CLOUD SECURITY AND DIGITAL SIGNATUREA ROAD MAP

[1]Dhina Suresh, [2]Dr.M.Lilly Florence

[1]Research Scholar, Department of Computer Science,
St. Joseph's College of Arts and Science for Women, Hosur, Tamilnadu, (India).
[2]Professor, Department of Computer Application,
Adhiyamaan College of Engineering,Hosur, Tamilnadu, (India)

ABSTRACT

The use of cloud computing is rapidly increasing now a days. Cloud is an internet based service delivery model which provides internet based services, computing and storage for users in all market including financial, health care, government and so on. Cloud is a model where user is provided services by CSP (Cloud Service Provider).There are also disadvantages with cloud computing mainly with the security concern. Especially data security and privacy protection issues remain the primary problem in cloud computing services. It is required to protect the stored data and applications in clouds from hackers and intruders. Cryptography is an essential tool that helps to assure our data storage and accuracy in cloud environment. There are different types of cryptographic algorithms. This article briefly discusses on the basics of cloud, security issues associated with cloud and it briefly explains the existing cryptographic algorithms that can be used to improve the security in cloud environment. Finally, this paper describes about the basic mechanism of digital signature and encryption.

Keywords: Cloud Security, Cipher Text, Cryptographic Techniques, Data Security, Privacy Protection, Virtualization.

I. INTRODUCTION

Cloud is where user is provided services by CSP (Cloud Service Provider) and we will be surrendering all our sensitive information to the third-party cloud service provider. It is difficult to control the data in cloud. Cloud service providers must ensure the privacy of the data by protecting them from unauthorized access. The cloud has different services. There are also different cloud models with which the individual or industry can be benefited. It is accepted that cloud has many advantages one of which is virtualization. Virtualization in all of its forms is a pillar of Cloud Computing. Virtualization refers to the creation of a virtual (not physically existing but made to appear) resource such as a server, desktop, operating system, file, storage or network. It is the key technique in cloud architectures because it allows greater flexibility and utilization of cloud. The most important concern is to guarantee that data integrity and confidentiality is attained while data is stored in the cloud. There are many cloud providers such as Google, Amazon, Microsoft and many. The vital issue in the cloud is that of security. Security in cloud can be enhanced by implementing cryptography. The concept of cryptography is the user has to encrypt the data before he stores or uploads the data in the cloud so that the data remains secure from invaders. Encryption can be defined as the conversion of data may be text, video so on during transmission or storage into another form called cipher text. The cipher text cannot be easily understood by anyone except authorized parties. Decryption is the reverse process of getting back the original data from the encrypted data / cipher text. Decryption restores the original data. To explain the concept of security encryption techniques are explained. The main aim of this paper is to explain the security in cloud and give a brief overview of digital signature.

II. TYPES OF CLOUD BASED ON SERVICE

2.1. Software-As-A-Service (Applications, processes and information)

With SaaS, a provider licenses an application to customers either as a service on demand in a "pay-as-you-go" model, or at no charge. SaaS is a rapidly growing market.

Some defining characteristics of SaaS include[1]

- Web access to commercial software.
- Software is managed from a central location.
- Software delivered in a "one to many" model.
- Users not required to hayndle software upgrades and patches.
- Application Programming Interfaces (APIs) provide integration between different pieces of software

Software as a Service may be the best known aspect of Cloud Computing, but developers and organizations all around the world are leveraging [1] Platform as a Service, which mixes the simplicity of SaaS with the power of IaaS, to great effect.

2.2. Platform-As-A-Service (Virtualized middleware)

Platform as a Service (PaaS) is mainly used for application development. PaaS is analogous to SaaS except that, rather than being software delivered over the web, it is a platform for the creation of software, delivered over the web. Developer's gaina framework with PaaS[1] to develop or customize applications. PaaS makes the development, testing, and deployment of applications quick, simple, and cost-effective. With this technology a third-party provider, can manage OSes, virtualization, servers, storage, networking, and the PaaS software itself. Developers, however, manage the applications. It allows the creation of web applications quickly and easily and without the complexity of buying and maintaining the software.

