International Journal of Advance Research in Science and Engineering
Vol. No.6, Issue No. 08, August 2017
www.ijarse.com
IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

Data Centric Security in FPGA Based Data Center Using Attribute Based Encryption

J. Joshua Daniel Raj[1], Dr.P . Karthik[2]

[1]*Assistant Professor NHCE, Bangalore (India)*

[2]*Professor , KSSEM, Bangalore (India)*

ABSTRACT

One of the most important concerns about the big data applications is privacy, because users share more personal data and content through their social networking sites and clouds. The security and privacy risks and developing efficient and effective frame works are critical for its success; hence a secure framework such as data centric security is the hot research areas. The Attribute based encryption would be a convenient mechanism to implement data centric security. As the Big data applications require more server computational power, in this paper we propose a novel approach to use FPGA based data centers for implementing both data acceleration which would increase the server computational ability and security mechanisms to achieve data centric security.

Keywords: *FPGA, Attribute based encryption, data center, OpenCL, data acceleration.*

I. INTRODUCTION

Big data is referred to the large set of data that is generated by connected devices and social network sites, which cannot be handled by a traditional database management system. Big Data analytics is the process of analyzing large data sets to dig out hidden patterns, unknown correlation, market trends, customer preferences and other useful business information. The result of analytics can be used for more effective marketing, new revenue opportunities, better customer service, improved operational efficiency and other business benefits. A data center is a place used to keep computer systems and related components such as communications and storage systems. A data analyst who analyses the big data will take large set of data from data center for analyzing. There are, three data analysis related challenges: movement, processing and interacting. The solution to overcome these challenges is hardware data acceleration [7].

With data acceleration organizations can move data from its source to the place of work without losing any of it quickly to extract insights from data and deliver it for processing and storage. Data acceleration supports fast processing of data by using appropriate hardware equipments. Interactivity is about usability of data infrastructure. Data acceleration allows users to connect to datacenters in universally acceptable manner such that results are provided quickly. The FPGA based data acceleration is the solution to data analysis performance challenges.

FPGA accelerated systems has three major benefits: performance, ease-of-use, and lower total cost of ownership. In this paper we presented a proposed implementation of data centric security in FPGA based data centers.

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

II. RELATED WORK

Young-kyu Choi [10] and his team have conducted quantitative analysis and in depth performance on modern FPGA-CPU architectures and they found that that a QPI-based platform has greater advantage on fine-grained (< 4KB) communication latency. Jagath Weerasinghe and Andreas Herkersdorf [11] proposed to decouple the FPGA from the CPU and to connect FPGA directly to the Data Center networks. By connecting the FPGA as standalone component enables large scale deployment of FPGA in cloud computing. A. Putnam [2] and his team at Microsoft have designed a medium scale deployed FPGA based data centers which improved the throughput by twice of Bing search engine.

III. FIELD PROGRAMMABLE GATE ARRAY

A field programmable gate array is a contemporary integrated circuit designed to be used by any type of customers for their applications. The details about the configuration of FPGA are specified using Hardware Description Languages. This sophisticated integrated circuit consists of huge set of resources and memory block to implement complex computational algorithms and it can be used to solve any problem which involves computation. Having confronted with the big data characteristics, there is an interest to use FPGA for the real time application. The data centers are now accelerating their data analytics and computation using FPGA based implementations that could meet the requirements of the big data era. The most widely used FPGA for big data applications is Altera Stratix V and Xilinx Kintex Ultrascale+. The Stratix V FPGA consists of Altera's 28 nm. Stratix® V FPGAs deliver the industry's highest bandwidth, highest level of system integration, and ultimate flexibility with reduced cost and the lowest total power for high-end applications. Kintex® UltraScale+™ devices provide the best price/performance/watt balance in a Fin-FET node, delivering the most cost-effective solution for high-end capabilities including transceiver and memory interface line rates, as well as 100G connectivity cores. Our newest mid-range family is ideal for both packet processing and DSP-intensive functions, and is well suited for applications ranging from wireless MIMO technology to Nx100G networking and data center.

