International Journal of Contemporary Research in Computer Science and Technology (IJCRCST) e-ISSN: 2395-5325
Volume 4, Issue 5 (October '2018)

CLOUD COMPUTING SECURITY ALGORITHMS

K.Amsaveni,
M.Phil., Scholar,
PG & Research Department of Computer Science,
Sengunthar Arts and Science College,
Tiruchengode,Tamilnadu,India.

P.Balamurugan,
Assistant Professor,
PG & Research Department of Computer Science,
Sengunthar Arts and Science College,
Tiruchengode,Tamilnadu,India.

Abstract: Cloud computing utilizes with an attractive tag line 'pay-as-you-use' for attracting users to its great elasticity and scalability of resources at relatively low cost. The authority of the cloud computing is considered with respect to its technological transformations and business benefits, the future enterprise applications are completely dependent on it. It has its individual benefits; nowadays cryptography is more useful than encryption and decryption. Authentication is a basic part of our daily life as the privacy protection. We use authentication throughout to process day-to-day lives when we sign our name to some document, where our agreements and decisions are communicated electronically for providing authentication. In this paper discussed Asymmetric or public-key encryption algorithms like Diffie-Hellman, RSA, ECDH, ECC, ECDSA etc.

Keywords: Cloud Computing, Security Algorithms, Elliptic curve cryptography,ECDH,ECDSA

I.INTRODUCTION

The biggest challenges that companies will face as they move into the cloud are secure data storage, high-speed access to the Internet, and standardization. Storing large amounts of data in centralized locations preserves user privacy, security, identity and their application-specific preferences, raises many concerns about data protection. These concerns, in turn, lead to questions about the legal framework that should be implemented for a cloud-oriented environment. In Value Proposition will describe the various attributes of cloud computing that make it a unique service. In Deployment Models**,** to illustrate the most typical cloud deployment models. These models demonstrate the performance and economic benefits of cloud computing. They are based on the needs of the widest possible range of consumers [1].

Today, companies continue to become larger and larger, not only in the number of the employees, but in the number of departments and type of employees. In this cases, cloud computing is a resource that is readily available to help companies meet their needs and accomplish their goals. Especially in small businesses, cloud computing is excellent technological tool that can benefit the business. All businesses need to respond to competition by making better use of Internet services and offering more incentives than their competitors. Cloud computing can help business shift their focus to the developing good business by acting as a potential disruptive innovation for its employees. However, these businesses should be aware of the uses of the cloud computing as well as which services provide suitable public or private clouds [2].

Security in cloud computing: It is important that the cloud is transparent. Any user that wants to access the cloud should provide an explanation of what data they want, how they use it, why they use it etc. Clearly all the behavior of the cloud users should be monitored and explained. The users then should also only be exposed to information that is necessary to do what they need to do. There should be no other data than what is required for the things a user wants to do (depending on the sort of user). Besides this there should be a data limit. Certain actions require only a certain amount of data and can be predefined [3]. This boundary limits anyone who tries to do any harm to an organization in the cloud. Next there should be a link between data and actions to be made in the system. This would only unblock data that is connected to a certain action in the cloud. When users want to know something about their own privacy, they should be able to see only information regarding to themselves. It is then important that personal information is correct, but also that they cannot see information about other users. In the end there has to be someone responsible for that everything happens as described above. There have to be certain functions that check whether all standard procedures are followed by all the users.

II. REVIEW OF LITERATURE

Pearlson, K., et al. [4] The model includes three stages viewed from two different perspectives: business demand and IT supply. Like other maturity models, it shows an evolutionary path for companies wanting to increase the value from IT and suggests that lower level requirements be satisfied first. Business demand is basically the business' needs for IT, while IT supply is the ability to meet those needs. More specifically, IT supply plays a dual role in this model: an IT organization's ability to satisfy the business demand for IT by providing solutions on the one hand and the stimulation of business demand for further IT capabilities to maximize benefits on the other hand. The model depicts an S-shaped learning curve, which reflects the learning process associated with increasing levels of maturity. The three levels, therefore, entail very different processes and practices and require radically different

organizational thinking, which is why higher levels of maturity build on preceding levels.

