An Approach towards Improved Cyber Security by Hardware Acceleration of Open SSL Cryptographic Functions

A. Thirueelakandan, T. Thirumurugan

Abstract*— Providing improved Information Security to the rapidly developing Cybernet System has become a vital factor in the present technically networked world. The information security concept becomes a more complicated subject when the more sophisticated system requirements and real time computation speed are considered. In order to solve these issues, lots of research and development activities are carried out and cryptography has been a very important part of any communication system in the recent years. Cryptographic algorithms fulfill specific information security requirements such as data integrity, confidentiality and authenticity. This work proposes an FPGA-based VLSI Crypto-System, integrating hardware that accelerates the cryptographic algorithms used in the SSL/TLS protocol. SSL v3 and TLS v1 protocol is deployed in the proposed system powered with a Nios-2 soft-core processor. The cipher functions used in SSL-driven connection are the Scalable Encryption Algorithm (SEA), Message Digest Algorithm (MD5), Secured Hash Algorithm (SHA2). These algorithms are accelerated in the VLSI Crypto-System that is on an Altera Cyclone III FPGA DE2 development board. The experimental results shows that, by hardware acceleration of SEA, MD5 and SHA2 cryptographic algorithms, the VLSI Crypto-System performance has increased in terms of speed, optimized area and enhanced level security for the target Cybernetic application.

Keywords*— Cryptographic algorithm, Hardware accelerator, SSL/TLS protocol, CtoH Compiler, VLSI Crypto - System.

I. INTRODUCTION

Universally all businesses, most government agencies, and many individuals now have web sites. As a result, businesses are enthusiastic about setting up facilities on the Web for electronic commerce. But the reality is that the Internet and the Web are extremely vulnerable to compromises of various sorts. It paves the demand for secure Web services. There are number of approaches to providing Web security are possible. The various approaches that have been considered are similar in the services, but they differ with respect to their scope of applicability and their relative location within the TCP/IP protocol stacks. One way to provide Web security is to use IP Security. Another relatively general-purpose solution is to implement security just above TCP. The for most example of this approach is the Secure Socket Layer (SSL) and its sister Internet standard known as Transport Layer Security (TLS). In General, SSL (or TLS) could be provided as part of the underlying protocol suite and therefore be transparent to applications. Application-specific security services are embedded within the particular application. For example, Netscape, Microsoft Explorer, Firefox and Chrome come equipped with SSL, and most Web Servers have implemented the protocol. However, deploying cryptographic algorithms in such SSL/TLS, could increase the computational complexity, causing poor performance for the Real Time System. Hence we go for the Hardware Accelerator, in which the Scalable Encryption Algorithm is coded in Verilog HDL; deployed into OpenSSL library; downloaded into an Altera Cyclone III FPGA; operated by NIOS II IDE. This paper is organized as follows. Section II is a brief discussion of related previous works. The next section presents the Existing system, which discusses the OpenSSL library, the Embedded Crypto-System design and the hardware accelerator cores used. The Section IV, V and VI describe the VLSI Crypto System Architecture, System Development and System Implementation Methodology. The paper concludes with the performance analysis of the developed system, conclusion and future scope.

II. RELATED WORK

Most papers on cryptographic processors describe algorithm-specific implementations. Hardware acceleration have been done by Mohamed Khalil-Hani in [1], where the embedded system integrates the AES-256, SHA-1,SHA-2, RNG, and RSA-2048 cryptographic hardware cores into one FPGA microchip. Acceleration of the Open SSL library resulted significant improvements in the system performance, which basically dependent on cryptography for operation. Another work by [2], designed and verified the working AES crypto Verilog core, which runs on top of an embedded Linux distribution, u Clinux. The Open SSL library has been ported and cross-compiled to work with only on AES that processes data blocks of 128 bits using a cipher key of length 128, 192, or 256 bits. His work proposed that the full suite of crypto cores can be accelerated by the Open SSL crypto library. In [3], the design and implementation of a crypto hash SHA-2 logic core in reconfigurable hardware is presented. With the crypto SoC implemented in an Altera Nios II Stratix FPGA-based prototyping system running on a 50 MHz system clock, he obtained a throughput of 644 Mbits/sec for our proposed by [4] developed a

Manuscript received on April 14, 2012.