3.1. Programming with FPGAs

Traditionally, hardware developers have designed and verified digital circuits on FPGAs at the register-transfer level (RTL) using hardware description languages (HDLs) such as Verilog HDL and VHDL. While these traditional methods are effective to ensure efficient use of the devices, they are impractical for implementing complex algorithms such as gene sequencing. In early 2012, Altera introduced the Altera SDK for OpenCL, a software development kit that allows use of the OpenCL programming language to program Altera's [1] FPGA as computing accelerator devices. In late 2014 Xilinx Corporation, another leading FPGA vendor, announced they were also developing a compiler for OpenCL. Altera's SDK for OpenCL has been utilized for a wide array of algorithms in a variety of computing fields such as deep learning , CNN algorithms, computer vision algorithm. Etc..

IV. FPGA BASED DATACENTERS

FPGA gives flexible acceleration for many operations. The CPU-FPGA heterogeneous acceleration has great potential for the performance and efficiency improvement for data centers. The FPGA based datacenters are

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

network connected stand alone resource with compute, memory and networking capabilities coupled with CPU.

4.1. Microsoft Catapult

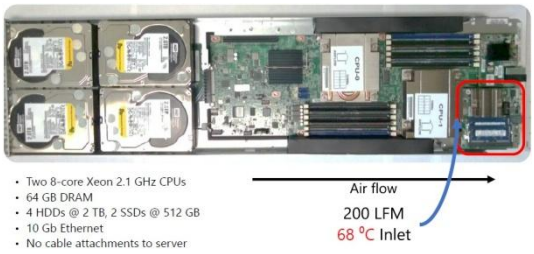

Figure 1: A diagram of the server that hosts the FPGA board.

Catapult is a research project conducted by Microsoft to use FPGAs as data center accelerators to improve performance, reduce power consumption, and provide new capabilities in the datacenter. For this project Microsoft has used Altera Stratix V FPGAs. Using FPGAs, Microsoft has built a kind of super-search machine network.

The system consists of 432 two-socket Intel Xeon-based nodes, each with 64 GB of memory and an Altera Stratix V D5 FPGA with 8 GB of local DDR3 memory. FPGAs communicate to their host CPUs via a PCIe Gen3 x8 connection, providing 8GB/s guaranteed-not-to-exceed bandwidth, and each FPGA can read and write data stored on its host node using this connection [2].

Microsoft has used small daughter boards in each server with a single high end FPGA, and connected the card directly with a secondary network in such a way that would provide low latency, high bandwidth and if an application requires more than one FPGA can be mapped across FPGAs located at multiple servers.Microsoft uses PCI to interface board to the CPU, local DRAM of 8GB.

Microsoft has found that Catapult improves the ranking throughput of each server by a factor of 95%. Microsoft have designed an FPGA board that plugs into the Microsoft-designed server that was released publically as the Open CloudServer V1. It's comprised of 1,632 servers, each one with an Intel Xeon processor and a daughter card that contains the Altera FPGA chip, linked to the Catapault network. The system takes search queries coming from Bing and offloads a lot of the work to the FPGAs, which are custom-programmed for the heavy computational work needed to figure out which webpages results should be displayed in which order. Figure 1 shows the position of the board in one of the datacenter servers.

The system consists of 432 two-socket Intel Xeon-based nodes, each with 64 GB of memory and an Altera Stratix V D5 FPGA with 8 GB of local DDR3 memory. FPGAs communicate to their host CPUs via a PCIe Gen3 x8 connection, providing 8GB/s guaranteed-not-to-exceed and width\ and each FPGA can read and write data stored on its host node using this connection.

V. FABRIC

The Coherent Accelerator Processor Interface is an innovative solution for data acceleration by IBM. It provides high performance solution for the cloud computation algorithms on an FPGA. This can replace application programs running on a dedicated core. CAPI removes overhead and complexity of the input output system, allows an accelerator to operate as part of an application. This requires less programming effort and can be used for wide range of applications [8].

