International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
Article Received: *25 July 2023* ***Revised:*** *12 September 2023* ***Accepted:*** *30 September 2023*

Data Encryption Strategies in Cloud Protecting Data at Rest and in Transita

[1]Rajashekar Reddy Yasani
Sr Cloud Security Engineer, Independent Security Researcher, Dallas,TX
Cloud Security, Cloud Computing, Cyber Security
rajshekaryasani@gmail.com

[2]Karthik Venkatesh Ratnam
Cloud Engineer, Independent Security Researcher, Boston, MA
Devsecops (cloud security)
karthikratnam1@gmail.com

ABSTRACT

In today's digital world, data encryption is an essential tool for protecting private information. The process entails applying encryption algorithms to convert readable data from its original format, known as plaintext, into an unreadable format, called ciphertext. In this way, the data is securely encrypted and cannot be accessed or understood by anybody without the correct decryption key. Symmetric and asymmetric encryption are the two most used forms. Symmetric encryption is an efficient method for protecting big volumes of data, but it demands careful key management because it uses the same key for both encryption and decryption. The use of two keys, public and private, in asymmetric encryption, also known as public-key encryption, increases security but also increases computing complexity. The security of data while it is in transit, such as information sent over networks, and data at rest, like information kept on physical drives, are both greatly enhanced by data encryption. Strong encryption methods, solid key management systems, strict access limits, and frequent protocol updates are all part of good security practice. The importance of encryption in safeguarding data from cyber risks and illegal access is highlighted by its broad use in different settings, such as cloud computing, mobile devices, and workplace networks.

Keywords: Cloud computing; data protection; data security; privacy; risks and threats.

1. INTRODUCTION

In order to protect sensitive information, data encryption uses encryption algorithms to transform the data into an unintelligible form called ciphertext [1]. With the proliferation of data breaches and cyberattacks in the modern digital age, protecting sensitive information must be a top priority.

Understanding Data Encryption

Data encryption is the practice of utilizing encryption algorithms to transform readable and understandable data from its original format, known as plaintext, into an unintelligible version, called ciphertext. Encryption makes it hard for anyone to read or interpret encrypted material unless they have the key to decode it [2]. Mathematical formulas govern the operation of encryption and decryption processes in encryption algorithms. Transforming plaintext into ciphertext and back again is the job of these algorithms, which rely on cryptographic keys. The complexity of the algorithm, the length of the cryptographic key, and the degree of unpredictability all contribute to the encryption strength [3].

Data encryption is primarily designed to protect the privacy and secrecy of sensitive information. Data stays unintelligible and unusable without the decryption key if it is encrypted, even if it is obtained by unwanted persons [4].

Importance of Data Security in the Digital Age

Companies like Google, Microsoft, and others have discovered that data is their new treasure in this digital world. Your information should be safe if you are utilizing a well-known and reputable provider. Maybe you're standing there. Still, even large corporations aren't immune to data breaches; what's more, some of them sell customer information to advertising firms, who then pay the hackers. After that, your information was simply shared with an outside company [5].

Data Encryption Basics

It is possible to restrict access to sensitive information by encrypting it so that only authorized parties may decipher it.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
***Article Received:** 25 July 2023 **Revised:** 12 September 2023 **Accepted:** 30 September 2023*

Protecting the privacy and authenticity of sensitive data is its primary function. Crucial to this procedure are encryption algorithms. Two primary categories of encryption algorithms are:

Symmetric Encryption

A single key is used for both the encryption and decryption processes in symmetric encryption. Two parties, the sender and the receiver, exchange keys. The sender converts plaintext to ciphertext by using the key during the encryption process [6]. After receiving the encrypted message, the receiver can recover the original plaintext by decrypting it using the identical key. Because of its speed and efficiency, this approach is well-suited for protecting massive datasets. Anyone in possession of the secret key can decode the data, thus keeping it safe while sharing and maintaining it is a major concern [7].

Asymmetric Encryption

In asymmetric encryption, which is also called public-key encryption, two keys—a public key and a private key—are utilized. To encrypt data, one uses the public key, and to decrypt it, one uses the private key [8]. The encryption process makes use of the publicly distributed public key, which is kept secret, and the decryption process makes use of the privately held private key. Although this method solves the key distribution issue with symmetric encryption, the mathematical calculations involved are difficult, thus it may be slower than other approaches [9].