A. Thiruneelakandan, Department of Electronics and Communication Engineering, Surya Group of Institutions, TamilNadu, India.Mob.No:9698209127., (e-mail: trizillion@gmail.com).

T. Thirumurugan, Department of Electronics and Communication Engineering, Surya Group of Institutions, TamilNadu, India. Mob. No.9789171713, (e-mail: thiru_ct77@yahoo.co.in).

hardware SHA-512 hardware core.

The work prototype of the cryptographic processor in FPGA technology. He implemented in the 1.5 GHz processor technology and the processor executed 5,265 RSA-1024 op/s and 25,756 ECC-163 op/s. Another work by [5] proposed, that the security methods use the advantage of digest authentication based on HTTP/1.1 and conceals data by using symmetric cryptography. The results indicate that using these methods expend more resources and time consuming.

III. THE EXISTING EMBEDDED CRYPTO-SYSTEM

The work [1] proposed an FPGA-based embedded system integrating hardware that accelerates the cryptographic algorithms used in the SSL/TLS protocol. The bottleneck of this proposal are that the AES – 256 and RSA – 2048 cryptography algorithm uses a large array of Substitution Box which requires a Heap of memory for Storage; Selection of a specific Random Prime Key; Matrix Transformation consume considerable time overhead.

Also the paper [2] focused on the use of the Altera Nios II CPU with a pre-designed and verified working AES crypto Verilog core, both of which runs on top of an embedded Linux distribution, uClinux. The OpenSSL library has been ported and cross-compiled to work on uClinux. The system runs on a 50 MHz clock. But the features that it lacks are three. Firstly, there are also other crypto functions that can be used, such as RSA, ECC and SHA. Secondly, it is also possible to link other hardware crypto core to the OpenSSL. And lastly, the computation time that the AES take to process were comparatively large, which decays the system performance.

So, we are in need of developing a system that best suit the embedded low power application, as well as high end security, must be satisfied. Hence, this paper deals with a more resource constrained, cryptographically strong and suitable for the low power Embedded system, that is VLSI Crypto System.

IV. VLSI CRYPTO-SYSTEM ARCHITECTURE

This paper integrates the lightweight at the same time stronger cryptographic function SEA into the accelerator core for use in networking security through the OpenSSL library, as shown in Fig. 1. The proposed VLSI crypto system is shown in the following architectural diagram. The Scalable Encryption algorithm, Message Digest algorithm, Secured Hash algorithm are incorporated in the OpenSSL Library and downloaded into an Altera Cyclone III FPGA. It is operated by Nios II CPU, connected through Network layer to host PC, by RS 232/USB cable.

This system is useful for embedded applications that need high security, speed and consume low power. Examples for this application include the safer surfing, secure document transfer file encryption/ decryption, certificate generation and cryptography for generic communication. The SEA, MD5, SHA-2 are coded in Verilog, synthesized and simulated. Many IP Stacks are implemented, such that layer 4 (e.g., TCP) and below are implemented in the operating system and anything above is implemented in a user process, as shown in