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

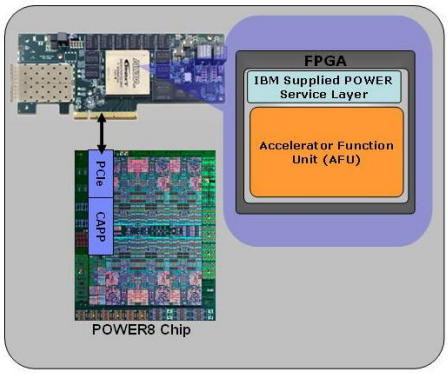

Figure 2: CAPI hardware system

While clouds with FPGAs are available in companies like IBM, there are, however, few FPGA clouds available for public, especially academic, use. To target this problem, we created FAbRIC (FPGA Research Infrastructure Cloud) a project led by Derek Chiou at The University of Texas at Austin. It enables FPGA research and development on large-scale systems by providing FPGA systems, tools, and servers to run tools in a cloud environment. The FAbRIC POWER8+CAPI system consists of a bunch of x86 servers and nine POWER8 servers. The x86 nodes are used as the gateway node, the file server and build machines are used for running FPGA tools. Each POWER8 node is a heterogeneous compute platform. Figure 2 shows the schematic of hardware system and it consists of three accelerating devices, a Nallatech 385 A7 Stratix V FPGA adapter, an Alpha-data 7V3 Virtex7 Xilinx-based FPGA adapter and a NVIDIA Tesla K40m GPU card. FPGA boards are CAPI enabled to provide coherent shared memory between the processor and accelerators.

VI. DATA CENTRIC SECURITY

Data centric security is a method to secure the data itself rather than the security of networks, servers of applications. Data-centric security is the only way to ensure the most important asset of the business—the data—is protected. Data centric protection makes the data unusable to anyone who does not have the key to decrypt it. Encryption is a well suited data-centric technique to address the risk of data theft in smart phones, laptops, desktops and even servers, including the cloud.

VII. ATTRIBUTE BASED ENCRYPTION

Attribute Based Encryption (ABE) [5] is a type of public key encryption in which the secret key of a user and the Cipher text are dependent upon attributes. In ABE the decryption of a Cipher text is possible only if the set of user key attributes of the user key matches the attributes of the cipher text. There are two types ABE Key-Policy Attribute-Based Encryption (KP-ABE) and Cipher text-Policy Attribute-Based Encryption (CP-ABE). In KP-ABE, cipher texts are encrypted with a set of attributes and each user's secret key is mapped with an appropriate policy as shown in figure 3.

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

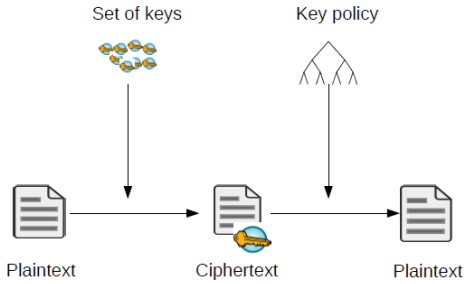

Figure 3: Schematic of KP-ABE

In Cipher text-Policy Attribute-Based Encryption (CP-ABE), the schematic is shown in figure 4. A cipher text is encrypted with a policy. Anyone whose attributes matches the policy can decrypt the cipher text; otherwise the decryption fails. One of the most promising approaches is Cipher text-Policy Attribute-Based Encryption (CP-ABE) [6].

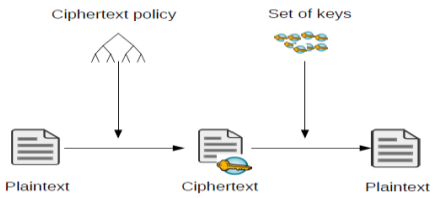

Figure 4: Schematic of CP-ABE

7.1 Proposed implementation of ABE

In this paper figure 5 depicts the proposed implementation to obtain a data centric security by realizing Attribute based encryption in the FPGA based data centers.

Figure 5: Proposed implementation of ABE in FPGA based data center

As the data are being generated at high speed and high volume, it is necessary to use data accelerated data center, for our work, we propose to use FPGA accelerated data centers such as catapult and FAbRIC to implement Attribute Based Encryption to obtain data – centric security.

The construction of cipher text ABE as follows, it consists of four algorithms setup, encryption,

Key generation and Decryption

6.1.1. Setup algorithm

It takes only the hidden parameter as an input and it outputs the public key and a master key. The setup algorithm uses the bilinear group and rando components as input to generate

$$\mathrm{PK} = \mathbb{G}_0, g, h = g^{\beta}, f = g^{1/\beta}, e(g,g)^{\alpha}$$

--- 6. 1

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

public key as shown in equation 6.1 and 6.2.

