International Journal on Future Revolution in Computer Science & Communication Engineering
Volume: 4 Issue: 1
ISSN: 2454-4248
330 – 336

Security Issues and Solutions in Cloud Computing: A Review

1* Maddala Sai Kumar 2* Bugata Hara Govinda Sai Praneeth3# Satish Kumar Negi4#Pushpendra Kumar Chandra
*Student (B. Tech _ 4th year), Department of Computer Science and Engineering (CSE), Institute of Technology,
Guru Ghasidas Vishwavidyalaya, Bilaspur,Chattisgarh, India
Assistant Professor, Department of Computer Science and Engineering (CSE), Institute Of Technology,
Guru Ghasidas Vishwavidyalaya, Bilaspur,Chattisgarh, India
1saikumar.maddala123@gmail.com2praneethbugata9@gmail.com 3#skn.ggv@gmail.com4#pushpendrachandra@gmail.com

Abstract: Cloud computing is a rising worldview which has turned into the present most trending topic because of its ability to reduce the costs associated with computing. In the present period, it is most intriguing and helpful innovation which offers the services based on demand over the internet to its users. Since Cloud processing stores the information and due to its wide spreading resources security has turned out to be a serious obstacle which is hampering the cloud users. There are number of clients utilizing cloud to store their own information. This paper lists the security problems that cloud computing facing today such as data, privacy, and account hijacking and some other security issues. It also discusses some solutions for tackling these issues and problem.

Keywords: *cloud computing, Security, Encryption, Cryptography, Data Encryption Standard (DES), Advanced Encryption Standard (AES), Rivest-Shamir-Adelman (RSA), Triple DES, Blowfish.*

*****

1. INTRODUCTION

Cloud computing is a rising field of computing where a set of resources (i.e. hardware and software resources) are accessible as a support to the client but not as a product. The best part about this computing is, client need not to be worried about the physical locations.

Now a days cloud computing is an extensively using distributed computing model, which depends on the economic size of the operator of cloud that is abstract, virtualized and dynamic. The main objective of the cloud computing is to manage security, storage allocation, various type of platforms and services which assigned to the external users by the demand through the internet. Cloud computing is a rapidly emerging computation model with a goal of freeing up users of cloud from the management of hardware, software, networks and data resources and assigning these works to cloud service providers [2]. Cloud computing provides various methods for managing the resources such that users of cloud can access them without facing any kind of performance related problems. Cloud Computing Services are divided into three classes, basing on the abstraction level and the service model of providers.

It can be **Software as a Service (SAAS)** model that offers software on a single platform. SAAS provides the user to run the applications which can be accessed through standard interfaces like web browsers and email clients on cloud infrastructure. It can be **Platform as a Service (PAAS)** model which offers a platform from where the software and data can be accessed by the user. PaaS provides customers with the capability to deploy and develop the applications based on tools and programming languages supported by the providers. It can be **Infrastructure as a Service (IAAS)** model which provides the safety and backup services. In IAAS the provider provides the virtual interface where the computing resources like processing units and storage unit etc., are provided to setup the deployment environment for their software system [3]. One of the main feature of cloud is Virtualization. In the virtualization technology complexity of underlying software or hardware are hidden.

2. OVERVIEW OF SECURITY

Cloud computing security or, simply we can state cloud security has mentioned a broad set of strategies, technologies, and controls sent to protectdata, applications, valuable information and the related framework of cloud computing. Basically, it is a sub-domain of network security and more comprehensively, data security. Cloud security envelops a wide set of security constraints from an end-user and cloud provider's point of view, where the end-user will essentially be worried about the provider's security strategy, how and where their data is stored and who has access to that data. For a cloud provider, on the other hand, cloud computer security issues can range from the physical security of the infrastructure and the access control mechanism of cloud assets, to the execution and maintenance of security policy. As cloud computing priority is increasing day by day various organizations such as NIST has put forth some guidelines for adopting cloud computing [1]. It categorizes cloud security issues into 9 categories. Similarly, Union Agency for Network and data Security (ENSIA) gives bits of knowledge to SMEs on issues related to data security risks for cloud computing. At the end Cloud Security Alliance (CSA) s Top threat working Group has published 12 most unpredictable cloud threats based on survey conducted on industry experts. Cloud computing has a

few noteworthy dangers, such as data security, trust, data loss, and data integrity, account hijacking.

