Research Results

An Advanced Encryption Standard in FPGA Paradigms

Dr. Ratnesh Kumar Jain[1], Dr. Virendra Singh Chaudhary[2]

[1]*RKDF University, Bhopal, (MP), INDIA*
[2]*RKDF College of Technology and Research, RKDF University, Bhopal, (MP), INDIA*

ABSTRACT

Cloud Computing models a convenient, on-demand network access to a shared pool of configurable computing resources. However, it makes the client data and computation vulnerable to attacks from potential threats as well as from untrusted system administrator. Many trials have been done to address the security concerns in cloud computing but not too much help came around, since using traditional CPU based system, we are unable to fabricate these computing nodes. In this paper, we explored the concept of effectively using FPGAs to engineer a lithe trusted computing platform by generating a smaller attack surface. Moreover FPGAs present a unique practical substitute to imitate the efficient performance within the cloud infrastructure.

KEYWORDS

Cloud computing; security; FPGA; RSA; ECC;

1. INTRODUCTION

Cloud Computing as defined by Brendl (2010) is the "collection of IT resources (servers, databases, and applications) which are available on an on-demand basis, provided by a service company, available through the internet, and provide resource pooling among multiple users". Fig I depicts the cloud computing as a multi-domain environment which highlights the finest quality of software and hardware components. Cloud is one of the best ways for a start-up company to initiate its functioning as it minimizes enormous extent of initial operating cost. But since this service application is in its inception stage, it is facing high criticism and hesitation. From security point of view, Cloud computing is most vulnerable to threats and attacks not only from external world, but also from internal administrators.

Cloud computing is totally a virtually based platform with the data and its processing completely based on virtual machines. The continuously increasing cost of managing IT systems has led many companies to outsource their commercial services to external hosting centres. Cloud computing has emerged as one of the enabling technologies that allow such external hosting efficiently[1]. Berl, et.al,suggests that [2] cloud computing can have significant impact, including:(i) reducing the software and hardware related energy cost of single or federated data centres that execute 'cloud'applications; (ii) reducing energy consumption due to communications.

The Information Technology sector faces a huge demand for services and at the same time building energy expenses [3]. At present Cloud Computing emerges as the unsurpassed way to reduce power utilization and carbon footprint. This has awakened the whole world and motivated to accept the cloud as its best alternative for a green world.

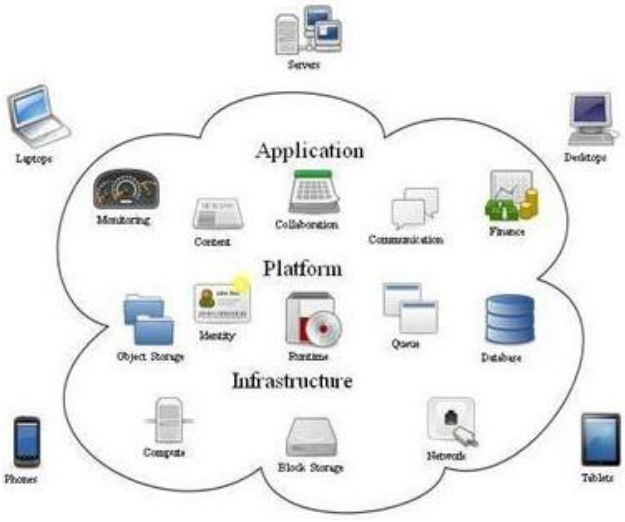

Fig 1 Cloud Computing

The Cloud Computing is a developing archetype with marvellous momentum, but its exceptional aspects are worsening the security and privacy challenges. Cloud computing is continuously evolving and there are several major cloud computing providers such as Amazon, Google, Microsoft, Yahoo and several others who are providing services such as Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS), Storage-as-a-Service and Infrastructure-as-a-Service (IaaS). Fig 2 highlights the different types of cloud deployment available in the market today. . Table 1 shows the pay per use competitive matrix of some of the major cloud computing providers for infrastructure as a service (IaaS), platform as a service (PaaS)[4]. Cloud computing is a

combination of several key technologies that have evolved and matured over the years (see Figure 3.) It is often criticized despite its huge benefits due to data segregation, availability and confidentiality of clients data, maintained by third party. Though cloud computing provides flexible choices through different types of cloud, and does not pressurize the organization to invest in operational costs since no physical servers are included, yet attack such as XML Signature element wrapping attack, Null Prefix attack, etc., compromise the data of cloud computing management and confidentiality of clients data, maintained bythird party vendors, put at high stake[5].

