OPEN ACCESS Freely available online

Journal of Information Technology & Software Engineering

Commentary

Encryption of Data Using Efficient Key-Dependent Cryptography for Public Cloud Security

Reyad Noura*

Department of Information Technology, University of Florence, Firenze, Italy

DESCRIPTION

Now-a-days, all human activities revolve around computer systems. Cryptography is a method for encrypting data and communications by using codes. So that only the intended audience can read and comprehend it. Data and communications are protected using cryptography so that only the sender and the intended receiver may access them. Cryptography can ultimately prevent data from being changed or stolen. It can also be used to verify user identities. In order to keep electronic data and messages secure and readable by the intended parties only, cryptography frequently uses encryption and an algorithm. There has been cryptography for ages. We use this computing technology for a variety of purposes, including banking, software, marketing, healthcare, and education. We might be curious in how businesses safeguard their data. In computer science, the term "cryptography" refers to safe information and communication methods that use mathematical principles and a system of calculations based on rules or algorithms to change messages in ways that are challenging to read. These deterministic algorithms are employed in the production of cryptographic keys, digital signature, online browsing on the internet, and private communications like email and credit card transactions. Symmetric key cryptography and asymmetric key cryptography are the two basic categories into which cryptography is divided. Data can be encrypted and decrypted using modern cryptography's algorithms and ciphers, such as 128-bit and 256-bit encryption keys.

Modern ciphers are thought to be nearly impenetrable, such as the Advanced Encryption Standard (AES). The field of cybersecurity known as cryptology combines elements of computer science, engineering, and mathematics to produce sophisticated codes that conceal a message's real meaning. Since the time of the ancient Egyptian hieroglyphics, cryptography has been used to secure communication and information in transit and keep it from being read by unauthorized parties. In order to secure data privacy, credit card transactions, email, and online browsing, it makes use of mechanisms like cryptographic keys and digital signing. In the area of quantum computing, cryptography is anticipated to take on a more significant role. Many of the present cryptography techniques will be vulnerable to attack when quantum computers grow in power. This will necessitate the creation of novel, quantum-resistant encryption methods. Cryptography has a assuring and is expected to stay an essential instrument for protecting the security and privacy of our online communications. In computer security, cryptography is frequently used, especially for creating and managing passwords.

With this method, the passwords are encrypted, preventing unauthorized users from reading them even if they gain access to the password database. Cryptography is used to ensure online browsing security, protecting users from listening in and man-in-the-middle attacks. Public key cryptography is used by the Secure Sockets Layer (SSL) and Transport Layer Security (TLS) protocols to encrypt data transferred between the web server and the client, establishing a secure communication channel. Attackers are able to defeat cryptography, gain access to the computers in charge of data encryption and decryption, and take advantage of poor-quality implementations such the usage of default keys. On the other hand, encryption makes it more challenging for attackers to access messages and data. In order for cryptographic techniques to be used as intended, they must be both powerful and simple to use. Even in cases when the hardware is lost, stolen, or hacked, the use of encryption functions can aid in preventing the loss or theft of data. Instead of relying on security through obscurity, a robust cryptosystem should be able to stand up to the scrutiny of the security community. Instead, the mechanism should be public knowledge, with the actual keys being the only thing kept private and unseen.

Digital currencies like Bitcoin also used cryptography to safeguard transactions and circumvents. Transactions are protected by intricate algorithms and cryptographic keys, making it nearly impossible to tamper with or counterfeit the transactions. Electronic signatures are used to sign papers and act as the handwritten signature's digital replica. Public key cryptography is used to validate digital signatures after they have been established using cryptography. Electronic signatures are becoming more prevalent, and numerous nations have passed laws requiring them.

Correspondence to: Reyad Noura, Department of Information Technology, University of Florence, Firenze, Italy, E-mail: noureyad@bks.it

Received: 21-Jun-2023, Manuscript No. JITSE-23-26316; **Editor assigned:** 23-Jun-2023, PreQC No. JITSE-23-26316 (PQ); **Reviewed:** 07-Jul-2023, QC No. JITSE-23-26316; **Revised:** 14-Jul-2023, Manuscript No. JITSE-23-26316 (R); **Published:** 21-Jul-2023, DOI: 10.35248/2165-7866.23.13.345

Citation: Noura R (2023) Encryption of Data Using Efficient Key-Dependent Cryptography for Public Cloud Security. J Inform Tech Softw Eng. 13:345.

Data and communications can be shielded from illegal access and disclosure using an encryption technique. Confidentiality, integrity, authenticity, non-repudiation, security, scalability, ease of use, adaptability, legal protection, interoperability with other systems internationally, increased productivity, and increased competitiveness are only a few benefits. For people and organizations longing to safeguard the privacy, integrity, and authenticity of their communications, cryptography is an invaluable instrument because of these benefits.