key for IOT based Cryptosystem.

II. BACKGROUND AND RELATED WORK

In [19] a tool has been discussed for performance analysis the time consumed by a symmetric-key encryption or decryption technique to encrypt or decrypt some data with some key with variable file size , data size, key size, processor load, device configuration etc. This work computes the encryption or decryption time taken by DES, 3DES, BLOWFISH , TWOFISH symmetric-key encryption techniques [20, 21] to encrypt or decrypt data possessing different size with a fixed size key and also in the case of a fixed size data with keys of different sizes to analyze the excellence of a technique in some circumstance that aids in the comparative study of an encryption technique and make us choose the efficient one. This needs in choosing an encryption or decryption technique to encrypt or decrypt some data with some key

IV. RESULTS AND DISCUSSION

The results in the table below were obtained by evaluating the time taken when data strings of variable lengths (64, 128, 256, 512, 1024 in Kilobytes) were enciphered and deciphered in the following scenario:

1. Serial Implementation
2. Parallel Implementation

Table 1. Comparison of encipher time (Seconds) for various file size(in kilobytes)

Input size in kilobytes	Serial Implementation	Parallel Implementation
64	9.10882	3.3151
128	17.894	6.3015
256	35.8313	12.3893
512	71.3537	24.9056
1024	142.7755	53.8180

Table 2. Comparison of decipher in kilobytes – time in seconds

Input size in kilobytes	Serial	Parallel
64	8.53390	3.3133
128	16.9896	5.9965
256	33.9818	11.8374
512	67.7031	25.0277
1024	135.1450	52.3342

Table 3. Comparison of parallel implementation – encipher – in seconds

Data in KB	Number of Workers			
	4	3	2	1
64	3.3151	4.1413	5.2268	9.10882
128	6.3015	7.5946	10.0691	17.894
256	12.3893	14.8538	20.173	35.8313
512	24.9056	29.3676	40.1785	71.3537
1024	53.8180	61.0181	81.2044	142.7755

Table 4. Comparison of parallel implementation – decipher – in seconds

data (KB)	Number of Workers			
	4	3	2	1
64	3.3133	3.7135	4.93184	8.53390
128	5.9965	7.19505	9.62411	16.9896
256	11.8374	14.2718	19.0550	33.9818
512	25.0277	38.5027	38.3164	67.7031
1024	52.3342	59.4039	76.1798	135.1450

It can be observed from the tables that the parallel implementation gives higher throughput than the serial implementation and the efficiency of the parallel implementation increases with increase in the number of workers.

V. CONCLUSION

In order to achieve better results, flexible combined mode supports for encryption and authentication need to be explored[8].optimal cipher generation with efficient implementations and low effort is to be seen, which otherwise could be easily broken, with current or near future computing power. To enhance IOT enabled systems cryptographic purposes and analysis is desirable and need to be assessed frequently [9].

In this paper we present a comparison between the serial and parallel implementations of the Blowfish Algorithm. The parallel implementation was then tested over systems with different number of cores. The implementation integrates a parallel execution of the F function along with dividing the data into chunks of 64 bits and processing them parallelly. The results show that parallel implementation provides better performance than the serial implementation and this implementation gives a higher throughput when the number of cores are increased, thus making the implementation useful in scenarios where there are a large number of cores.

VI . REFERENCES

[1] D. Miorandi, S. Sicari, F. D. Pellegrini, I. Chlamtac, Internet of things: Vision, applications and research challenges, Ad Hoc Networks 10 (7) (2012) 1497.

[2] E. Isa, N. Sklavos, “Smart Home Automation: GSM Security System Design and Implementation”, proceedings of the 3rd Conference on Electronics and Telecommunications (PACET’15), Ioannina, Greece, May 8-9, 2015.

[3] M. Katsaiti, A. Rigas, I. Tzemos, N. Sklavos, “Real-World Attacks Toward Circuits & Systems Design, Targeting Safety Invasion”, proceedings of the International Conference on Modern Circuits and Systems Technologies (MOCAST’15), Thessaloniki, Greece, May 14-15, 2015.