H. Lamba, et al [5] Cloud computing concept is a nascent type of distributed computing which is still in its formative years. Cloud computing is an up-and-coming computing paradigm for delivering computing services that aims to provide scalable and inexpensive on-demand computing infrastructures with good quality of service levels. The term cloud computing is habitually used in the present day with an assortment of connotations and elucidations. Recent literature is awash with examples which demonstrate that cloud computing may possibly bring about cost reductions and make possible ground-breaking online services. However, it is the same literature which indicates that barricades to adopt cloud computing are diverse.

M. Armbrust, et al. [6] this research showed that there are a number of benefits of Google docs to Lecturers and these benefits are that; Google docs is a free facility for anyone with a Gmail account. What is only required is internet connectivity. The facility enables better collaboration amongst peers in academia. Lecturers working on a research project can easily share knowledge and ideas on the platform. The most critical tools an academic may need is found on Google docs. Google is one of the most secure platforms in the internet world with a solid track record so what the lecturers need is to be educated and these writers believe workshops are necessary to accomplished.

M. A. H. Masud, et al [7] education needs a new generation of academic staff, and students are different from their ancestors. As a result, students prefer the increased usage of new technology and applications. The CC application can benefit the students by enabling them with quick connections with each other and to the core of educational materials. CC provides the HEIs with the following benefits: 1) facilitate interactive learning; 2) the availability of huge amount of processing power; 3) no need for backup; and 4) provide a digital education environment and web-based services for academic staff and students. For these valuable features, currently, all universities are transitioning to cloud-based applications.

III. CLOUD AUTHENTICATION ATTACKS

Authentication is a process that ensures and confirms correctness and validity of a user's credentials (an essential property that is selected for a given authentication process).1Authentication begins when a user tries to access information. First, the user must prove his access rights and possessing the required essential property selected for the given authentication process [8]. In a cloud environment a user tries to establish a connection with cloud services using his own credentials that authenticate him in order to allow him access to cloud services.
Threats and attacks on authentication in cloud environment, shown in Figure 1, include:

- *Brute Force Attacks*: An attacker guesses the credentials of a user.
- *Cookie Replay Attacks:* An attacker gains access to a user's system through the reuse of a stolen cookie to a session, which contain important confidential information.
- *Credential Theft*: An attacker exploits the system and gain access/credentials through data theft, e.g., via phishing.
- *Dictionary Attacks:* An attacker guesses credentials through trying in turn different terms from the dictionary.

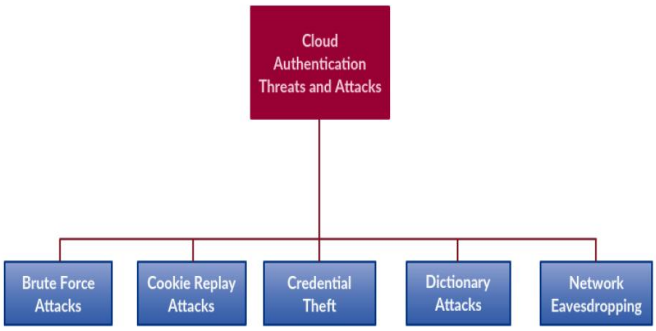

Figure 1: Cloud Authentication Threats and Attacks.

- *Network Eavesdropping:* An attacker steals credentials by reading network traffic. As the browser cannot generate cryptographically valid XML tokens to authenticate a user before accessing cloud services, a protocol involving a trusted third party (TTP) is used. A prototype for such protocols is Microsoft's Passport [9]. The browser may not have the essential credentials, making direct login at the server impossible. A Passport login server receives an HTTP via redirection, allowing users to enter their credentials, such as username or password. Later, the Passport server translates the credentials into a Kerberos token, which is sent to the requesting server via another HTTP redirection. The main security issue with Passport is that the tokens are not bound to the browser. In case of an exploit, the cracker accesses not only the token but also all victims' services. MS Cardspace is a Microsoft initiative to replace user IDs and passwords with a digital or virtual identity. It serves as an example of a solution against attacks on cloud authentication services.

IV.CLOUD DATA SECURITY ALGORITHMS

A digital signature attaches a document to the processor using a particular key, while a digital timestamp connects a document to a particular time. The risk may be difficult to find its solution needs some secret knowledge like signing few digital documents or decrypting an encrypted message. Cloud uses various cryptographic techniques necessary for cloud security. A key is utilized for data encryption and data decryption. This supports in securely protecting integrity and confidentiality of data. It ensures to protect the security of data to be shared in cloud and allows data to be stored securely [10].