Fig 2 Different types of cloud deployment (AcuteSys, 2011)

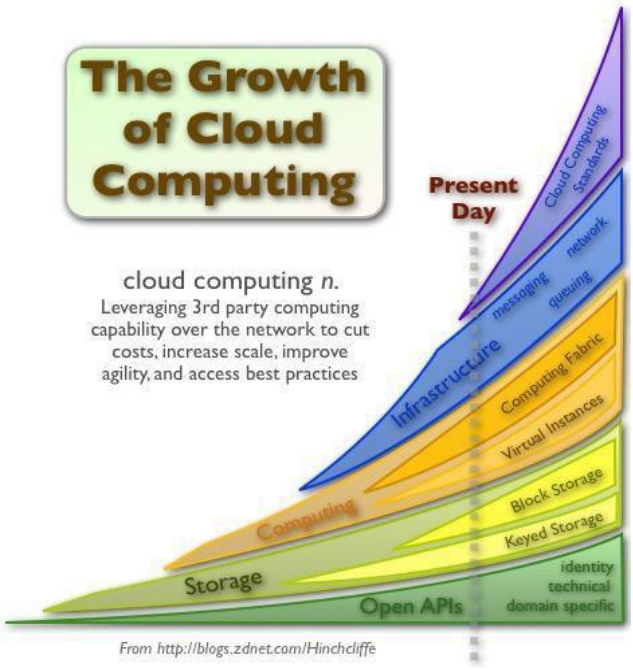

Fig 3. The growth of Cloud Computing. (Hinchcliffe, 2009)

2. SECURITY IN THE CLOUD

Cloud security issues and the risks of cloud computing are one of the biggest barriers to adopt cloud/grid services. Understanding the security and privacy risks in cloud computing and developing efficient and effective solutions are critical for its success. Heightened security threats must be overcome in order to benefit fully from this new computing paradigm [6]. With the cloud model control physical security is lost because of sharing computing resources with other companies. Company has violated the law (risk of data seizure by (foreign) government). Storage services provided by one cloud vendor may be incompatible with another vendor's services if user decides to move from one to the other (e.g. Microsoft cloud is incompatible with Google cloud). Who controls the encryption/ decryption keys? Logically it should be the customer. Ensuring the integrity of the data (transfer, storage, and retrieval) really means that it changes only in response to authorized transactions. A common standard to ensure data integrity does not yet exist. In case of Payment Card Industry Data Security Standard (PCI DSS) data logs must be provided to security managers and regulators. Users must keep up to date with application improvements to be sure they are protected. Some government regulations have strict limits on what data about its citizens can be stored and for how long, and some banking regulators require that customer's financial data remain in their home country. The dynamic and fluid nature of virtual machines will make it difficult to maintain the consistency of security and ensure the audit ability of records. Customers may be able to sue cloud service providers if their privacy rights are violated, and in any case the cloud service providers may face damage to their reputation. Concerns arise when it is not clear to individuals why their personal information is requested or how it will be used or passed on to other parties.

Table I

Competitive Matrix. (Cloudtweaks, 2010) Diagrams

Provider	IaaS	PaaS	Compute Billing Model	Storage Billing Model	Relational Database Service	Hybrid capabilities
Windows Azure	No	Yes (.Note, Java, Ruby, Python, PHP)	Pay-per-use	Pay-per-use	Yes (SQL Server)	Yes (on-premise to cloud)
Amazon Web Services	Yes	No	Pay-per-use	Pay-per-use	Yes (MySQL-based)	Yes (via third-party tools)
Rackspace	Yes	Yes (LAMP, .Net (PaaS)	Pay-per-use (IaaS); Monthly (PaaS)	Pay-per-use (IaaS); Included in monthly fee (PaaS)	Yes (FathomDB)	No (but dedicated resources to cloud planned)
Joyent	Yes	Yes (Java, Ruby, Python, PHP)	Monthly (IaaS); PaaS pricing not announced	Included in monthly fee (IaaS)	No	Yes (on-primise to cloud)
Google	No	Yes (Python, Java)	Pay-per-use	Pay-per-use	No	No
GoGrid	Yes	No	Pay-per-use or pre-paid	Included with each instance	No	Yes (dedicated resources to cloud)

Cloud as one would expect puts the machines to a huge number of latent viruses and various malwares owing to its access-from anywhere and high-scale load balancing philosophies. Thus the clients' community must be ensured about the security and privacy of their data. Moreover they must take proactive measures to initially run applications and data transfer in their own private cloud and then transmit it into public cloud. Also, the cloud vendor must be geared up with proper certifications and proper assessment to decrease their risk. A Cloud Security Alliance in order to curtail hazards should design pertinent standards soon. A case may arise where somehow due to some unintentional reason a client's data is leaked; in this scenario the whole allegation comes on the head of these cloud vendors, may be on the virtual machines or may be on any of the administration staff, and nobody can attest its innocence. In this paper we try to prevent this kind of situation from happening by taking the help of FPGAs. In a rather smaller but much effective platform, FPGAs aid us in building a defensive system that can verify various forms of attacks, much better than showcased by the software versions.