[4] N. Sklavos, P. Souras, “Economic Models and Approaches in Information Security for Computer Networks”, International Journal of Network Security (IJNS), Science Publications, Vol. 2, No 1, Issue: January, pp. 14-20, 2006.

[5] S. Gusmeroli, S. Piccione, D. Rotondi, “A capability-based security approach to manage access control in the internet of things”, Mathematical and Computer Modelling 58 (5) (2013) 1189.

[6] Kiev Gama, Lionel Touseau, Didier Donsez, “Combining heterogeneous service technologies for building an Internet of Things middleware”, Computer Communications, Volume 35, Issue 4, 15 February 2012, Pages 405-417, ISSN 0140-3664.

[7] R. Roman, J. Zhou, J. Lopez, “On the features and challenges of security and privacy in distributed internet of things”, Computer Networks 57 (10) (2013).

[8] N. Sklavos, R. Chaves, F. Regazzoni, Wireless-SoC-Security: “FPGA Based System-On-A-Chip Security Schemes for 4G & 5G”, Tutorial, 11th HiPEAC Conference 2016 (HiPEAC’16), Prague, Czech Republic, January 18-20, 2016.

[9] N. Sklavos, “Securing Communication Devices via Physical Unclonable Functions (PUFs)”, Information Security Solutions Europe (isse’13), Brussels, 22-23 October, Belgium, 2013, pp. 253-261, Springer, ISBN: 978-3-658-03370-5

[10]http://circuitcellar.com/cc-blog/light-weight-data-encryption-for-iot-and-m2m-applications).

[11] Peter Mell and Timothy Grance, ‘The NIST Definition of Cloud Computing’ Special Publication 800-145, Jan. 2011.

[12] Shakeeba S. Khan, Prof. R.R. Tuteja, ‘Security in Cloud Computing using Cryptographic Algorithms’ International Journal of Innovative Research in Computer and Communication Engineering , Jan. 2015 , ISSN (Print): 2320-9798 Vol. 3, Issue 1.

[13] Er. Ashima Pansotra and Er. Simar Preet Singh, ‘Cloud Security Algorithms’ International Journal of Security and Its Applications , 2015 , Vol.9, No.10 , pp.353-360.

[14] Ako Muhamad Abdullah, ‘Advanced Encryption Standard (AES) Algorithm to Encrypt and Decrypt Data’, June 16, 2017.

[15] B. Schneier, Description of a New Variable-Length Key, 64-bit Block Cipher (Blowfish), In proc. Cambridge Security Workshop, 191204 ,1993.

[16] B. Schneier, Applied Cryptography: Protocols, Algorithms, and Source Code in C. John Wiley and Sons, New York, 1996.

[17] Soufiane Oukili and Seddik Bri, ‘High Throughput Parallel Implementation of Blowfish Algorithm’ Applied Mathematics & Information Sciences No. 6, 2087-2092 2016

[18] B. Schneier, 'The Blowfish Encryption Algorithm'. ‘https://www.schneier.com/academic/blowfish/ .

[19] Shaligram Prajapat , Ramjeevan Singh Thakur, "Cryptic Mining for Automatic Variable Key Based Cryptosystem", Procedia Computer Scienc , Volume 78, PP.199-209,2016,https://doi.org/10.1016/j.procs.2016.02.034

[20] Shivlal Mewada, Pradeep Sharma, S.S Gautam, “Exploration of Efficient Symmetric AES Algorithm”, IEEE 2016 Symposium on Colossal Data Analysis and Networking (CDAN), pp.1-5, Mar, 2016. DOI: dx.doi.org/10.1109/CDAN.2016.7570921

[21] Shivlal Mewada, Sharma Pradeep, Gautam S.S., “Exploration of Efficient Symmetric Algorithms”, IEEE 2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom)”, pp.663-666, March, 2016, DOI: http://www.dx.doi.org/10.13140/RG.2.2.22077.05607