2.1 SECURITY THREATS

The model of cloud computing has changed the way we utilize the IT resources. The development of the cloud service model conveys business-supporting innovation more effectively than any time in recent memory. The CSA (Cloud Security Alliance) has recognized some cloud computing threats. These threats are the most fundamental threats that can be conceivable in the cloud environment. These threats are as follows:

- **Trust:** Trust between the cloud provider and the client is one of the major issues that cloud computing facing today. There is no chance for the client to make sure whether the administration of the Service is trustable or not, and whether there is any danger of insider attacks. This is a noteworthy issue and has gotten solid consideration by organizations [4]. The only legal report between the client and cloud provider is the Service Level Agreement (SLA). This report contains every one of the understandings between the client and the cloud provider; it contains what the service provider is doing and willing to do. However, right now there is no reasonable format for the SLA, and as such, there may be services not documented in the SLA that the customer may be unaware that it will need these services at some later time.
- **Legal Issues:**There are several regulatory requirements, protection laws and information security laws that cloud frameworks need to stick to. One of the significant issues with sticking to the laws is that laws change from nation to nation, and clients have no power over where their information is physically located.
- **Data Breaches:** A data breach is an occurrence that includes the unauthorized or illegal viewing, access or recovery of information by an individual, application or administration [5]. It is a kind of security breach particularly designed to steal or publish information to an unsecured or illegal area. A data breach is otherwise called as data spill or data leak. A data breach happens when an unapproved programmer or attacker accessing a secure database. Data breach is commonly referred towards logical or digital information and regularly directed over the Internet or a network connection. A data breach may result in losing personal information, financial information etc.
- **Data Loss:**Data loss is a process that results in data/information being deleted, corrupted and/or made unreadable by a user and/or software or application. It happens when at least one or more data elements can never again be used by the data owner. Data loss is also known as data/information leakage. Data loss may occur when in motion (data transmitted over the network). Data loss can happen for different reasons, including:
  - Data corruption
  - Data being deliberately or incidentally deleted or overwritten by a client or an attacker
  - Data stolen over the network by network intervention attack
  - Data storage device physically harmed or stolen
  - Data loss may occur when the system is attacked by Virus it results in erasing documents

  Data loss is typically avoided by implementing data backup solutions and adding strong data access controls and security mechanisms on data storage assets.
- **Data Integrity:** Data integrity is a standout amongst the most critical elements in any system. Data integrity is effectively achieved in an independent framework with a single database. Data integrity in such a framework is maintained by means of database constraints and transactions. Transactions should follow ACID (atomicity, consistency, isolation and durability) properties to ensure data integrity. Most databases support ACID properties and can save data integrity. Next in the complexity chain are distributed systems. In a distributed system, there are various databases and multiple applications. To keep up data integrity in a distributed system, exchanges over different information sources should be taken care of effectively in a safeguard way. This can be done using a central global transaction manager. Every application in the distributed system ought to have the capacity to take an interest in the global transaction through resource manager.
- **Data Center Operation:** If there is an occurrence of disaster, organizations using cloud computing applications needs to secure the client's information with no loss. If data is not managed properly, at that point there is an issue of data storage and data access. If there should arise an occurrence of earthquake or any natural calamite, the cloud providers are responsible for data loss [6].
- **Account Hijacking:** Account hijacking is a procedure through which a person's email account, PC account or some other record related with a computing device or administration is stolen or seized by a programmer. It is a sort of wholesale fraud in which the programmer utilizes the stolen account data to complete malicious or unauthorized activity. In account hijacking, a programmer utilizes an email account to imitate the account owner. Typically, account hijacking can be done through phishing, sending parodied messages to the client, password guessing or a few other hacking strategies.

 ISSN: 2454-4248
330 – 336

In most of the cases an email account is connected to a client's different online administrations, for example, social networks and other financial accounts. The programmer can utilize the account to recover the individual's personal information, perform financial exchanges, make new accounts, and approach the account owner's contacts for money or help with an illegal action [15].