2. LITERTAURE REVIEW

The public cloud is being utilized by a multitude of businesses in order to address a wide variety of business concerns. These concerns include expanding scalability, worldwide resilience, increasing dependability and performance, and expediting the deployment of applications. When it comes to the challenging process of shifting workloads and applications to the cloud, data security is typically at the forefront of people's minds. The number of documented cyberattacks on American firms increased by 69% in 2020 compared to 2019, as stated in the internet and crime report [10] published by the Federal Bureau of Investigation. Because of this, there are certain companies who are afraid to move their critical data to the cloud. This occurs when they have difficulty understanding the regulatory requirements that businesses are required to meet and when they investigate their security procedures.

It is not viable to simply create a data security policy for workloads that are stored on pre-existing premises. This is as a result of the fact that it does not take into account cloud-centric requirements and does not make advantage of the vast array of security capabilities that the cloud has to offer [11].

In order for organizations to successfully move data to the cloud in a manner that assures stringent safeguards, complies with regulatory requirements, and reduces risk, they need to rethink their outmoded data security procedures and build a plan that is suitable for the cloud. In order to accomplish this, you will need to examine how the cloud influences your existing on-premises strategy and then modify it such that it makes use of the wonderful cloud properties. Security specialists who have managed data security projects for on-premises installations are starting to come to the realization that their organization's shift to the cloud requires a reevaluation of the way in which data is protected [12]. Misconfiguration came in first place with 68 percent of the organizations that were asked to rate the major security threats associated with public clouds. Illegal access came in second with 58 percent, followed by unprotected interfaces with 52 percent, and account hijacking with 50 percent. As you will see, cloud-based data security strategies usually continue to use the well-known security patterns that have long protected data on-premises. In addition, cloud-based security strategies give a more modern security infrastructure that makes use of the efficiency and power that cloud platforms provide.

When you move your information technology infrastructure to the cloud, you are adopting a model known as shared responsibility [13]. Your operational burden is reduced as a result of this shared approach because the CSP is responsible for the operation, management, and control of all the layers of information technology components. These levels range from the host operating system and virtualization layer all the way down to the physical security of the premises in which the services are operated.

It is your role, along with that of your CSP, to manage, operate, and verify the controls of the information technology environment. You are also responsible for executing the software. That being said, your cloud service provider (CSP) is the one responsible for the security "of" the cloud, while you, as the client, are the one responsible for the security "in" the cloud [14]. The majority of security standards and compliance certifications, such as SOC 2, PCI-DSS, HIPAA/HITECH, FedRAMP, GDPR, FIPS 140-2, and NIST 800-171, are typically supported by contemporary public cloud service providers (CSPs), assisting clients in meeting compliance requirements for almost all international regulatory bodies [15].

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
Article Received: *25 July 2023* ***Revised:*** *12 September 2023* ***Accepted:*** *30 September 2023*

3. ROLE OF CRYPTOGRAPHIC KEYS IN ENCRYPTION

Encryption relies heavily on cryptographic keys. Data can be encrypted and decrypted using these. As previously stated, public keys and private keys are the two primary categories of cryptographic keys. Encrypted data can only be decoded using the corresponding key. Encryption becomes more robust as the key length increases. For optimal security, it is generally advised to use keys with a minimum of 2048 bits. To prevent compromise, keys must be generated, stored, and managed securely. The RSA and AES encryption techniques make use of these keys. Encryption and decryption employ the same algorithm, but they use separate keys.

Securing Data at Rest with Encryption

Physical storage drives, including hard disks, solid-state drives, and others, hold data when it is at rest. At the moment, neither this data nor its transmission are in use. The data remains susceptible to unwanted access even while it is not in motion, particularly in the event that the storage device is misplaced, stolen, or corrupted. Files kept on a computer's hard disk, information kept on a flash drive, or data maintained in a database are all instances of data at rest.

Importance of encrypting data at rest

Data at rest encryption is a must for keeping private information safe from prying eyes. Because sensitive information is not encrypted, it is easy for a malevolent person to read and steal it if they physically obtain the storage device. Data is encrypted when it is changed into an unintelligible form that can only be read by someone with the correct decryption key. In the event that the storage device is hacked, the data will still be safe thanks to this additional safeguard.

Full Disk Encryption

By employing full disk encryption (FDE) shown in figure 1, one can secure an entire storage device, encrypting not just data but also the operating system and user folders. The right encryption key is required to decrypt data using this method. Data at rest is well-protected with FDE since it prevents illegal access regardless of the whereabouts of the storage device.

