Int. Jrl. of Computational Learning & Intelligence
Vol. 02, Issue No. 01, 2023

ORIGINAL RESEARCH

One Time Pad Encryption Technique in Cryptography

Alle Bhavana Kumari . HalavathBalaji . N Ch S N Iyengar

Sreenidhi Institute of Science and Technology,
Yamnampet,Ghatkesar, Hyderabad (T.G), India

Received: 06 November 2022 / Revised: 21 November 2022 / Accepted: 08 December 2022

Abstract – Cloud Computing is a term that is used for the provision of host services over the Internet The secure data storage on cloud environments is the primary requirement of such applications, where data are being transferred or transmitted between the servers and their users. The existing paper consists of a text steganography approach for hiding loaded secret English text file in a cover English text file which is less confidential. In this paper we are using one of the most effective technique for secure communicating is cryptography in cloud. Cryptography involves the creation of codes written or generated that allow secrecy of information. To ensure security of data in cloud computing, this paper presents an encryption technique called One Time Pad(OTP).The one time pad (OTP) is an uncrack able encryption technique, but it requires the use of a shared key of the same size as, or longer than, the message sent. The proposed system offers information theoretic security, data hiding capacity.

Index Terms - Cloud Computing, Cryptography, One-Time Pad (OTP).

I. INTRODUCTION

Cloud Computing provides computer services — servers, storage, databases, networking, software, analytics, and more — on the Internet which is "the cloud" to deliver faster innovation, flexible resources, and economies of scale. It is a dynamic technology platform that addresses a wide range of demand through the provision of cyber infrastructure for maintenance and expands the capabilities of information storage. It depends on resource sharing to achieve consistency and economies of scale. Cloud Computing provides access to software and hardware without significant capital investment and provides easier access to applications and services that can be implemented with minimal interaction between service providers.

This has developed cloud computing as a technological innovation capable of handling large amounts of information transferred and stored through electronic applications. Most researchers classify cloud computing deployment approaches into four major categories: Public, Private, Community, and Hybrid. A cloud deployment model is a specialized cloud environment, characterized primarily by ownership, size, and access. A Public cloud is a cloud environment owned by a third - party cloud provider that is publicly accessible. A Private cloud is held by a unique organization. A Community cloud resembles a public cloud preventing its access from being limited to a specific cloud consumer community. While hybrid cloud is a cloud environment consisting of two or more different models of cloud deployment. The four base cloud deployment models may have additional variations.

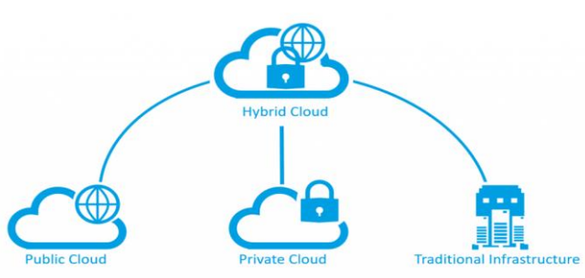


Fig.1. Approaches in cloud deployment

Int. Jrl. of **Computational Learning & Intelligence**
Vol. 02, Issue No. 01, 2023

Cloud computing researchers have divided cloud computing into three layers: The provision of technology infrastructure as a scalable service on demand is Infrastructure as a Service (IaaS). Platform as a Service (PaaS) provides run - time circumstances for applications, deployment and development tools, etc. Software as a Service (SaaS) model allows end - user services to be used with software applications.

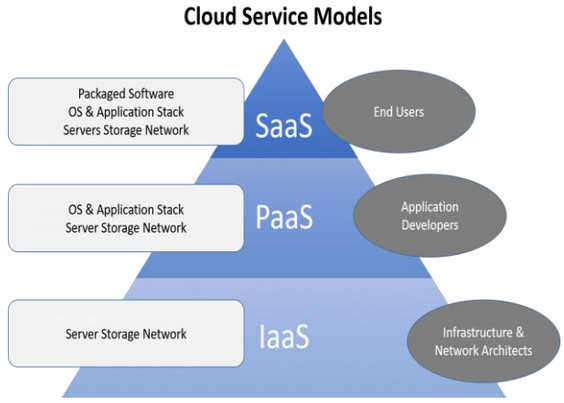


Fig.2.Structure of cloud computing-services

Cloud computing security is a major concern. Cloud security refers to a wide range of policies, technologies, applications and controls used to protect virtualized IP, data, applications, services and the associated cloud computing infrastructure, for many reasons, naturally pose new challenges to security.Data should be kept in encrypted form in the cloud. Before deploying a specific resource to the cloud, several aspects of the resource should be analysed, such as:

- Choose the resource to move into the cloud and analyze its risk sensitivity.
- Users can frequently update data stored in the cloud, including deletion, insertion, attachment, modification, reordering, etc.
- It is very important to ensure authentic storage to update dynamic data.
- Understand the data storage system of the cloud service provider and its transfer to and from the cloud.