Some defining characteristics of PaaS include[1]

- Services to develop, test, deploy, host and maintain applications in the same integrated development environment. All the varying services needed to fulfill the application development process.
- Web based user interface creation tools help to create, modify, test and deploy different UI scenarios.
- Multi-tenant architecture where multiple concurrent users utilize the same development application.
- Built in scalability of deployed software including load balancing and failover.
- Integration with web services and databases via common standards.
- Support for development team collaboration – some PaaS solutions includes project planning and communication tools.
- Tools to handle billing and subscription management.

2.3. Infrastructure-As-A-Service (Virtualized servers, storage, networks)

Infrastructure as a Service (IaaS)[1] is a way of delivering Cloud Computing infrastructure – servers, storage, network and operating systems – as an on-demand service.Rather than purchasing servers, software, datacenter space or network equipment, clients instead buy those resources as a fully outsourced service on demand.

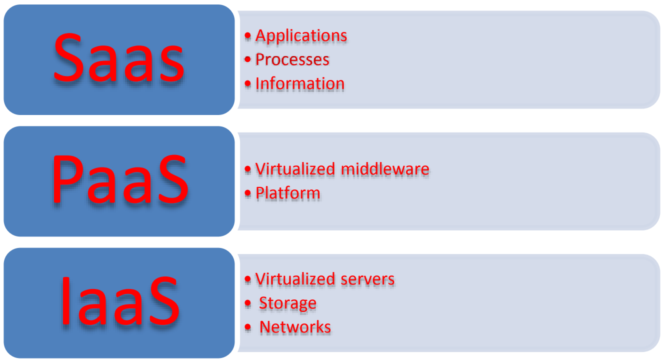


Figure 1: Cloud Service Models

Generally IaaS can be obtained as public or private infrastructure or a combination of the two. “Public cloud” is considered infrastructure that consists of shared resources, deployed on a self-service basis over the Internet. By contrast, “private cloud” is infrastructure that emulates some of cloud computing features, like virtualization, but does so on a private network. Additionally, some hosting providers are beginning to offer a combination of public and/ or private cloud networks. This combination approach is generally called “Hybrid Cloud”.

Some defining characteristics of IaaS include[1]

- Resources are distributed as a service.
- Allows for dynamic scaling.
- Has a variable cost, utility pricing model.
- Generally includes multiple users on a single piece of hardware.

III. TYPES OF CLOUD BASED ON LOCATION

3.1. Public Cloud

In Public cloud the computing infrastructure[3] is hosted by the cloud vendor at the vendor premises. The customer has no visibility and control over where the computing infrastructure is hosted. The computing infrastructure is shared between any organizations.

3.2. Private Cloud

The computing infrastructure is dedicated to a particular organization and not shared with other organizations. Private clouds are more expensive and more secure when compared to public clouds. Private clouds are of two types: on-premise private clouds and externally hosted private clouds. Externally hosted private clouds are also exclusively used by one organization,[3] but are hosted by a third party specializing in cloud infrastructure. Externally hosted private clouds are cheaper than on-premise private clouds.

3.3. Hybrid Cloud

Organizations may host critical applications on private clouds and applications with relatively less security [3] concerns on the public cloud. The usage of both private and public clouds together is called hybrid cloud.

3.4. Community Cloud

Involves sharing of [3] computing infrastructure in between organizations of the same community. For example all Government organizations within the state may share computing infrastructure on the cloud to manage data.

IV. CLOUD COMPUTNG ADVANTAGES

4.1. Cost Efficient

Cloud computing is probably the most cost efficient method to use, maintain and upgrade. The cloud, on the other hand, is available at much cheaper rates.

4.2. Almost Unlimited Storage and Scalability

Storing information in the cloud gives you almost unlimited storage capacity. With the cloud, you basically have access to unlimited storage capability and scalability.

4.3. Mobility

You can have your cloud, anywhere.