The security concerns surrounding the visibility of sensitive

data and the integrity of sensitive computations to attackers can be alleviated by offering trusted compute resources within the cloud [7]. The motivation of the paper is to provide the cloud customers a security protocol as an addendum with the Service Level Agreement (SLA). This will assure the clients with the certainty that their data is safe and secure with the cloud vendors, and there will not be any eves dropping with their data. For service providers to offer SLA with security features, they need to follow the general procedure of cryptography, which includes storing a key, decrypting and authenticating the data and performing processes needed to authenticate the data.

Software-based models do not have the flexibility to check the attack models, as is feasible in hardware-based system. FPGAs save the reliance on physical memory space requirement in the case of software based models. In case of FPGAS, the Look- up-tables, Flip Flops do the major job of the memory. Moreover, concurrent processing of data is quite efficiently performed in the case of FPGAs, hence non-dependence on OS.

The work in [8] implements a full system, including a processor and a TPM inside an FPGA. It focuses on bringing the full suite of TPM functionality to a soft processor running on the FPGA. As seen in fig 5, the device processing on the clients data can securely be decrypted, execute the necessary operation, without loss of data, and without the interference of the system administrator or any other eves dropper. Following the homomorphic encryption suggested in [9], Ken Eguro and Ramarathnam Venkatesan proposed the work in [7].

3. RELATEDWORK

The proposed FPGA system infrastructure and user application in paper [7] implements homomorphic encryption of AES, SHA and RSA in a pattern. We propose a pattern wherein we use AES, RSA and ECC which will be a better way of dealing with the security issues referring the strength of attacks that may hamper a client's data on the cloud computing vendor's side. The methodical concept is described in Fig 4, which is a alternative approach to the method described in the work proposed by Ken and Ramarathnam [7]. The weakness of RSA encryption and decryption are attuned with the presence of ECC encryption and decryption and a strong cryptographic algorithm comes into play[10]. An AES core is independently sufficient to authenticate and encrypt any data with its 128, 192 or 256 bit sized keys, rounded by S- Box and can decrypt the original forwarded data without any loss or interference from any unwanted source. Apt security of data from client side is of utmost priority for the cloud providers, so that no tampering with those is endorsed. In a virtual environment any block of data is vulnerable to numerous spasms. To verify the authenticity of any security pattern we need to set up an environment which is analogous to the virtual world created by the cloud computing paradigm.

FPGAs create a strong computing platform with the help of which we can thoroughly test the efficiency of various cryptographic patterns to protect the vulnerable and valuable data blocks from being fiddled. In this paper we have taken a few FPGA kits to demonstrate the cryptographic pattern we described earlier. VHDL codes of RSA, ECC and AES cryptographic algorithm are coded and implemented individually on these platforms. Most modern FPGA blocks have onboard memory which can be written from an external port. This key memory can be over-written externally, but cannot be read otherwise. Hence the key plays a major role and has to be copied to the FPGA in a non-vulnerable site. This FPGA can then be installed in a PCI express slot in a server of the clod providers virtual machines.

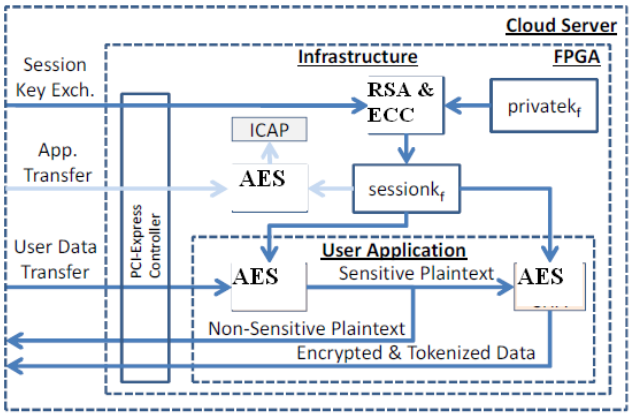

Fig. 4 FPGA System Infrastructure and user application

A proof-of-concept shown in Fig.5, depicts the bootstrapping binary. It shows a PCI Express which is a controller used to link the FPGA with the host server. Moreover an RSA/ECC core is implemented to settle a symmetric session key trade with clients, and an AES core to decrypt and authenticate communication with clients. Thereafter, when the client ascertains a secure session to a device that supports their computation, they can send sensitive input data from their local machine (encrypting with the session key) and either receive output data back in their local machine or on cloud machines.