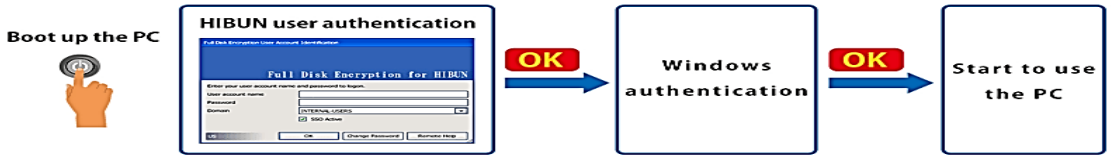

Fig 1: full disk encryption (FDE)

File-level encryption

Instead of encrypting the whole storage device, file-level encryption encrypts specific files or folders. The authorized user decrypts a file whenever they access it, since each file is encrypted independently. This method allows for finer-grained management over encrypted files, but it necessitates handling encryption keys individually for each file. Fig 2 shows File Encryption and file Decryption.

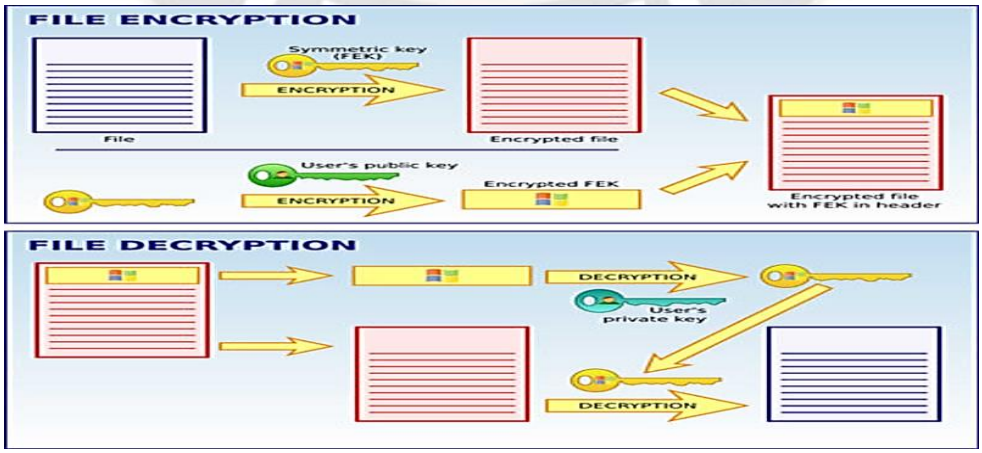

Fig 2: File Encryption and file Decryption.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
***Article Received:** 25 July 2023 **Revised:** 12 September 2023 **Accepted:** 30 September 2023*

Database Encryption

Data held within databases is the primary focus of database encryption. You have the option to encrypt the whole database, just the tables that hold sensitive information, or even individual columns. Even if a malicious actor manages to obtain access to the database files, the data will remain encrypted and indecipherable without the correct keys, thanks to database encryption and was shown in figure 3.