- **Insecure APIs:** If the Application Programming Interfaces which are used by the users to communicate with the cloud services are weak or not sufficiently secured [5], accidental or malicious attempt to violate them may expose the cloud data to many security threats related to inflexible access control, scalability and limited monitoring and many other issues.
- **Denial of Service:**DoS have become very serious threat when the organizations are dependent on the services for 24/7. It temporarily denies the access of data stored in the cloud to the authorized users by make an attack on the server by sending thousands of requests to it become unable to respond to the regular clients [5].
- **Data Recovery**: Data Recovery has also become one of the threat to cloud computing. If the data has been lost or corrupted and if there is no any back up copy for that data, then it is very difficult to recover the lost data [7]. There are many possibilities of losing data because of a malignant attack and sometimes because of server crashes or unintentional deletion by the provider [8] without having back up for that data. Disastrous occasions like a earthquake and fire could be the reasons for data loss. In that cases, data recovery is to be exceptionally troublesome.
- **Key Management:** Since encryption is the most used techniqueto ensure data security, we are facing the issue of key management. The encryption keys cannot be put away in the cloud; so, the client must manage and control a key management framework for any cryptographic strategy used [4].

3. SOLUTIONS TO SECURITY THREATS

To secure the Cloud means secure the calculations and databases, a few solutions have been proposed for the security and privacy issues.

3.1 ENCRYPTION The principle strategy used for data security in the cloud is encryption. Encryption appears like the ideal answer for ensuring data security. Encryption takes fundamentally more computing power, and this is expanded by few variables because of database. There are a few methodologies developed to deal data encryption [4]; each having its own advantages and disadvantages, some give better security mechanisms, and some emphasis on encouraging more operations to the clients.

3.2 HONEYPOT

A honeypot is a trap set to recognize, avoid or in some way to counteract the attempts at unauthorized use of information systems by unknowns [16]. By this honeypot technique, the official can watch the programmer misuse the vulnerabilities of the framework, in this manner realizing where the framework has shortcomings that should be upgraded. The programmer can be caught and stop while attempting to acquire root access to the system. By concentrate the exercises of programmers, designers can better make more secure frameworks that are possibly resistant to future programmers. If deployed effectively, a honeypot can fill in as an early-cautioning and propelled security surveillance tool, limiting the risks of attacks on IT systems.

3.3 CRYPTOGRAPHY

Cryptography is a technique generally used for information security. Cryptographic strategies have turned out to be fundamental for security in cloud. A key is used for data encryption and decryption. This helps in securing integrity and trustworthiness of information. It ensures security of data being shared in the cloud and enables information to be put away safely. Cryptography refers only to encryption, which is the way toward changing over normal data (plain content) into ambiguous content (called cipher content). Encryption alludes to the strategy for changing over plain content to secret content (cipher content) which must be authorized by the owner of the secret key [9]. Cryptography, in modern days is considered combination of two types of algorithms. They are

- Symmetric-key algorithms (DES, AES, Triple DES)
- Asymmetric-key algorithms (RSA)

The difference is established by the way of using keys. In symmetric key algorithms, the individual who is sending the information and the individual who is accepting the information share a key which is kept secret. This is then used to encrypt and decrypt the messages. In asymmetric-key algorithms, two keys are included wherein one is used for encryption (this is freely accessible) and the other is used for decoding (this is kept secret) [17].