Many cryptographic algorithms are considered with two major categories.

- Symmetric algorithms like DES, Triple DES, AES,
- Asymmetric or public-key encryption algorithms like Diffie-Hellman, RSA, ECDH, ECC, ECDSA etc.

In symmetric key encryption, the sender who is transmitting the data and the receiver who is receiving the data to be share a key which is kept secret [11]. This is the way used to encrypt and decrypt the messages. In asymmetric key encryption, two keys are involved wherein one key is used for encryption (publicly available) and the other key is used for decryption (kept secret).

- **Attribute based encryption:** The secret key of a user and the cipher text are depending upon attributes by using the public-key encryption, (e.g. the kind of subscription he has, or the country he lives,). A user can encrypt a message under a policy and a public key. Decryption process will only handle work if the attributes related with the decryption key match the policy used to encrypt the message.
- **Cloud-managed-key:** An additional possible threat with conventional cryptographic techniques can be allowing users manage their decryption keys themselves. Additionally, if a user has not provided permissions as long to access data, after that it can decrypt data if he has the key. The cloud is managed the key using a cryptographic technique as a possible solution for this issue can be resolved. The public key cryptography is managed in the cloud and the decryption key processing is securely handling outsourced to the key management cloud. Because of the decryption processes can be enabled or disabled on the authentication process by the key management cloud, it can also possible to enable or disable the reading of the distributed cipher text at a later time.
- **Identity based encryption:** The Identity-based encryption (IBE) is a kind of public-key encryption wherein the public key of a user is some unique information about the identity of the user (e.g. a user's email address). A public key allows generating to any party from a known identity value like an ASCII string. A trusted third party access is called as the Private Key Generator (PKG) that generates the corresponding private keys. This type of encryption process is able to cut down the complexity for utilizing both administrators and users.

4.1 RSA

The RSA schema is block cipher, original message and cipher message are integer in the interval [0, n-1].propose another schema in which have the original message and encrypted message are h*h square matrices, this method don't have any restriction to encryption and decryption order and it's consider as more scalable, efficient and dynamic [10]. If we said a computing system is secure, we can trust both hardware and software of that system. In a computing system, if the hardware layer is compromise the security, it's difficult for software to find out that attack is underway. Because of the increasing demand of security in communication channel its necessary to develop a new and efficient hardware security module. Hardware implementation of RSA schema using the modular exponentiation [11] propose for the above security purpose. Along with provide security it's also help to reduce to processing time.RSA algorithm is most widely a general purpose approach to public-key encryption. It is an encryption-decryption technique. It consists of plaintext and cipher text in the form of integers between 0 to n-1. This plain text is encrypted in blocks; each and every block has a binary value which should be less than n.

This algorithm is done in three steps:

- Key generation
- Encryption
- Decryption

Key Generation:

In key generation consider two prime numbers (i.e.) p and q. it consists of public key and a private key. The public key will be known to everyone. Calculate the value of n. select a random encryption key e calculates the gcd and it should be equal to 1. Then find the decryption key d. finally calculate the public key and private key. The plain text is encrypted in blocks, with each block having a binary value less than some number n i.e., for block size i bits, $2^i<n<2^{i+1}$.

- Input: None
- Computations: Select two relatively prime numbers p and q.Where n=p*q and v-(p-1)*(q-1).
- Compute the integer d such that (d*e)%v=1.
- e is the integer.
- Output: n, e and d

Encryption process:

In the encryption process represent a plaintext in series of numbers modulo n. the encryption process to obtain cipher text C from plaintext M is very simple. It is formulated as:

$C=M^e \bmod n$

Where C = cipher text

M = message text

E = public key

D = private key

The file will be encrypted by sending a symmetric File Encrypted Key **(FEK)** simultaneously asymmetric public key will generated both will be combined and forms an encrypted FEK with a header file.

- Input: Integers n, e, M
- M is integer representation of the plain text.
- Computation: Let C be the integer representation of the cipher text. $C=(M^e \bmod n)$
- Output: Encrypted text or cipher text C.

Decryption process:

The reverse process of encryption will be decryption. It can be generated using the formula: $m= e^d \bmod n$.