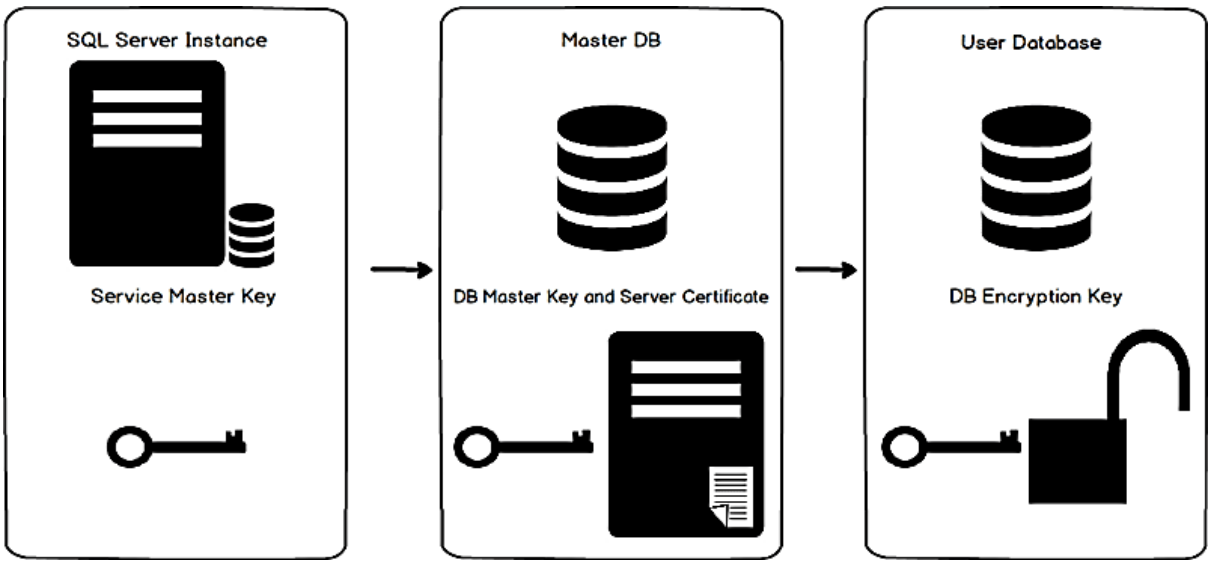

Fig 3: Database Encryption

4. BEST PRACTICES FOR DATA AT REST ENCRYPTION

The five most critical guidelines for encrypting data when it is at rest are as follows:

Encryption Algorithms

Implement robust encryption methods, such as AES (Advanced Encryption Standard), using keys of an adequate length (128-bit, 256-bit). If the encryption is strong enough, reading the encrypted data will be very difficult, even if unauthorized individuals manage to get their hands on it.

Key Management

Establish strong procedures for managing keys. Ideally, you should use trusted key management systems or hardware security modules (HSMs) to store the encryption keys independently of the encrypted data. Unauthorized individuals cannot access sensitive data if keys are not managed properly.

Access Control and Authentication

Implement robust authentication and access control measures. The encrypted data should only be accessible to authorized individuals who have the correct authentication credentials. An additional safeguard is provided by multi-factor authentication.

Regular Security Assessments

Make sure your encryption implementation is secure by regularly auditing and assessing it. Maintaining the efficacy of your encryption requires regular testing to keep ahead of potential attacks.

Employee Training and Awareness

Make sure your staff is well-versed in the best practices for data encryption and security. Every employee has a responsibility to know how to properly handle encryption keys, apply secure authentication, and adhere to data handling policies in order to keep encrypted data secure.

Securing Data in Transit with Encryption

There is always some kind of data in transit whenever it travels from one location to another across a network. Just think about it: every time you send a message, share a photo, or make a financial transaction online, data is in transit. Unauthorized parties may be able to intercept the data as it travels from your device to a server.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
***Article Received:** 25 July 2023 **Revised:** 12 September 2023 **Accepted:** 30 September 2023*

5. IMPORTANCE OF ENCRYPTING DATA IN TRANSIT

Protecting the privacy and security of sensitive data requires the use of data encryption while in transit. Sending sensitive material in this way is analogous to placing it in a locked envelope. Hackers and thieves could potentially gain access to and utilize your data if it is not encrypted. Encryption makes it nearly impossible for unauthorized parties to decipher your data by converting it into a code that can only be deciphered by the authorized recipient. To those who do not possess the decryption key, it will seem like a chaotic mess of letters. The data you store will be even more protected with this.

SSL/TLS protocols for secure communication

Protocols for security include SSL and TLS. They make it possible for websites and web browsers to communicate in a safe and secured way. Because of this, you may rest assured that any information transmitted between them will stay secret and unreadable. To secure sensitive information, many websites employ SSL/TLS. Throughout the transfer, they safeguard your data. A secure connection (SSL or TLS) is used when the address of a website begins with https: This ensures that your information, including passwords, is securely delivered to the website. Online businesses and banks are examples of websites that frequently employ SSL/TLS protocols because of the sensitive nature of the information they handle and was shown in figure 4. Credit card information and login passwords are among the data types that are encrypted when transmitted to these websites. Online communications and transactions are now safer because of this.

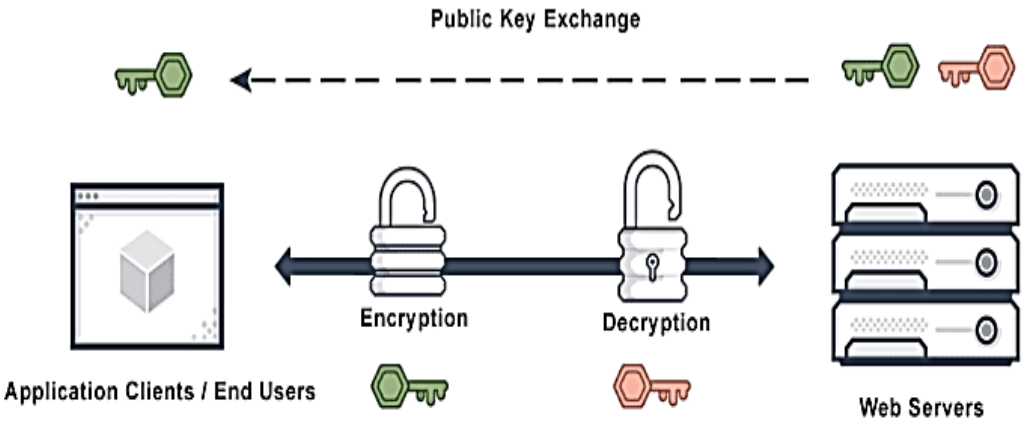

Fig 4: SSL/TLS protocols.