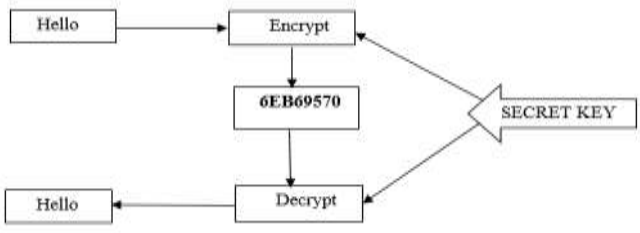

Fig-5: Symmetric-key Cryptography

 ISSN: 2454-4248
330 – 336

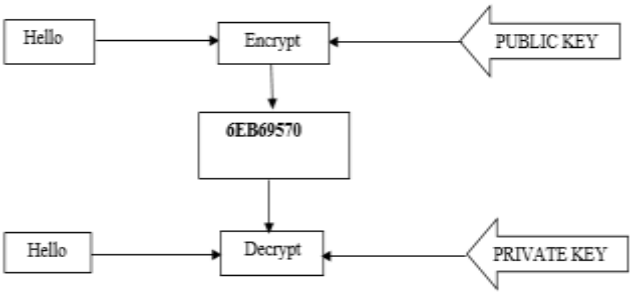

Fig-6: Asymmetric-key Cryptography

3.3.1 STUDYOF CRYPTOGRAPHIC TECHNIQUES

- **Data Encryption Standard:**DES is a block cipher. It encrypts information in block of size 64 bits each. 64 bits of plain content goes as the input to DES, which produces 64 bits of cipher text [10]. The key length is 64 bits. Cryptanalyst can perform cryptanalysis by exploiting the characteristic of DES algorithm, however nobody has succeeded in finding the shortcoming. DES results in permutations among the 2^{64} conceivable arrangement of 64 bits, each of which may be either 0 or 1. Each block of 64 bits is divided into two blocks of 32 bits each, a left half L and right half R. The DES algorithm changes 64-bit messages block M into a 64-bit cipher block C. If each 64-bit piece is encrypted independently, then the technique for encryption is known as the Electronic Code Book (ECB) mode. There are two other distinctive modes of DES encryption, to be specific Chain Block Coding (CBC) and Cipher Feedback (CFB).
- **Triple DES(3DES):** Triple DES is an alternative option to DES, which applies the Data Encryption Standard (DES) encryption algorithm three times to every data block.3DES is essentially the DES symmetric encryption algorithm, utilized three times on similar data. Three DES can also be called as T-DES. It utilizes the normal DES encryption algorithm three times to enhance the security of cipher text [11]. In this, same information is encoded two times more than DES, this makes the encryption more stronger and hard to break. Triple DES is a Block cipher which utilizes 48 rounds in its computation, and has a key length of 168 bits. There are following modes:
  Encrypt →Decrypt →Encrypt with three different keys K1, K2, K3
  Encrypt →Encrypt →Encrypt with three different keys K1, K2, K3
  Encrypt →Decrypt →Encrypt in which first and last encryption is done using same key. So here two keys are used.
  Encrypt →Encrypt →Encrypt This also done using same key for first and last encryption.
  The fundamental advantage of Triple DES is that it is three times secure, since it is a combination of three DES algorithms. It gives sufficient security to the information, yet it isn't the best since it takes lot of time and its encryption speed also not as much as DES encryption algorithm.
- **Advanced Encryption standard(AES):**AES is the new encryption standard prescribed to replace DES. AES algorithm can accept any combination of information (128 bits) and key length of 128, 192, and 256 bits [12]. The algorithm is alluded to as AES-128, AES-192, or AES-256, depends upon the key length. while processing encryption decryption process, AES framework experiences 10 rounds for I28-bit keys, 12 rounds for I92-bit keys, and 14 rounds for 256-bit to deliver the last cipher content or to recover the first plain-content. AES permits a 128-bit data length that can be partitioned into four essential operational blocks. Before achieving the last round, this yield goes through nine principle rounds, during each of those rounds four transformations are performed; 1) Sub-bytes, 2) Shift rows, 3) Mix-columns, 4) Add round Key.
- **Rivest Cipher4(RC4):** RC4 is perceived as the most normally used stream cipher in the world of cryptography [10]. RC4 has a use in both encryption and decryption while the information stream undergoes XOR together with a series of generating keys. It takes in keys of irregular lengths and this is known as a maker of pseudo arbitrary numbers. The output is then XORed together with the stream of information to produce a newly encrypted information**.**
- **Blowfish:** Blowfish algorithm is a symmetric block cipher having variable length key from 32 bits to 448 bits. It works on block size 64 bits. It is a 16-round Feistel cipher network and uses S-Boxes. Every S-box contains 32 bits of data.

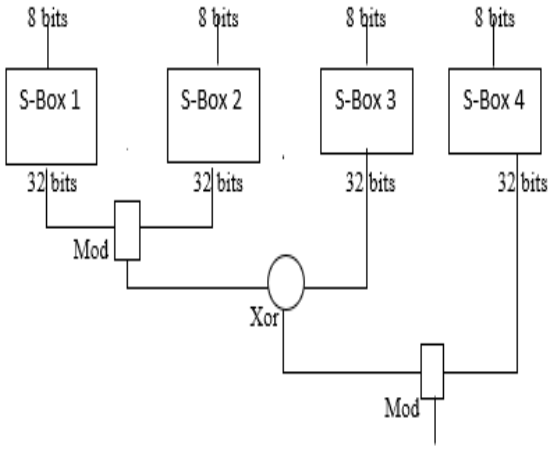

Fig: Blowfish Function

Above Diagram demonstrates the Blowfish's F-function. The function parts the 32-bit input into four 8-bit quarters, and uses the quarters as input to S-boxes. The outputs are added (Mod) modulo and

XORed to create the last 32-bit output i.e. cipher data [11]. For Decryption at another end a similar procedure happens, but in reverse order. Blowfish gives a decent encryption rate in software. It is significantly quicker than 3DES. In many experiments, Blowfish encryption algorithm is announced best because security level that is offers and speed of encryption, which is better than many existing encryption algorithms.