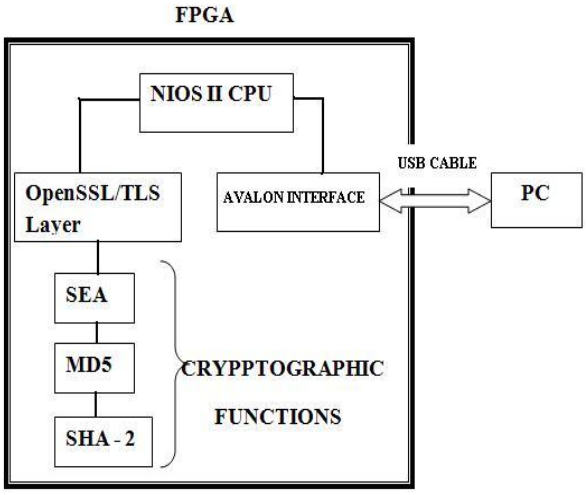

Fig. 1. System Architecture

Fig.2.The philosophy of SSL is that it is easier to deploy user processes and it don't require to change the operating system library is divided into two major sub-libraries [1]: (a) Libcrypto is the sub library that provides the cryptographic, arithmetic and certificate generation routines, and (b) Libssl is the sub-library that handles the SSL/TLS protocol routines. It invokes the libcrypto functions to execute these protocols.

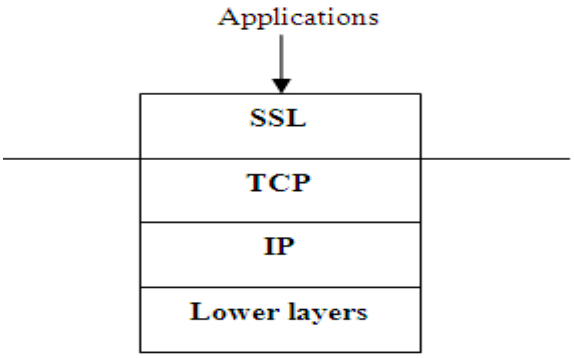

Fig. 2. Operating Point of the SSL at layer 3 (OSI ISO Layer).

V. SYSTEM DEVELOPMENT

SOPC Builder (System on a Programmable Chip Builder) is software made by Altera that automates connecting soft-hardware components to create a complete computer system that runs on any of its various FPGA chips. SOPC Builder incorporates a library of pre-made components (including the flagship Nios II soft processor, memory controllers, interfaces, and peripherals) and an interface for incorporating custom ones. Interconnections are made though the Avalon bus. Bus arbitration, bus width matching, and even clock domain crossing are all handled automatically when SOPC Builder generates the system.

A GUI is the only thing used to configure the soft-hardware components (which often have many options) and to specify the bus topology.

The resulting "virtual" system can then be connected to the outside world via the FPGA's programmable pins or connected internally to other soft components. The FPGA's pins are routed to connectors, such as for PCI or DDR, or as is often the case in embedded systems to other chips mounted on the same PCB.

The Processing steps in the SOPC Builder are:

1. SOPC Builder from the Quartus 9.0 IDE is selected.
2. From the Component Library, the following components, are selected,

i. Nios II Processor
ii. Interface Protocols ->Serial -> Avalon-ST->JTAG Interface.
iii. Memories and Memory Controllers ->On-Chip-> On-Chip Memory(RAM/ROM)

3. The desired system is built by choosing the HDL Files and adding into the System component. The top level module is assigned.
4. Upon running the Simulator, it generates 3 files with the extension .sof, .ptf, .qpf.
5. The .sof file is downloaded into the Cyclone III FPGA, using the Nios II C-to-Hardware (C2H) Acceleration Compiler.

Whereas, the other two files were used in Nios II IDE, to integrate and co-ordinate the developed system in the FPGA.

VI. SYSTEM IMPLEMENTATION

The generated .sof, .ptf, .qtf are processed to implement the desired VLSI Crypto System. The implementation steps are listed, as follows,

1. The system with filename.sof file is clicked, which invokes the Quartus II software.
2. The desired HDL and Implementation code files are added to the Project directory and the top level entity is fixed**.**
3. Start Compilation & Synthesis button are clicked, which compiles and synthesize our **System.**
4. The Bugs (if any) are corrected and the Pin Configurations are assigned, by going through Assignments → Device (Select the specific IC number) and Pins.
5. The Programmer tool is in invoked and the file that needs to be downloaded to the FPGA is selected**.**
6. After successfully downloading the generated system, turn off Reset button, which shows the Encryption & Decryption output of the given input at the coding.