4.4. Backup and Recovery

Since all your data is stored in the cloud, backing it up and restoring the same is relatively much easier than storing the same on a physical device.

4.5. Automatic Software Integration

In the cloud, software integration is usually something that occurs automatically. We need not take any effort.

4.6. Easy Access to Information

Once you register yourself in the cloud, you can access the information from anywhere, where there is an Internet connection.

4.7. Quick Deployment

Lastly and most importantly, cloud computing gives you the advantage of quick and easy deployment.

V. CLOUD COMPUTNG DISADVANTAGES

5.1. Technical Issues

Though it is true that information and data on the cloud can be accessed [2] anytime and from anywhere, you will need a very good Internet connection to be logged onto the server at all times and also be stuck in case of network and connectivity problems.

5.2. Dependency

Dependency is one of the major drawback of Cloud computing. This is known as "vendor-lock-in" as it difficult to migrate from one Cloud vendor to another because of the huge data migration. This risk may also harm the security and privacy of the data.

5.3. Limited Control

Since all the services run [2] on a remote virtual environment, the service consumer has less control over the hardware and the software.

5.4. Security in the Cloud

The major issue in the cloud is the security issues. [2] Security issues in cloud are a major obstacle. Security issues can be grouped into sensitive data access, data segregation, privacy, bug exploitation, recovery, accountability, malicious insiders, management console security, account control, and multi-tenancy issues. There are wide ranges of encryption algorithms at the cutting edge which have been proved to be securing that can be used to perform encryption/decryption operations.

VI. ENCRYPTION ALGORITHMS REVIEW

6.1. What is encryption? Why it is important?

The usage of encryption as a technique to the data guarantees the confidentiality of data and helps to detect any corruption in data. [12] When the user wants to store data on an un-trusted resource he encrypts the data at a point (it may be either the user's machine or within the trusted environment) then the encrypted data is sent to the storage service and also the keys are stored on the key store. The key store can be either on a portable device (an USB pen-drive) owned by the user or in a specialized server which is somewhere in the trusted environment. Modern encryption algorithms play a vital role as they can provide confidentiality.

The following are key elements of security.

6.1.1. Authentication

The origin of a message can be verified.

6.1.2.Integrity

Proof that the contents of a message have not been changed since it was sent.

6.1.3. Non-repudiation

The sender of a message cannot deny sending the message.

VII. BRIEF STUDY OF EXISTING ENCRYPTION ALGORITHMS

To provide secure communication over the network, [12] encryption algorithm plays a vital role. It is the fundamental tool for protecting the data. Encryption algorithm converts the data into scrambled form by using “the key”. Basically there are two types of encryption.

7.1. Symmetric Encryption

In symmetric key encryption, [11] only one key is used for both encryption & decryption. The key is kept secret. The main advantage of this type is it has less computing time and high speed. Other terms for symmetric key encryption are secret key, single key, and shared key, one key and eventually private key encryption. DES, 3DES, AES and RC4 are the commonly [11] used symmetric key algorithms. 3DES and AES are commonly used in IP security and other types of virtual private networks. RC4 have seen wide deployment on wireless networks. A very simple example of how a secret key algorithm might work might be substituting the letter in the alphabet prior to the target letter for each one in a message. The resulting text - "gdkkn," would make no sense to someone who didn't know the algorithm used (x-1), but would be easily understood by the parties involved in the exchange as "hello."The problem with secret or symmetric keys is how to securely get the secret keys to each end of the exchange and keep them secure after that.

7.1.1. Key Management in Symmetric Key Encryption

In order to ensure secure communications between everyone in a group of n people a total of n(n - 1)/2 keys are needed, which is the total number of possible communication channels. For security it is required that the keys should be changed regularly and kept secure during distribution and in service [11].

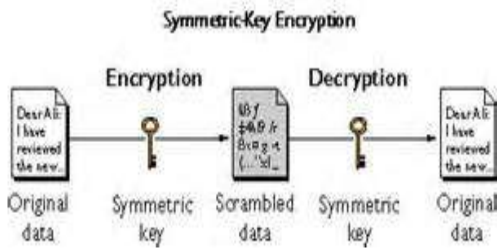


Figure 2: Symmetric Encryption

The process of selecting, distributing and storing keys is known as key management, and is difficult to achieve reliably and securely.