VPN (Virtual Private Network) encryption

To protect your anonymity and data when surfing the web on public Wi-Fi, a virtual private network (VPN) encrypts all of your traffic and was shown in figure 5. A virtual private network (VPN) encrypts and tunnels all of your network traffic through its secure server whenever you connect to one. No one will be able to intercept or alter your data while it is in route because of this. Virtual private networks encrypt your data while it is in transit using a variety of standards, including OpenVPN, IPSec, and AES-256. This encrypts all of your data, making it unintelligible to anyone other than the VPN server and your device. Your VPN service provider will provide you an IP address the moment you establish a connection to their server. This will alter your perceived location and mask your real IP address. The security and privacy offered by VPN encryption is second to none. Nevertheless, the encryption standards utilized by the VPN service determine this. There can be security holes in some suppliers.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
Article Received: *25 July 2023* ***Revised:*** *12 September 2023* ***Accepted:*** *30 September 2023*

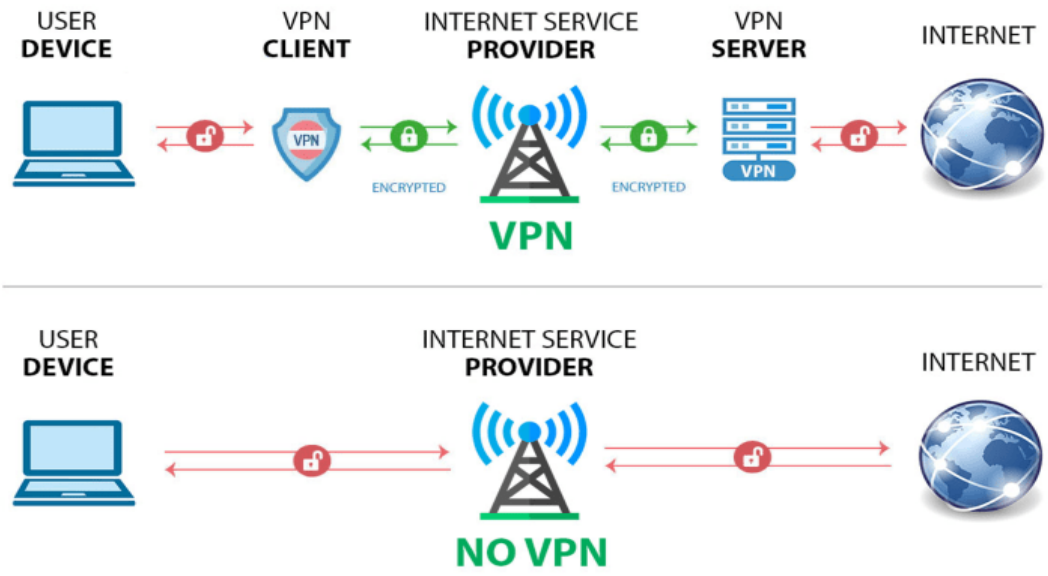

Fig 5: VPN (Virtual Private Network) encryption

Email encryption

Encrypting emails with cryptographic methods ensures that only the person who sent them can decipher them and it was shown in figure 6. By utilizing the recipient's public key, an encrypted email is transformed into ciphertext, rendering it unintelligible. To restore the message's original, readable form, decryption requires the recipient's private key. Both end-to-end and transport layer encryption are commonly used for email security. Your message will be securely encrypted on both your device and the recipient's device with end-to-end encryption. Even email providers are unable to access the content because of this. In contrast, email security during transmission between servers is ensured by transport layer encryption. While the email is in transit, it is protected from prying eyes.