Figure 3.(a) shows the developed system working in the DE1 Development board of Altera Cyclone III FPGA.

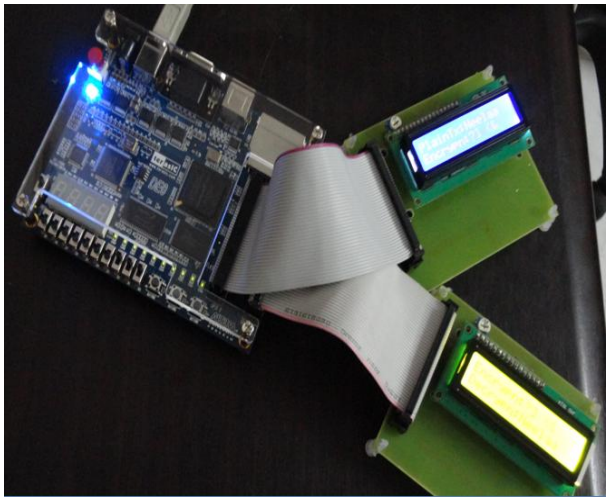

Fig. 3.(a). The Complete System

There are two LCD's used to display the system output. The cipher text for the given plaintext is displayed in LCD-1 as shown in Fig. 3.(b)

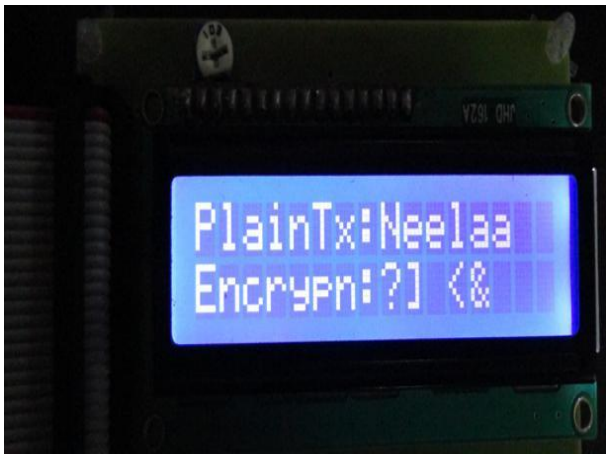

Fig. 3.(b). LCD 1

And the corresponding plaintext for the ciphertext is displayed in the LCD-2, as shown in Fig. 3.(c).

Fig. 3.(c). LCD 2 System Implementation

VII. SYSTEM PERFORMANCE ANALYSIS

Performance analysis is designed to test the run-time performance of software within the context of an integrated system. It is often necessary to measure resource utilization (e.g., execution time, CPU usage etc.,) of the proposed system and compare with an existing system. The area, execution time and power consumption of the proposed system are tabulated as:

ALGORITHM	EXECUTION TIME(MHz)	TOTAL LE	POWER (mW)
SEA	207.08	595	78.28
MD5	36.9	1869	97.54
SHA2	47.42	4095	75.66

TABLE I. PERFORMANCE ANALYSIS

VIII. CONCLUSION

This paper proposed a secure VLSI Crypto system that accelerates computation intensive cryptographic algorithms used by the OpenSSL library for networking security. The result proves that the performances of the cryptographic functions are improved. Therefore, it can be concluded that hardware acceleration improves the performance of cryptography in VLSI crypto-systems.

FUTURE SCOPE

Scopes for further research include low power ASIC implementations of Quantum SSL (QSSL). And the design can be used for a new family of block ciphers, named FOX, developed by the company Media Crypt AG. Also a new design of strong and efficient key-schedule algorithms can be used to accelerate the performance of the Hardware accelerator.