- **Rivest-Shamir-Adelman (RSA)**: RSA is one of the best-known algorithm for digital signatures and encryption of blocks of data. RSA uses a variable size encryption block and a variable size key. It is an asymmetric (open key) cryptosystem which is based on number theory. It utilizes two prime numbers to create public and private keys. These two diverse keys are utilized for encoding and decoding purpose [12]. Sender encodes the message using Receiver public key and when the message gets transmit to receiver, at that point receiver can decode it utilizing his own private key. RSA operations can be disintegrated in three steps; key generation, encryption and decryption. RSA have numerous defects in its plan, so it is not favorable for commercial purpose. When small values of p and q are chosen for designing a key then the encryption procedure turns out to be easy and one can have the capacity to decode the information by utilizing random probability theory and side channel attacks. If large p and q lengths are chosen, then it takes more time and performance get degraded compared to DES.

  Key Generation Procedure

1. Choose two distinct large random prime numbers p & q such that $p \neq q$.
2. Compute $n = p \times q$.
3. Calculate: phi (n) = (p-1) (q-1).
4. Choose an integer e such that $1<e<phi(n)$
5. Compute d to satisfy the congruence relation $d \times e = 1 \bmod phi(n)$; d is kept as private key exponent.
6. The public key is (n, e) and the private key is (n, d).
7. Keep all the values d, p, q and phi secret.
8. Encryption Plaintext: $P < n$ Ciphertext: $C = Pe \bmod n$.
9. Decryption Ciphertext: C Plaintext: $P = Cd \bmod n$.

In cloud computing security has more importance while we talk about data storage. Today cloud computing is facing many problems related to security. To avoid that security issuesvarious cryptographic algorithms have mentioned above.

4. COMPARISION OF CRYPTOGRAPHIC TECHNIQUESS

The number of the cryptography calculations and correlation between them depends on the key size, speed and security. The best encryption algorithm relies upon key management, security and cipher type. Key size gives the number of bits that the cryptography algorithm utilizes, speed is the parameter which characterizes whether the algorithm is slow, moderate, quick when compared with the other cryptographic techniques. Security characterizes the security status of the algorithm i.e., after using the algorithm is the cloud completely secure, moderately secure or insecure [11].

4.1 TABLE OF COMPARISION

Algorithm	Data Encryption Standard(DES)	Advanced Encryption Standard (AES)	TRIPLE DES (3 DES)	Rivest Cipher 4(RC4)	Rivets-Shamir-Adelman(RSA))	Blow Fish
Key Size	56 bits	128,192,256 bits	112/168 bits	264 Bytes	1024 bits and above	32-448 bits
Speed	Slow	Fast	Very Slow	Very Fast	Fast	Fast
Speed depends on key?	Yes	Yes	No	No	Yes	No

 ISSN: 2454-4248
330 – 336

Security	Insecure	Secure	Moderately Secure	Moderately Secure	Secure	Secured, but less attempted cryptanalysis than other algorithms
Cipher Type	Symmetric Block Cipher	Symmetric Block Cipher	Symmetric Block Cipher	Symmetric Block Cipher	Asymmetric Block Cipher	Symmetric Block Cipher
Rounds	16	10,12,14	48	01	01	16

4.2 ANALYSIS OF COMPARISION:

From the work that we have done so far, it is observed thatthe strength of every encryption algorithm relies on the key management, number of keys, number of bits used as a part of a key. Longer the key length more will be the power consumption that will prompt more heat dissipation. Thus, it is better to use short key length algorithm. The keys having more number of bits requires more computation time which basically indicates that system takes more time to encrypt the information. From above analysis, we can say that Blowfish algorithm is leading with the security level that they provide and faster encryption speed. Though Blowfish algorithm key size is longer it is the best till now in terms of processingtime [13]. Blow Fish algorithm [14] is the secure one because the fundamental concept in this algorithm is encryption and decryption. It uses secret key method. Blowfish algorithm can be considered as a best encryption algorithm for cloud computing when throughput and power consumption considered.