II. CRYPTOGRAPHYIN CLOUD COMPUTING

Computer application is growing every day in real life. The need for data security is therefore becoming an increasingly essential part of message or data transmission. So, security of information became part of our daily lives. Hidden exchange of information is a concern in the field of information security among the various techniques. Different methods have been used for this purpose, such as cryptography, steganography, coding, etc.

In cloud, cryptography uses encryption techniques to secure data that is used or stored in the cloud. It converts data into an unreadable format for an unauthorized user and also enables users to access shared cloud services conveniently and securely, like any data that is secured with encryption by cloud providers. Cloud cryptography protects receptive data without binding exchange of information.

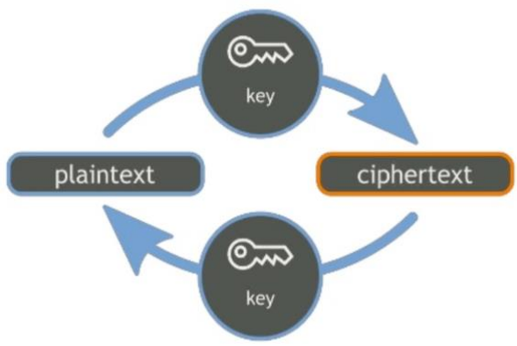


Fig.3.Structure of Cryptography

The word “cryptography” is of Greek origin and means "hidden writing" from the Greek words “kryptos” meaning "secret", and “graphein” meaning "writing”. Earlier cryptography was synonymous with encryption,

but nowadays cryptography is primarily based on mathematical theory and practices in computer science. Cryptography is used in many applications such as banking transaction cards, computer passwords and e - commerce.

The primary purpose of using cryptography is to provide the following four basic information security services.

- Confidentiality: It is a security service which keeps an unauthorized person's information.
- Data integrity: The security service is responsible for identifying any changes to the data.
- Authentication: It confirms to the recipient that only an identified and verified sender has sent the received data.
- Non - repudiation: It is a security service that establishes that an entity cannot deny ownership of a prior undertaking or action.

The most accessible use of cryptography is encrypting communications between us and another system, and the one that we all use frequently. This is most commonly used for a client program to communicate with a server. Examples are a web browser and web server, or client email and email server. The best example is web encryption because, by switching between HTTP and HTTPS in the URL, we can choose between a clear or encrypted version of a website.By default, most large companies are now using the encrypted form, and we can see that any visit to Google, Facebook, Microsoft Office 365 or other sites will be on the site's HTTPS version.

III. ONE TIME PAD

The term "one - time pad" refers to any encryption method that encrypts each byte of the plaintext which uses one byte key stream and use each key byte once and never again - and it's the only accurate secure cipher in use today. The one - time pad was re - invented in 1917, first described by Frank Miller in 1882.Random keys were written on paper sheets intended to form a pad together. The name, one - time pad, was used only once for each key. The following equation can be used to generalize the one - time pad encryption algorithm:

$Ci=E(P_i, K_i)$ for I=1,2,3,…,n

Where E is the encryption operation, Pi is the plaintext's I - th character, Ki is the key's I - th byte for that accurate message, Ci is the resulting cipher text's I - th character and n is the key stream's length. It is necessary to keep secret both the key stream K and the encryption operation E. One - Time Pad (OTP), also known as Vernam - cipher or the perfect cipher, is a crypto algorithm that combines plaintext with a random key.It is the only extant encryption that is mathematically invulnerable. A plaintext is combined with a random secret key (also known as a one - time pad) in this technique. Then, by merging it with the corresponding bit or character from the pad using modular addition, each bit or character of the plaintext is encrypted. When the key is

- truly random,
- non - deterministic,
- cannot not be reused ,and
- kept completely secret, it will be impossible to decrypt or break the resulting cipher text.