REFERENCES

1. Mohamed Khalil-Hani, Vishnu P., Nambiar M., Marsono N., (2010) "Hardware Acceleration of OpenSSL cryptographic functionsfor high-performance Internet Security"International Conference on Intelligent Systems, Modelling and Simulation.
2. Nambiar V. P., Khalil-Hani M., and Zabidi M. M, *(IJCTS 2009)*, "Accelerating the AES encryption function in OpenSSL for embedded systems," *International Journal of Information and Communication Technology*, vol. 2, no. 1/2, pp. 83–93.
3. Khalil-Hani M., Nazrin M., and Hau Y. W., *(ICED 2008)* "Implementation of SHA-2 hash function for a digital signature System-on-Chip in FPGA," in *International Conference on Electronic Design.*
4. Praveen Kumar B., Ezhumalai P., Ramesh P., Dr SankaraGomathi S., Dr.Sakthivel P., (Febraury 2010), "Improving the Performance of a Scalable Encryption Algorithm (SEA) using FPGA", IJCSNS International Journal of Computer Science and Network Security, VOL. 10 No.2.
5. Maharak C. and Sowanwanichakul B., (in *TENCON 2004)*, "Security methods for Web- based applications on embedded system," *2004 IEEE Region 10 Conference*, vol. C, 2004, pp.56–59 Vol. 3.
6. Colleen E. Garcia, Naval Postgraduate School, Monterey, California, (June 2010) "Regulating nation-state cyber attacks in Counter terrorism operations" – Master Thesis.
7. EkawatHomsirikamol, MarcinRogawski, Kris Gaj, in George Mason University, (2010) "Comparing Hardware Performance of Fourteen Round Two SHA-3 Candidates Using FPGAs" – Master Thesis.
8. Jury: Prof.Y.Willems ,voorzitter in atholiekeuniversiteitleuven, Kasteelpark, Arenberg 10, B–3001 Heverlee, (May 2007), "Analysis and design of symmetric encryption algorithms" - Master Thesis .
9. Pravir Chandra, Matt Messier, John Viega, (June 2002) Publisher : O'ReillyPub Date : ISBN : 0-596-00270. Network Security with OpenSSL..
10. Pascal junod, in EcolePolytechnique, Federale De Lausanne, (2005)"Statistical Cryptanalysis of Block Ciphers" – Master Thesis.
11. Stephen A. Weis in Massachusett Institute of Technology, (May 2006), "New Foundations for Efficient Authentication, Commutative Cryptography, and Private Disjointness TestinG".
12. Saar Drimer in University of Cambridge United Kingdom, (November 2009) "Security for volatile FPGAs" – Master Thesis
13. Wollinger .T, J. Guajardo, C. Paar, (2003) "Cryptography in Embedded Systems: An Overview," in *Proc. of the Embedded World 2003 Exhibition and Conference.*
14. William Stallings 3'rd Edition, Publisher : Pearson Education."Cryptography and Network Security– Principles and Practices".
15. "Hacking Techniques – High Tech Crime Brief" An Article by Australian Institute of Criminology, 2005.
16. "2010 Data Breach Investigations Report" A study conducted by the Verizon Business RISK team in cooperation with the United States Secret Service.
17. www.openssl.org and www.cryptography.org

AUTHORS PROFILE

A. Thriuneelakandan is a Post Graduate in M.E (VLSI DESIGN) from Anna University, Chennai, in the year 2011.He is working as an Assistant Professor in Surya Group of Institutions. He is a Member of IACSIT and IAENG from 2011. His area of interest includes Cyber Security and VLSI Technology.

T.Thirumurugan has received his both the U.G and P.G Degree from Pondicherry University in 1999 and 2002.He is at present working as Assistant Professor (Sr.G) in Surya Group of Institutions..He is a life meber of ISTE and Published 3 International Journals s.