Where C =cipher text

M=message text

E =public key

D =private key

- Input : d, n, C
- C is the cipher text.
- Computation: Let D be the decrypted text such that $D=(C^d \text{ Mod } n)$
- Output: D is the decrypted message.
- Public Key: {e, n}
- Private Key: {d, n}

4.2 ELLIPTIC CURVE CRYPTOGRAPHY (ECC)

Elliptic curve cryptography (ECC) is a cryptographic scheme that uses the properties of elliptic curves to generate cryptographic algorithms [12]. In the 1980s Koblitz and Miller proposed using the group points on an elliptic curve defined over a finite field in discrete logarithmic cryptosystems. An elliptic curve is the solution set over a non-singular cubic polynomial equation with two unknowns over a field F. In short terms it is a discredited set of solutions to a curve that is in the form:

$$y^2 = x^3 + ax + b$$

These curves holds the property that if you draw a straight line that intersects the curve in two points, it will also intersect the curve in a third point that is either on the curve or the point of infinity (also referred to as the neutral element). Another important property of elliptic curves is that they are symmetric over the x-axis. That means that if you have a point P(x, y) then -P will be (x, -y). Using these properties one can define some interesting and useful arithmetic rules. We will now briefly explain how point addition over elliptic curves is done, as this is used for key generation. Suppose that you have a point A and a point B on an elliptic curve and you want to perform an addition of these two points. Then you draw a line from A through B. This line will intersect the curve in a third point. Take this third point and mirror it over the x-axis and that will be the result of the addition.

ALGORITHM FOR ECC

There has to be some information that is publicly known to all the users, thus making it the public key cryptography. The publicly known entities are:-

1. From the equation of the elliptic curve, we need to know:-
   - The values of the constants a and b.
   - The value of m, where elliptic curve is defined over GF(2m).
2. The group of the elliptic curve.
3. A base point B, i.e. any point on the curve E that belongs to the group taken as a base.

The algorithms for different parts of ECC are:-

Key Generation Algorithm

- Randomly select an integer Apriv. It acts as the private key for A.
- Then generate Apub such that Apub = Apriv * B, where Apub is the public key for A.
- Randomly select an integer Bpriv. It acts as the private key for B.
- Then generate Bpub such that Bpub = Bpriv * B, where Bpub is the public key for B.
- Finally, A generates key, Ka = Apriv * Bpub
- B generates key, Kb = Bpriv * Apub

Signature Generation Algorithm

- Calculation of message digest with a HASH function, preferable SHA-1, where e is the message digest, m is the message such that e = HASHfun(m)
- Generate a random integer r and between 1 and n-1.
- The first of the signature, sign1 is calculated from sign1 = x mod n where x is the product of B with rand i.e. x = xcod(rand * B) where xcod is a function to get the x co-ordinate.
- But if sign1 is 0, then redo the previous step.
- The second part of the signature, sign2 is calculated from the equation sign2 = rand -1(e + (Apriv*sign1)(mod n)
- But if sing2 is 0, then re-generate r and follow the procedure again.
- The signature generated is a pair (sign1, sign2).

Signature Validation Algorithm

- Check if sign1 and sign2 lie between the range of 1 and n-1. If not, the signature is not valid.
- Calculate the message digest from the received message with the same hash function, e = HASHfun(m).
- Calculate var1, where var1 = sign2 1(mod n)
- Calculate var2, such that var2 = (e*var1) mod n
- Calculate var3, such that var3 = (sign1*var1) mod n
- We then calculate X, such that X = (var2*B) + (var3*Apub)
- If sign1 (mod n) is equal to xcod(X), then signature is verified.

Encryption Algorithm

- The plain text M is mapped onto the elliptic curve at a point P.
- Generate a random integer rand between 1 and n-1.
- The cipher text is then encoded as a pair C, where C = [(rand * B),(P + (rand * Bpub)]

Decryption Algorithm

- Get x, where x = xcod(C).
- Calculate prod, where prod = Bpriv * x
- Calculate (P + (rand * Bpub)) prod), this gives the mapped point P
- Then un-map P to the plain text M

4.3 ECDH – Elliptic Curve Diffie Hellman

Today, the scientific efforts are looking for a smaller and a very faster public key cryptosystem, at the same time the approach should be practical and very secure, even for the most constrained environments. For any cryptographic technique, there is an analogue for Elliptic Curve. One of these systems is Diffie – Hellman key exchange system. ECDH [13] is a key agreement protocol that allows two parties to establish a shared secret key that can be used for private key algorithms. Both parties exchange some public information to each other. Using this public data and their own private data these parties calculates the shared secret. Any third party, who doesn't have access to the private details of each device, will not be able to calculate the shared secret from the available public information.