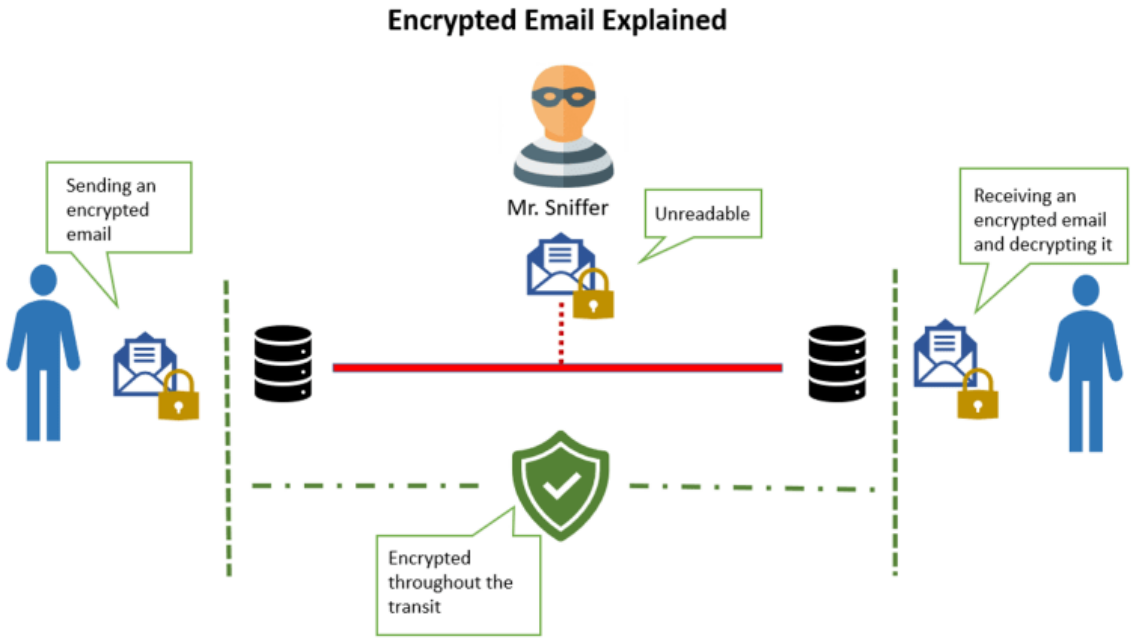

Fig 6: Encrypted Email Explained.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
***Article Received:** 25 July 2023 **Revised:** 12 September 2023 **Accepted:** 30 September 2023*

6. BEST PRACTICES FOR DATA IN TRANSIT ENCRYPTION

The five most critical guidelines for encrypting data while it is in transit are as follows:

Use Strong Encryption Protocols

Protect information at rest and in transit by using a trusted encryption protocol, such as Secure Sockets Layer (SSL) or Transport Layer Security (TLS). Data remains private and safe from interception due to these protocols, which set up an encrypted connection between your device and the server.

Implement Virtual Private Networks (VPNs):

Make use of VPNs to set up an encrypted "tunnel" that all your data can pass through. Virtual private networks (VPNs) encrypt data in transit and block eavesdropping, providing an additional safeguard, particularly when connecting to public Wi-Fi networks.

Enable Two-Factor Authentication (2FA)

Verify your account access with two-factor authentication whenever you can. With two-factor authentication (2FA), an additional verification step—often a number texted to your phone—is added, enhancing security even if your password is compromised.

Regularly Update Software and Systems

Always use the most recent versions of your operating system, web browser, and security software. Updates to software frequently contain fixes for security holes, making it less likely that malicious actors will be able to exploit them.

Be Cautious with Public Wi-Fi

Keep in mind that data eavesdropping is a real possibility when utilizing public Wi-Fi networks. To keep your data more secure when using public Wi-Fi, connect using a reliable VPN.

7. COMMON ENCRYPTION TECHNOLOGIES AND TOOLS

Data, communications, and networks can be protected using a variety of encryption technologies and tools. When it comes to protecting sensitive data, several encryption methods are indispensable.

Advanced Encryption Standard (AES)

One popular way to encrypt data such that it can't be read without the right decryption key is with the Advanced Encryption Standard (AES). Imagine it as a key that, when entered, unlocks specific pieces of data. To further understand how AES works, think of it as a digital lock that requires a unique key to unlock and decrypt data.

RSA Encryption

An analogy that might be made to RSA encryption is the use of virtual keys and locks. To encrypt your communication, you'll need a public key, and the receiver will need a private key to decrypt it. This way, the message can only be viewed by the person who is supposed to receive it. Picture this: you're sending a letter that can only be opened with the special key that the receiver has. It was created by Leonard Adleman, Ron Rivest, and Adi Shamir.