The key for each specific message is the starting location for the whole random key stream that is used for the encryption .While the term byte has been used and will continue to be used for each key stream unit, there is no need for each key unit to be 8 bits long.A key with larger units actually provides better protection against a known - plaintext attack.Since then, several key values can result in a given cipher text byte from the known plaintext byte.The plaintext may be encrypted in units other than 8-bit bytes equivalently. It has also been demonstrated that any cipher with the perfect secrecy property, it has to use the keys with the same requirements as OTP keys. For some critical diplomatic and military communication, nations used digital versions of one - time pad ciphers, butsecure key distribution problems have made them unworkable for most of the applications.

MILESTONE RESEARCH FOUNDATION
Int. Jrl. of Computational Learning & Intelligence
Vol. 02, Issue No. 01, 2023

Applicability of one time pad

The one - time pad has some effective interest. The one - time pad may be useful in some hypothetical spying situations as it can be computed by hand with only pencil and paper. Indeed, almost all other high - quality ciphers without computers are completely impractical. Agent can accept their pads from their "treaters" in person. However, computers in the modern world (such as those incorporated into personal electronic devices such as mobile phones) are omnipresent that having a computer suitable for typical encryption (for example,a phone capable of running hidden cryptographic software),will not usually be suspicious. With hypothetically perfect confidentiality, the one-time pad is the optimum cryptosystem.

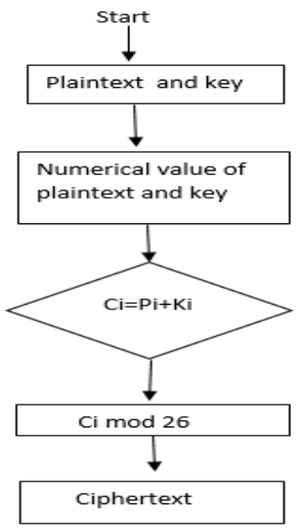
The one - time pad is one of the most feasible encryption methods where one or both parties are required to do all their work manually, without computer assistance.In the pre - computer era, this made it important,and it might still be useful in situations where computer occupancy is prohibited or where reliable computers are not available. One - time pads are feasible in situations where two parties must be able to vacate each other in a secure environment and communicate with perfect isolation from two separate secure environments. The most commonly correlated algorithm with the distribution of the quantum key is the one - time pad which can be used in overcoding .Stream ciphers imitated by the one - time pad technique.It can be part of a cryptography.An OTP may be unbreakable if the key is random and never reused.Any ciphertext may be decrypted using the appropriate key to any message of the same length.Thus, ciphertext alone cannot determine the actual original message, as all possible plaintexts are equally same.

Uses forOne-Time Pad:-

Using methodological taken from the one-time pad schema it is possible to store a password with multiple individuals or parts. All parts or shares of the encrypted password must be combined before the final password may be reviled.

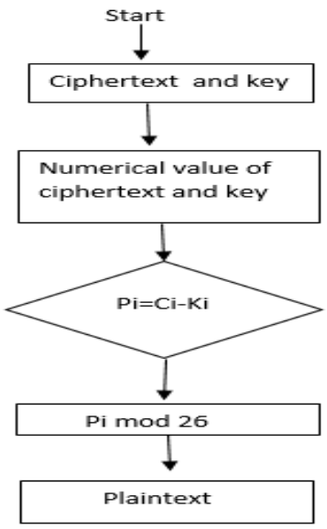
IV. PROCESS OF PAD TECHNIQUE

- Encryption Process of One Time Pad technique



- Decryption Process of One Time Pad technique

Pi = Plaintext, Ci = Cipher text, K = Key that is used based on the flow of encryption ,describes the stages in changing a document (plaintext) into a cipher text which starts from the input plaintext and key, and then apply the formula Ci= (Pi+Ki) mod 26, where the results obtained from implement of the formula such is the ciphertext. While the decryption process performed by the ciphertext input, the initial key, and the next step is to restore the cipher text into its original form, using a decryption formula Pi= (Ci-Ki) mod 26.



Algorithm for OTP

Step1:-Select the Plaintext and Key.
Step2:-Convert each letter from A to Z into the numbers from 0 to 25.
Step3:- Now plaintext number added to the random number of key.
Step4:-Perform modulo 26 with the resulted valueof ciphertext for each digit that results in Ciphertext.
Step5:- Now Ciphertext value issubtracted from the key value.
Step6:-Again calculate modulo 26 with the resulted value of Plaintext for each digit that results in the original Plaintext.