For generation of a shared secret key between A and B using ECDH, both have to agree up on EC domain parameters. Both end have a key pair consisting of a private key d(a

randomly selected integer less then n, where n is the order of the curve) and another is a public key Q= d*G (G is the generator point). Let (d_A, Q_A) be the private-public key pair of A and (d_B, Q_B) be the private-public key of B.

1. The end A Computes K_A= (X_A, Y_A) = d_A * Q_B
2. The end B Computes K_B= (X_B, Y_B) = d_B * Q_A
3. Since d_A * Q_B = $d_A d_B$ G= $d_B d_A$ G = d_B * Q_A .
   Therefore K_A= K_B and hence X_A =X_B
4. (Where G is generator point)
5. Hence the shared secret is K_A.

Since it is practically impossible to find the private key dA or dB from the public key K_A.

The Algorithm of Diffie–Hellman key exchange system Using ECC

- Alice and Bob first choose a finite field Fp and an elliptic curve E defined over it (E(Fp)).
- They publicly choose a random base point B belongs E.
- Alice chooses a secret random integer e. He then computes eBεE. In addition, send it to Bob.
- Bob chooses a secret random integer d. She then computes dBεE. And send it to Alice.
- Then eB and dB are public and e and d are secret.
- Alice computes the secret key edB = e(dB).
- Bob computes the secret key edB = d(eB)

4.4 Elliptic Curve Digital Signature Algorithms (ECDSA)

ECDSA is the elliptic curve analogue of the DSA. That is, instead of working in a subgroup of order *q* in Z **p*, we work in an elliptic curve group *E*(Z*p*). Signature algorithm is used for authenticating a device or a message sent by the device. For example consider two devices A and B. To authenticate a message sent by A, the device A signs the message using its private key. The device A sends the message and the signature to the device B. This signature can be verified only by using the public key of device A. Since the device B knows A's public key, it can verify whether the message is indeed send by A or not.

ECDSA is a variant of the Digital Signature Algorithm (DSA) that operates on elliptic curve groups. For sending a signed message from A to B, both have to agree up on Elliptic Curve domain parameters. Sender 'A' have a key pair consisting of a private key d_A (a randomly selected integer less than n, where n is the order of the curve, an elliptic curve domain parameter) and a public key Q_A = d_A * G (G is the generator point, an elliptic curve domain parameter) [94].

ECC Domain Parameters

The operation of public-key cryptographic schemes involves arithmetic operations on an elliptic curve over a finite field determined by some elliptic curve domain parameters. ECC domain parameters over F_q (where F_q is either F_p and $F_2{}^m$) are a septuple: T = (q,FR,a,b,G,n,h). Consisting of a number q specifying a prime power (q = p or q = 2^m), an indicator FR (field representation) of the method used for representing field elements ε F_q, two field elements a and b ε F_q , that specify the equation of the elliptic curve E over F_q (i.e., $y^2 = x^3 + ax + b$ in the case p>3 and $y^2 + xy = x^3 + ax^2 + b$ when p = 2), a base point G = (x_G and y_G) on E(F_q), a prime n which is the order of G and an integer h which is the co factor h = # E(F_q)/n.

ECDSA Key Generation

The user A follows these steps where p is a large prime:

- Select a random integer d ∈ [1, n - 1].
- Compute Q = d x P.
- The public and private keys of the user A are Q and d, respectively.

The other parties can check if the public key is valid by;

- Checking that Q ≠ 0.
- Checking that x_Q and y_Q are properly represented elements of F_q.
- Checking that Q is on the elliptic curve defined by a and b.
- Checking that n_Q = Q.

If any of these checks fail the public key Q is invalid, otherwise Q is valid. The following procedure describes how to generate the signature.

ECDSA Signature Generation

The user A signs the message m using the following steps

- Select a pseudorandom integer k ∈ [1, n - 1].
- Compute k x P = (x_1, y_1) and r = x_1 mod n.
  If x_1 ∈, GF(2^k), it is assumed that x_1 is represented as a binary number.
  If r = 0 then go to Step 1.
- Compute k^{-1} mod n.
- Compute s = k^{-1}(H(m) + d • r) mod n.
  Here H is the secure hash algorithm SHA-1.
  If s = 0 go to Step 1.
- The signature for the message m is the pair of integers (r, s).