Elliptic Curve Cryptography

When compared to RSA, the key sizes of Elliptic Curve Cryptography (ECC) are significantly smaller, yet it still provides strong security. The theory of elliptic curves on finite fields is the foundation of ECC. When compared to competing methods, it can achieve the same degree of security while using significantly smaller key sizes. To illustrate the point, a 3072-bit RSA key is just as secure as a 256-bit ECC key. Devices with limited resources, like mobile phones and smart cards, benefit greatly from this improvement to ECC's computing power and memory utilization efficiency.

Data Encryption in Various Environments

Now more than ever, protecting our private data is a top priority. Protecting our data from breaches and illegal access is the primary function of data encryption. To improve data security, it is helpful to use encryption techniques in various settings.

Encryption in cloud computing

Data storage and processing in the cloud has recently grown in popularity. There are two main factors to think about while implementing encryption in the cloud:

Cloud Storage Encryption

We must take extra precautions to guarantee that our data remains indecipherable in the event that an unauthorized third party gains access to our cloud storage. Data stored in the cloud can be encrypted so that only authorized users can decipher it. A hacker who gains access to the cloud will not be able to read the stolen data unless they possess the correct key.

Encryption for cloud-based applications

The cloud hosts many of the programs that we use on a daily basis, such as email and collaboration tools. Protecting information as it moves from your smartphone to the server

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
***Article Received:** 25 July 2023 **Revised:** 12 September 2023 **Accepted:** 30 September 2023*

in the cloud is what encryption for these apps is all about. By doing so, sensitive data cannot be intercepted by hackers while it is in route.

Encryption for On-Premises Systems

The term "on-premises systems" refers to the practice whereby an enterprise keeps its critical information and applications on servers and computers located inside the enterprise's own physical location, such as an office or data center. Since they are physically present at their workplace, they are able to exert control over these systems. Encrypting your data is similar to this. It is very difficult to decipher encrypted data without the corresponding decryption key. This key is analogous to the one that opens your home's safe. This key is necessary to decipher the secret code and restore the original data.

Mobile Device Encryption

A great deal of private and sensitive data is kept on portable electronic devices such as tablets and smartphones. Encrypting data on a mobile device means that no one other than you, armed with a password or PIN, can decipher it. Assuming your password is secure, your data will be safe even if someone were to steal or lose your device.

Encryption in Enterprise Networks

It is common practice for large corporations to use interconnected networks to communicate data across different departments and locations. Data in transit between departments within an organization is protected by encryption in corporate networks. This protects the data from possible transmission breaches or eavesdropping.

Key Lifecycle Management

An encryption key is analogous to a secret code that allows us to access and secure sensitive information. Encryption keys are like house keys in that they must be kept secure in order to prevent unauthorized access to sensitive information. Managing keys during their whole "life" is equivalent to providing care for these unique keys. Key lifecycle management encompasses generating, distributing, using, storing, and, finally, retiring keys.

Key Generation

Producing robust, randomly generated encryption keys is the initial stage of key lifecycle management. Keys with a high entropy or randomness level are often generated using cryptographic methods in this procedure.

Key Usage

After we have these keys, we encrypt our data using them. This ensures that only those who have the correct key can decipher it. To keep the encrypted data private and uncompromised, it is crucial to employ keys appropriately and securely.

Key Storage

It is crucial to store these keys safely. Encryption keys are quite sensitive, so we must take the same precautions as we would with our house keys.

Key Rotation

Crucial parts of key management that ensure encrypted data remains secure over time are key rotation and disposal. Part of these procedures includes making sure to dispose of obsolete or compromised encryption keys in a secure manner and change them frequently.

Key Deletion or Key Disposal

There are occasions when specific keys are no longer necessary. Encryption keys, like any other worn-out key, need to be disposed of in a proper manner to prevent their misuse.

Wrapping up

Protecting private information is of the utmost importance in today's environment, when these assets are more precious than ever. Encryption, the practice of transforming data into a secret code, now serves as our digital protector. Whether your data is safely stored on a server or traversing the expansive internet, we have discussed the wonders of encryption technology. Your data is protected against eavesdropping by learning about encryption at rest and in transit. Never forget that encryption at rest keeps your data safe in a secure vault while it's not in use, and encryption in transit keeps it safe when it moves from one digital location to another.