$MK = (\beta, g^{\alpha})$ -- 6.2

6.1.2. Encryption algorithm

The encryption algorithm is function of PK, M (Message) and A (access structure), and it

--- 6.3

$$\mathrm{CT} = \big(\mathcal{T},\ \tilde{C} = Me(g,g)^{\alpha s},\ C = h^{s},$$
$$\forall y \in Y:\quad C_y = g^{q_y(0)}, C'_y = H(\mathsf{att}(y))^{q_y(0)}\big).$$

generates Cipher text as shown in equation 6.3.

6.1.3. Key generation algorithm

The key generation algorithm will use set of attributes and produces a key SK (secret key) as shown in equation 6.4 .

$$\mathrm{SK} = \big(D = g^{(\alpha+r)/\beta},$$
$$\forall j \in S:\quad D_j = g^{r} \cdot H(j)^{r_j}, D'_j = g^{r_j}\big).$$

-- 6.4

VII. EXPECTED OUTCOME

In the age of big data, the data is being generated at a higher volume and velocity. Hence the security mechanism should be able to encrypt the streaming data without missing anything. For this higher data acceleration and faster encryption methods are essential. The expected timing requirement for the proposed implementation is illustrated in Table in 1.

Operation	**Approximate Time**
Private key gen.	35 ms per attribute
Encryption	27 ms per leaf node
Decryption	0.5–0.8 ms per leaf node

Table 1: Approximate time calculations

As the FPGA is considered for the proposed implementation, it is necessary that the FPGA resource consumption is necessary to be monitored. Table 2 shows the approximate FPGA resource consumption in percentage

Table 2: Approximate estimation of FPGA area consumption

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

Module	Generation of Public key	Encryption	Key generation
Logic (%)	75	85	80
Memory (%)	84	78	96
DSP (%)	85	69	90

VIII. CONCLUSION

This paper is the first ever approach to propose the importance of data centric security in FPGA based data centers. We have proposed that data centric security can be achieved by using Cipher text policy Attribute Based Encryption. We believe that this approach can be implemented in FPGA based data centers to protect the user data at both rest and transmit.

IX. REFERENCES

[1]. Chris Rauer and Nicholas Finamore Jr. *"Accelerating Genomics Research with OpenCL and FPGAs"*, Altera

[2]. A. Putnam et al., *"A reconfigurable fabric for accelerating large-scale datacenter services,"* (ISCA), Page(s):13 – 24, 2014.

[3]. Heiner Giefers ; IBM Research - Zurich ; Raphael Polig ; Christoph Hagleitner, *"Accelerating arithmetic kernels with coherent attacjhed FPGA coprocessors "* Design, Automation & Test in Europe Conference & Exhibition (DATE) , Pages 1072 – 1077, 2015

[4]. Junzuo Lai ; Robert H. Deng ; Chaowen Guan ; Jian Weng*," Attribute-Based Encryption With Verifiable Outsourced Decryption "* IEEE Transactions on Information Forensics and Security (Volume:8 , Issue: 8), Page(s): 1343 – 1354.

[5]. Brent Waters "*Ciphertext-Policy Attribute-Based Encryption: An Expressive, Efficient, and Provably Secure Realization*", Public Key Cryptography – PKC 2011 Volume 6571 of the series Lecture Notes in Computer Science pp 53-70

[6.] T. M. Brewer, *"Instruction set innovations for the convey hc-1 computer,"* IEEE micro, no. 2, pp. 70–79, 2010.

[7]. **"***Data Acceleration: Architecture for the Modern Data Supply Chain*", Accenture.

[8]. J. Stuecheli et al., *"CAPI: A coherent accelerator processor interface,"* IBM Journal of Research and Development, vol. 59, no. 1, pp. 7–1, 2015.

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

[9]. *"Top Ten Big Data Security and Privacy Challenges"* https://cloudsecurityalliance.org/.../top-ten-big-data-security-and-privacy-challenges

[10]. Young-kyu Choi et all "*A quantitative analysis on microarchitectures of modern CPU-FPGA platforms***"** Proceedings of the 53rd Annual Design Automation Conference, Article No. 109 , 2016.

[11]. Jagath Weerasinghe et all *"Enabling FPGAs in Hyper-scale Data Centers"*, IEEE International Conference on Cloud and Big Data Computing , 2015.