ECDSA Signature Verification

The user B verifies A's signature (r, s) on the message m by applying the following steps:

- Verify that r and s are integers in the interval [1,n-1].
- Compute c = s^{-1} mod n and H(m).
- Compute u_1 = H(m) • c mod n and u_2 = r • c mod n.
- Compute u_1 x P + u_2 x Q = (x_0, y_0) and v = x_0 mod n.
- Accept the signature if v = r.

V.CONCLUSION

Clouds can be flexible and cost-efficient. In a cloud infrastructure, sensitive information for a customer is kept on geographically dispersed cloud platforms, under direct control of the cloud —not of the customer. Securing users data in a cloud is one of the most challenging tasks Cloud resources (such as software, platforms, and infrastructure) are vulnerable to abuse, theft, unlawful distribution, harm, or compromise. Among others, there is a risk that user's information can be leaked to a competitor. Unauthorized

access to data stored in clouds can be minimized through ensuring security.

VI.REFERENCES

[1]. R. Buyya, C. S. Yeo, S. Venugopal, J. Broberg, and I. Brandic, Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility, Future Generation Computer Systems, 2009.

[2]. L. M. Vaquero, L. Rodero Merino, J. Caceres, and M. Lindner, A break in the clouds: Towards a cloud definition, SIGCOMM Computer Communications Review, 2009.

[3]. M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, and R. Katz, Above the Clouds: A Berkeley View of Cloud Computing, UC Berkeley Reliable Adaptive Distributed Systems Laboratory White Paper, 2009.

[4]. P. Mell and T. Grance, The NIST Definition of Cloud Computing, National Institute of Standards and Technology, Information Technology Laboratory, Technical Report Version 15, 2009.

[5]. B. Sotomayor, R. S. Montero, I. M. Llorente, and I. Foster, Virtual infrastructure management in private and hybrid clouds, IEEE Internet Computing, 13(5):14_22, September/October, 2009.

[6]. J. Rittinghouse, J.Ransome Cloud Computing: Implementation, Management and Security 2010, p 28 Amazon Simple Storage Service (Amazon S3), [online], available at: http://aws.amazon.com/s3, retrieved 5 Jan 2009.

[7]. Ahuja R. (June 2011) 'SLA Based Scheduler for Cloud storage and Computational Services', International Conference on Computatonal Science and Applications (ICCSA).

[8]. Ahmed S, Raja M. (2010) 'Tackling Cloud security issues and forensics model', *High Capacity Optical Networks and Enabling technologies (HONET)* , 19-21 Dec.

[9]. Doelitzscher F, Reich C. (July 2010) 'Designing Cloud services adhering to Government privacy Laws ', IEEE 10th International Conf. on Computer and Information Technology.

[10]. D. Catteddu and G. Hogben, "Cloud Computing: Benefits, risks and recommendations for information security," ENISA, 2009.

[11]. Z. S. Z. Shen and Q. T. Q. Tong, "The security of cloud computing system enabled by trusted computing technology," *Signal Process. Syst. (ICSPS), 2010 2nd Int. Conf.*, vol. 2,2010.

[12]. Hogganvik, F. Vraalsen, F. Braber, K. Stølen, and M. S. Lund, "Model-based security analysis in seven steps — a guided tour to the CORAS method," *BT Technology Journal*, 2007.

[13]. I. Foster, Y. Z. Y. Zhao, I. Raicu, and S. Lu, "Cloud Computing and Grid Computing 360-Degree Compared," *2008 Grid Comput. Environ. Work.*, 2008.

[14]. P. Mell and T. Grance, "The NIST Definition of Cloud Computing Recommendations of the National Institute of Standards and Technology," 2011.

[15]. D. F. Ferraiolo, D. R. Kuhn, R. Sandhu, S. Gavrila, and R. Chandramouli, "Proposed NIST standard for role-based access control," *ACM Transactions on Information and System Security*, 2009.

[16]. Barry Wilkinson, Grid computing: techniques and applications, 2010, Internet-connected computers in the Search for Extraterrestrial Intelligence (SETI), [online] available at: http://www.seti.org.