7.1.2. Two Types of Symmetric Key Encryption

7.1.2.1. Block Cipher Symmetric Key Encryption

In block cipher the input is taken as a block of plaintext of fixed size. The key is applied to the block of plain text and a block of cipher text is obtained. Blocks of 64 bits have been commonly butmodern techniques use 128-bit blocks. [11]DES has a block size of 64 bits and AES has a block size of 128 bits. Blowfish algorithm is also a type of block cipher.

7.1.2.2. Stream Cipher Symmetric Key Encryption

In stream cipher one bit is encrypted at a time and so it is time consuming. RC4 is an example of stream cipher.

7.2. Asymmetric Encryption

It is also called as public key encryption.[12]It uses two keys , a public key known to everyone and a private or secret key known only to the recipient of the message. Although two keys are different the two parts of this key pair are mathematically linked. The public key is used to encrypt plain text or to verify a digital signature whereas the private key is used to decrypt cipher text or to create a digital signature. The first asymmetric key encryption was found in 1976 called Diffie Hellman algorithm.

Public key encryption is pretty good and popular for transmitting information via theInternet. They are extremely secure and relatively simple to use. The only difficulty with public-key systems is that you need to know the recipient's public key to encrypt a message for him or her. Therefore global registry of public keys is required.

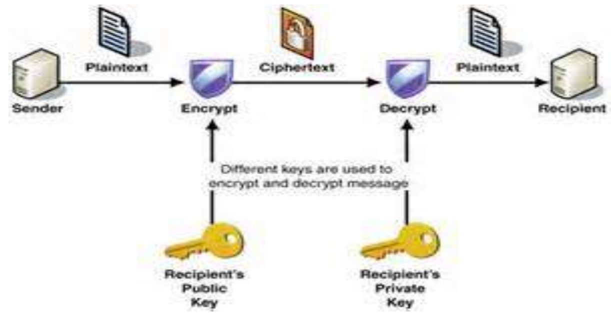


Figure 3: Asymmetric Encryption

Some public key algorithms [11]provide key distribution and secrecy e.g., Diffie–Hellman key exchangesome provide digital signatures e.g., Digital Signature Algorithmand some provide both e.g., RSA.

VIII. DIGITAL SIGNATURE & ENCRYPTION

8.1. Encryption and Decryption

Encryption [11] is a mechanism by which message is transformed so that only the sender and recipient can see. A simple example is when Rose wants to send a secure message to John, she uses John's public key to encrypt the message. John then uses his private key to decrypt it.

Rose sends a secret msg to John by encrypting the message with John’s public key [message] PuKJohn

[Message]PuKJohn

John receives the encrypted msg from Rose. In order to decrypt it John uses his own private key[message] PrKJohn

Encryption/Decryption

8.2. Digital Signature and Verification

Digital signature [5] is a mechanism by which a message is authenticated. It is proved that a message is effectively coming from a given sender, much like a signature on a paper document. A digital signature[13] is most often a message digest encrypted with someone's private key to certify the contents. This process of encryption is called signing.

8.2.1. Hashing

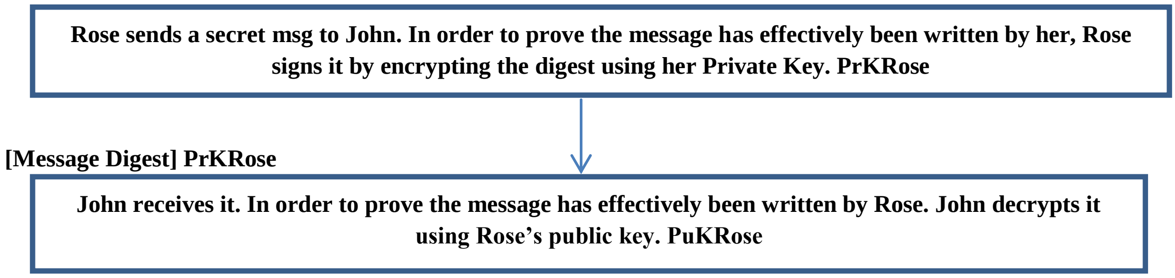
Hashing is the transformation of a string of characters into a shorter fixed-length numeric value or key called message digest.