CONCLUSION

In today's interconnected digital world, data encryption is a crucial tool for protecting sensitive information. Data remains secure even if it comes into the wrong hands thanks to encryption, which converts plaintext into ciphertext using robust algorithms. While symmetric encryption is great for efficiency and speed, asymmetric encryption is great for increased security when it comes to key distribution, and both approaches are essential in their own right. Data at rest, like files saved on physical devices, and data in transit, like information carried across networks, are both critically

vulnerable without encryption. The use of robust encryption techniques, secure management of cryptographic keys, and regular system updates are all best practices that may be put into place to bolster data protection. From cloud computing to mobile devices and workplace networks, encryption will always be an essential part of cybersecurity methods for protecting digital information, no matter how technology advances. Finally, by using encryption, you can ensure the safety of your digital life. Encryption acts as a rock-solid barrier, protecting your data from possible dangers as you utilize internet services, purchase, interact, and operate remotely. No matter where your data is going or how long it's been traveling, encryption technologies will keep it private and secure in our linked world.

REFERENCES

1. Abbate P. 2020 Internet Crime Report. Federal Bureau of Investigations. 2021;3. Available:https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf
2. Schulze H. 2020 Cloud Security Report [ISC2]. Cybersecurity INSIDERS. 2021;8. Available:https://www.cybersecurityinsiders.com/wpcontent/uploads/2020/08/2020-Cloud-SecurityReportISC2.pdf&ved=2ahUKEwi05dLb04_6AhV7x QIHHaMuCOcQFnoECA0QAQ&usg=AOvVaw3VnzUFhyieI7fwKTTrQclM
3. Amazon Web Services. AWS Security and Compliance Quick Reference Guide. AWS. 2021;8. Available:https://d1.awsstatic.com/executiveinsights/en_US/guide-security-compliancequick-reference.pdf
4. Lance A, Chuvakin A. Designing and deploying a data security strategy with Google Cloud. Google Cloud. 2021;10. Available:https://cloud.google.com/blog/products/identity-security/start-a-data-securityprogram-in-a-cloud-native-way-on-googlecloud
5. App security not keeping up with rapid development — Radware. [Blog]; 2021. Retrieved 12 September 2022, from https://securitybrief.com.au/story/app-securitynot-keeping-up-with-rapid-developmentradware/
6. Muraidhara, P. (2013). Security issues in cloud computing and its countermeasures. International Journal of Scientific & Engineering Research, 4(10).
7. Sriram, I., & Khajeh-Hosseini, A. (2010). Research agenda in cloud technologies. arXiv preprint arXiv:1001.3259.
8. Yonbawi, S., Alahmari, S., Daniel, R., Lydia, E. L., Ishak, M. K., Alkahtani, H. K., ... & Mostafa, S. M. (2023). Modified Metaheuristics with Transfer Learning Based Insect Pest Classification for Agricultural Crops. Computer Systems Science & Engineering, 46(3).
9. Lee, E., Rabbi, F., Almashaqbeh, H., Aljarbouh, A., Ascencio, J., & Bystrova, N. V. (2023, March). The issue of software reliability in program code cloning. In AIP Conference Proceedings (Vol. 2700, No. 1). AIP Publishing.
10. Sharmili, N., Yonbawi, S., Alahmari, S., Lydia, E. L., Ishak, M. K., Alkahtani, H. K., ... & Mostafa, S. M. (2023). Earthworm Optimization with Improved SqueezeNet Enabled Facial Expression Recognition Model. Computer Systems Science & Engineering, 46(2).
11. Rutskiy, V., Aljarbouh, A., Thommandru, A., Elkin, S., Amrani, Y. E., Semina, E., ... & Tsarev, R. (2022). Prospects for the Use of Artificial Intelligence to Combat Fraud in Bank Payments. In Proceedings of the Computational Methods in Systems and Software (pp. 959-971). Cham: Springer International Publishing.
12. Aljarbouh, A., Tsarev, R., Robles, A. S., Elkin, S., Gogoleva, I., Nikolaeva, I., & Varyan, I. (2022). Application of the K-medians Clustering Algorithm for Test Analysis in Elearning. In Proceedings of the Computational Methods in Systems and Software (pp. 249- 256). Cham: Springer International Publishing
13. Albarakati, A. J., Boujoudar, Y., Azeroual, M., Eliysaouy, L., Kotb, H., Aljarbouh, A., ... & Pupkov, A. (2022). Microgrid energy management and monitoring systems: A comprehensive review. Frontiers in Energy Research, 10, 1097858.
14. Bouti, A., & Keller, A. J. (2012). Securing cloud-based computations against malicious providers. *Journal of ACM SIGOPS Operating Systems Review*, *46*(1), 38-42.
15. Buyya, R., Vecchiola, C., & Selvi, S. T. (2013). *Mastering Cloud Computing: Foundations and Applications Programming* (1st ed.). Morgan Kaufmann Publishers. ISBN-13: 978-0124114548.