5. CONCLUSION:

Cloud computing seems extremely valuable service for many individuals; many of the people are experiencing cloud services in various ways. Because of its flexibility, many people are exchanging their data to cloud. Since organizations have large amount of information to store and cloud gives that space to its client and enables its client to get their data from anyplace anytime effectively. As individuals are saving their personal and important information, security has become a major issue to store that information securely. Cryptography algorithm is the science which is written in cipher(secret) text. Today security has become a major challenge in cloud computing. Some of the threats have been mentioned above. To regulate the risk factor in cloud computing in terms of security, some well-known algorithms have been analyzed in this paper.Of all the algorithms Blowfish algorithm is the most secure one. No one can get 100% output in terms of security, but we can work towards to regulate the risk in the cloud computing. Still more effective approach should be done for the best cryptography algorithm**.**

References:

[1] NaimAhmed"Cloud Computing: Technology ,Security Issues and Solutions" *978-1-5090-5814-3/17/$31.00 2017IEEE*

[2] NattakarnPhaphoom, Xiaofeng Wang and PekkaAbrahamsson "Review Article Foundations and Technological Landscape of Cloud Computing" *ISRN Software Engineering* Volume 2013 (2013), Article ID 782174, 31pages.

[3] NattakarnPhaphoom, Xiaofeng Wang and PekkaAbrahamsson "Review Article Foundations and Technological Landscape of Cloud Computing" *ISRN Software Engineering* Volume 2013 (2013), Article ID 782174, 31pages.

[4] Irfan Hussain,Imran Ashraf "Security Issues in Cloud Computing",*Int. J. Advanced Networking and Applications* Volume: 6 Issue: 2.

[5] Chandan Prakash, Surajit Dasgupta "Cloud Computing Security Analysis: Challenges and Possible Solutions", *International Conference on Electrical, Electronics, and Optimization techniques* (ICEEOT)-2016.

[6] R. VelumadhavaRaoa,, K. Selvamanib, "Data Security Challenges and Its Solutions in Cloud Computing"*International Conference on Intelligent Computing, Communication & Convergence (ICCC-2014)*

[7] Manpreet Kaur, Hardeep Singh "A REVIEW OF CLOUD COMPUTING SECURITY ISSUES" *International Journal of Advances in Engineering & Technology*, June 2015. IJAET ISSN: 22311963

[8] William Allen"Data Security, Privacy, Availability and Integrity in Cloud Computing: Issues and Current Solutions"*(IJACSA) International Journal of Advanced Computer Science and Applications*, Vol. 7, No. 4, 2016.

[9] Radhika Patwari "Security issues and Cryptographic techniques in Cloud Computing" *International Journal of Innovative Computer Science & Engineering* Volume 2 Issue 4.

[10] Vekariya Meghna "Comparative Analysis of Cryptographic Algorithms and Advanced Cryptographic Algorithms", *International journal of computer engineering and science*, 2015.

ISSN: 2454-4248
330 – 336

[11] Rajdeep Bhanot1 and Rahul Hans "A Review and Comparative Analysis of Various Encryption Algorithms" *International Journal of Security and its applications*, vol. 9, No.4 (2015), pp. 289-306.

[12] Gurpreet Singh, Supriya "A Study of Encryption Algorithms (RSA, DES, 3DES and AES) for Information Security"*International Journal of Computer Applications (0975 – 8887) Volume 67– No.19, April 2013*

[13] T.Ramaporkalai"Security Algorithms In Cloud Computing "*International Journal Of Computer Science Trends and Technology(IJCST)*—Volume 5 Isssue2,Mar-Apr 2017

[14] OMAR MOHAMMED ABDULRAHMAN ABDULKAREEM, N. SHANKER"Implementation of Data Encryption by using Blowfish Encryption Algorithm to Protect Data in Public Cloud*"ISSN 2321-8665 Vol.03,Issue.02, June-2015,*

[15] Accounthijacking https://digitalguardian.com/blog/what-cloud-account-hijacking

[16] Honeypot https://ethics.csc.ncsu.edu/abuse/hacking/honeypots/study.php

[17] Cryptography https://en.wikipedia.org/wiki/Cryptography