8.2.2. Hash Function

The hash function is used to index the original value or key and then used later each time the data associated with the value or key is to be retrieved. Thus, hashing is always a one-way operation. Hash functions MD2, MD4, and MD5, used for hashing digital signatures into a shorter value called a message-digest, and the Secure Hash Algorithm (SHA), a standard algorithm, that makes a larger (60-bit) message digest and is similar to MD4.

8.2.3. Message Digest

A digest [5] takes a plain text and generates a hash code which can be used to verify if the plain text is unmodified but it cannot be used to decrypt the original text form the hash value.



Rose sends a secret msg to John. In order to prove the message has effectively been written by her, Rose signs it by encrypting the digest using her Private Key. PrKRose

[Message Digest] PrKRose

John receives it. In order to prove the message has effectively been written by Rose. John decrypts it using Rose's public key. PuKRose

Digital Signature/Verification

IX.DIGITAL SIGNATURE WITH ENCRYPTION AND DECRYPTION EXAMPLE

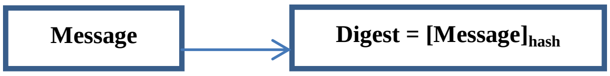
In the following example we are going to create a digital signature and encrypt a message. We have to first sign then encrypt [5] only then the receiver can decrypt and then verify. If we encrypt then sign then anybody can verify the authenticity but only receiver can decrypt it.

9.1. Digital Signature Process

Digital signature includes two steps

9.1.1 Message Digest evaluation.

- Rose wants to send a message to John.
  E.g. Hello how are you
- Rose wants to make sure that John knows that the message is sent only by her.
- Rose creates a message digest and signs it.
- To create a message digest, Rose uses a cryptographic hash function (let's consider MD4).



Message

Digest = [Message]$_{hash}$

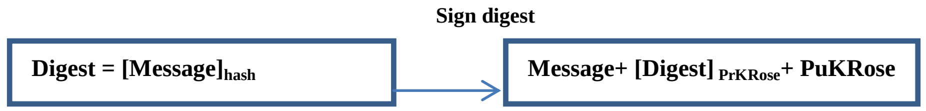
Calculate digest

- The message is now converted into an ID number. This is called as message digest.

9.1.2. Digest signature

A signature is in fact an encryption of the message digest using the sender's private-key.

- Now to sign the digest, Rose needs a secret private key (let's consider RSA) that no one else knows. Rose has now created a private key and she has signed the digest.
- To verify that only Rose has signed it, she needs to publish her public key so that it is available to everyone.
- Using her private key, Rose signs the digest. The combination of her message and his signature is obtained.


Sign digest
Digest = $[\text{Message}]_{hash}$
Message+ $[\text{Digest}]_{PrKRose}$+ PuKRose

9.2. Encryption Process

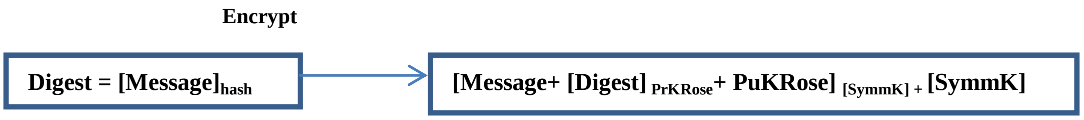
Encryption includes the following steps

9.2.1. Encrypting the Message and the Digest

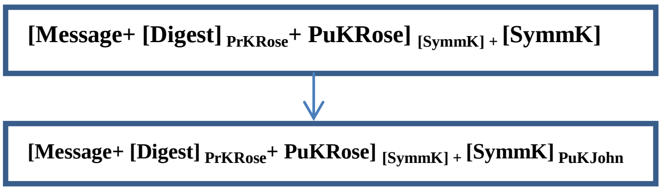
- A onetime symmetric key is created. Symmetric keys are also efficient. So the symmetric key here is same for both Rose and John.