4. RESULTS

The proof-of-concept has been prototyped using various FPGAs. Table II shows the logic and memory utilization of the various cryptographic algorithm in different FPGAs. The resource allocation is less than expected, and can be compared with their prior implementations in other works. Hence if implemented by the cloud providers can save a lot in infrastructure. Table III also shows the area and frequency requirement of the individual algorithms when implemented in various FPGAs.

Table II

Resource Utilization

ALG.	FPGA	LUT	FF	Slices
AES	SPARTAN3 E xc3s500e- fg320	425345%	4534%	222647%
AES	VIRTEX2P Xq2vp70- 5ff1704	42846%	4510%	22356%
RSA & ECC	VIRTEX2P Xq2vp70- 5ff1704	31562%	3135	14290

Table III

Resource Utilization

ALG.	Bond IOBs	GClK	Freq (MHz)	Area
AES	239%	28%	41.5	-
AES	232%	212%	43.5	-
RSA & ECC			44.91	776K Gate

5. CONCLUSIONS

Cloud computing is a combination of several key technologies that have evolved and matured over the years. Cloud computing has a potential for cost savings to the enterprises but the security risk are also enormous. We have argued that it is very important to take security and privacy into account when designing and using cloud services. In this paper security in cloud computing was elaborated in a way that covers security issues and challenges, security standards and security management models. There is no doubt that the cloud computing is the development trend in the future. Cloud computing brings us the approximately infinite computing capability, good scalability, service on-demand and so on, also challenges at security, privacy, legal issues and so on. To welcome the coming cloud computing era, solving the existing issues becomes utmost urgent.

This paper talks about the concept of FPGAs as a trusted platform for cloud services. Though the real world scenario of using these cryptographic algorithms in these patterns may not be effectively acceptable, yet FPGAs provide a better alternative to emulate the successful performance of a cloud computing platform in such software and hardware based model.

REFERENCES

[1]. Abdelsalam,H., Maly, K., Mukkamala,R., Zubair, M., & Kaminsky, D. (2009). Towards energy efficient change management in a cloud computing environment. In Proceedings of the 3rd International Conference on Autonomous Infrastructure, Management and Security: Scalability of Networks and Services (AIMS '09), Ramin Sadre and Aiko Pras (Eds.). Springer-Verlag, Berlin, Heidelberg, 161-166. DOI=10.1007/978-3-642-02627-0_13

[2]. Berl, A., Gelenbe, E., Di Girolamo, M., Giuliani, G., De Meer, H., Dang, M., & Pentikousis, K. (2009). Energy-efficient cloud computing. The Computer Journal, 53(7), 1045-1051.

[3]. Jason James. The Potential for Cloud Computing to Lower Power Consumption and Reduce Carbon Emissions, MSc Thesis, University of Oregon Applied Information Management Program.

[4]. Anthony Bisong and Syed (Shawon) M. Rahman. An overview of the security concerns in Enterprise cloud computing, International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.1, January 2011.

[5]. Harish Vepuri, Moshin Rahman., Implications of cloud computing in it organizations master thesis 2011 Informatics

[6]. Krešimir Popović, Željko Hocenski, Cloud computing security issues and challenges, MIPRO 2010, May 24-28, 2010, Opatija, Croatia

[7]. Ken Eguro, Ramarathnam Venkatesan, "FPGAs for Trusted Cloud Computing," IEEE International Coference on Field-Programmable Logic and Applications.

[8]. T. Eisenbarth, T. Guneysu, C. Parr, A. Sadeghi, D. Schellenkens, and

[9]. M. Wolf, "Reconfigurable Trusted Computing in Hardware," ACM Conference on Computer and Communications Security, 2007.

[10]. Vinod Vaikuntanathan, Computing Blindfolded: New Developments in Fully Homomorphic Encryption, 2011 52nd Annual IEEE Symposium on Foundations of Computer Science

[11]. Yi Wang, Douglas L. Maskell, Jussipekka Leiwo A unified architecture for a public key cryptographic coprocessor, Journal of Systems Architecture 54 (2008) 1004–1016.