V. IMPLEMENTATION

Suppose Alice wants to send the message "START" to Bob which is a plaintext

```
S   T   A   R   T   plaintext
```

A Paintext is paired with a random secret key “POWER”. Each letter will be combined in a predetermined way with one letter of the message. (It is common, but not required, to assign each letter a numerical value, e.g., "A" is 0, "B" is 1, and so on.)

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

```
18  19   0   17   19   numerical value
                       Of plaintext
P   O    W   E    R    key
15  14   22  4    17   numerical value
                       Of key
```

The technique of one time pad is to combine the key and the message using “modular addition”.

	18	19	0	17	19	
	15	14	22	4	17	
=	33	33	22	21	36	→ plaintext + key

Calculate modulo 26 with the resulted value of plaintext and key.

	33	33	22	21	36	→ mod 26
=	7	7	22	21	10	→ value of mod 26
	H	H	W	V	K	→ ciphertext

The ciphertext to be sent to Bob is “HHWVK". Bob uses the matching key page and the same process, but in reverse, to obtain the plaintext.

H	H	W	V	K	ciphertext
P	O	W	E	R	key

In Decryption the key is subtracted from the ciphertext, again using modular arithmetic.

	7	7	22	21	10	
	15	14	22	4	17	
=	-8	-7	0	17	-7	→ ciphertext – key

Now Calculate modulo 26 with the resulted value of Ciphertext and key.

	-8	-7	0	17	-7	→ mod 26
	18	19	0	17	19	→ value of mod 26
	S	T	A	R	T	→ Original Plaintext

Thus Bob recovers Alice's plaintext, the message "START". Both Alice and Bob destroy the key immediately after use, thus preventing reuse and an attack against the cipher.

VI. CONCLUSION

One-time pad encryption is only possible if both sender and receiver are in possession of the same key which is more secure than steganography. The secure communications are therefore expected and planned within a specific time frame.In this proposed system the perfect cipher technique has been implemented by performing arithmetic operations. It is considered as the more secure type of encryption where the information is confidential. In order to use this algorithm, each party must possess the same random key. This typically involves meeting the other party in person or using a trusted messenger.

REFERENCES

1. Rubin, F. (1996). One-time pad cryptography. *Cryptologia*, *20*(4), 359-364.
2. Upadhyay, G., & Nene, M. J. (2016, May). One time pad generation using quantum superposition states. In *2016 IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT)* (pp. 1882-1886). IEEE.
3. Iqbal, M., Pane, M. S., & Siahaan, A. P. U. (2016). SMS Encryption Using One-Time Pad Cipher. *IOSR J. Comput. Eng*, *18*(6), 54-58.
4. Widiasari, I. R. (2012). Combining advanced encryption standard (AES) and one time pad (OTP) encryption for data security. *International Journal of Computer Applications*, *57*(20).
5. Ahmed, S. T., & Basha, S. M. (2022). *Information and Communication Theory-Source Coding Techniques-Part II*. MileStone Research Publications.
6. Wang, X., Wang, Y., Zhu, X., & Luo, C. (2020). A novel chaotic algorithm for image encryption utilizing one-time pad based on pixel level and DNA level. *Optics and Lasers in Engineering*, *125*, 105851.

7. Deepa, B., & Maheswari, V. (2022, January). An enhanced DNA structure for one-time pad together with graph labeling techniques. In *AIP Conference Proceedings* (Vol. 2385, No. 1, p. 130045). AIP Publishing LLC.
8. Basha, S. M., Ahmed, S. T., & Naidu, S. K. M. (2022). *Artificial Intelligence: Practical Approach* (Vol. 1). MileStone Research Publications.
9. Ragaventhiran, J., Vigneshwaran, P., Kodabagi, M. M., Ahmed, S. T., Ramadoss, P., & Megantoro, P. (2022). AN UNSUPERVISED MALWARE DETECTION SYSTEM FOR WINDOWS BASED SYSTEM CALL SEQUENCES. *Malaysian Journal of Computer Science*, 79-92.
10. Kuang, R., & Barbeau, M. (2022). Quantum permutation pad for universal quantum-safe cryptography. *Quantum Information Processing*, *21*(6), 1-22.