Create a Symmetric Key [SymmK]

- The whole message with the digest is encrypted with the onetime symmetric key.


Encrypt
Digest = $[\text{Message}]_{hash}$
$[\text{Message+ } [\text{Digest}]_{PrKRose} \text{+ PuKRose}]_{[SymmK]\,+}$ [SymmK]

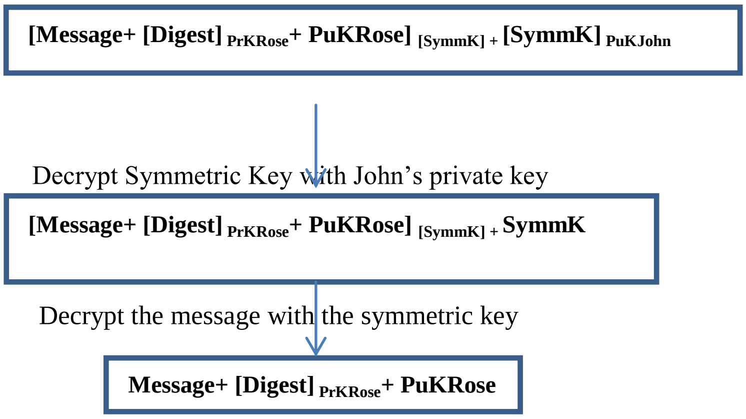
- Since the same Symmetric key is used to decrypt the message, anyone can decrypt the message. They can use Rose's public key to verify that Rose created the message. ButRosewill want onlyJohn to read and verify her message. To accomplish this, Rose needs to use John's public key to encrypt the symmetric key.


$[\text{Message+ } [\text{Digest}]_{PrKRose} \text{+ PuKRose}]_{[SymmK]\,+}$ [SymmK]
$[\text{Message+ } [\text{Digest}]_{PrKRose} \text{+ PuKRose}]_{[SymmK]\,+}$ $[\text{SymmK}]_{PuKJohn}$

- Rose uses John's public key and encryptedthe symmetric key.This ensures that only John who has his private key can read the message,because Rose signature [5] is part of the message. John will know that the message came from her.

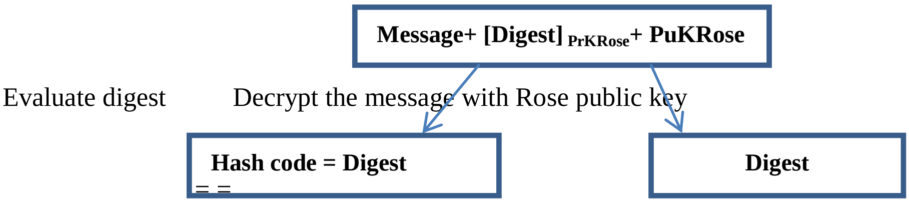
9.3. Decryption Process

- To reverse this process, John uses his private key to decrypt the symmetric key. Using the symmetric key John decrypts the message.


[Message+ [Digest]$_{\text{PrKRose}}$+ PuKRose]$_{\text{[SymmK] +}}$ [SymmK]$_{\text{PuKJohn}}$
Decrypt Symmetric Key with John's private key
[Message+ [Digest]$_{\text{PrKRose}}$+ PuKRose]$_{\text{[SymmK] +}}$ SymmK
Decrypt the message with the symmetric key
Message+ [Digest]$_{\text{PrKRose}}$+ PuKRose

After the message is decrypted the following processes takes place.

- Evaluate the digest [13] with the same hashing algorithm.
- Decrypt the digest with Rose's public key which is in the message.


Message+ [Digest]$_{\text{PrKRose}}$+ PuKRose
Evaluate digest
Decrypt the message with Rose public key
Hash code = Digest
= =
Digest

- Check if both are same. If both are same the message [13] is decrypted and the signature is verified.

X. CONCLUSION

In this paper much of the work has been focused on the basics of cloud. It gives brief study on the basics of existing encryption techniques and an overview of digital signature. This review shows the process involved in digital signature and encryption. Although cloud computing has many advantages, there are still many actual problems yet to be solved.

XI. ACKNOWLEDGEMENT

I would like to thank THE LORD MY SAVIOUR for guiding and showering HIS blessings throughout my life. I take immense pleasure in thanking my guide Dr. M. Lilly Florence for rendering her valuable knowledge and guidance. I would like to thank my husband for his love and support. I would like to thank my parents and my son for their patience and care.

REFERENCES

[1]UNDERSTANDING the Cloud Computing Stack SaaS, Paas, IaaS, © Diversity Limited, 2011 Non-commercial reuse with attribution permitted.

[2] Tripathi, A.; Mishra, A.; IT Div., Gorakhpur Centre, Gorakhpur, India "Cloud Computing Security Considerations", Signal Processing, Communications and Computing (ICSPCC), 2011 IEEE International Conference.

[3] Peter Mell, and Tim Grance, "The NIST Definition of Cloud Computing,"Version15,10-7-09, http://www.wheresmyserver.co.nz/storage/media/faq-files/cloud-def-v15.pdf.

[4] Laura Smith on " A health care community cloud takes shape" http://searchcio.techtarget.com/news/2240026119/a-health-care-community-cloud-takes-shape

[5]National Institute of Standards and Technology (NIST), Digital Signature Standard, FIPS PUB 186-2, http://csrc.nist.gov/publications/fips/fips186-2/fips186-2.pdf

[6] "Sampling issues we are addressing", http://cloudsecurityalliance.org/issues.html#15, accessed on April 09, 2009.

[7] "Cloud security alliance: Security guidance for critical areas of focus in cloud computing v2.1," Dec 2009. Available at: www.cloudsecurityalliance.org.

[8]Cetin Kaya Koc, "RSA Hardware Implementation", RSA Laboratories, RSA Data Security, Inc., on line available http://security.ece.orst.edu/koc/ece575/rsalabs/tr-801.pdf

[9] A. F. Webster, Stafford Tavares, "On the Design of S-Boxes," *CRYPTO'85* (1985).

[10] Sriram Ramanujam and Marimuthu Karuppiah "Designing an algorithm with high Avalanche Effect" IJCSNS International Journal of Computer Science and Network Security, VOL.11 No.1, January 2011

[11]Yogesh Kumar, Rajiv Munjal, "comparison ofsymmetric and asymmetric cryptography withexisting vulnerabilities" IJCMS-Oct.2011.

[12]William Stallings, "Cryptography and Network Security: Principles & Practices", fourth edition.

[13] Ronald L. Rivest, Adi Shamir, Len Adelman, "On Digital Signatures and Public Key Cryptosystems," MIT Laboratory for Computer Science Technical Memorandum 82 (April 1977).

AUTHOR BIOGRAPHY

Dhina Suresh was born in Tirunelveli,Tamil Nadu (TN), India, in 1983. She received the Master in Science (M.Sc) in Software Engineering degree from Periyar University, Salem, TN, India, in 2005 and Master of Philosophy(M.Phil.) in Computer Science from the PU, in 2007. Currently she is pursuing her Ph. D in Computer Science in Periyar University, Salem under the guidance of Dr. M. Lilly Florence. Her research area is cloud computing.

Dr. M. Lilly Florence, Professor, Department of M.C.A, Adhiyamaan College of Engineering, Hosur. She received her Bachelor degree in Mathematics during 1995 and Master degree in Computer Application during 1998 at Manonmaniam Sundaranar University. She completed her M.Tech at Punjab University at 2003. She completed her Ph. D in computer science at Mother Teresa University during 2006 – 2011. She has published over 14 research papers in International and National journals.