Cryptography integration for data encryption and secure communication

Amritesh Tiwari
Department of Computer Science and Engineering,
Lovely Professional University,
Kapurthala, Punjab, India
amriteshtiwari2003@gmail.com

Harika Gade
Department of Computer science and Engineering
Lovely Professional University,
Kapurthala, Punjab, India
harikagade.3339@gmail.com

Jahnavi Sarkar
Department of Computer Science and Engineering
Lovely Professional University,
Kapurthala, Punjab, India
sarkarjahnavi03@gmail.com

Abstract:-

This article aims to provide detailed information about how and where cryptography is used in this modern era. what is cryptography? and its vital role in secure communications and data protection. Furthermore, this paper focuses on the integration of cryptographic techniques within various applications and systems, highlighting the importance of cryptographic standards in cybersecurity risks. and what's a pivotal role cryptography plays in protecting sensitive information in an increasingly digitalized world. Cryptography plays a major role in protecting sensitive information against malicious users and unauthorized access.

Introduction:

Cryptography, the art of secure communication and data protection, has experienced more advancements in recent years. cryptography means conversion of plain text to cipher text or conversion of cipher text to plain text. Plain text is easily understandable by hackers or anyone, whereas ciphar text is not that easy to understand cause its locked by sender, if sender provides the encrypted key, then it's easy to understand or else not. Strong encryption methods and secure protocols are now essential due to the rapid advancement of technology and more usage of digital platforms. To guarantee the confidentiality, integrity, and validity of information in the digital world, **cryptography** offers the necessary tools and techniques. highlighting its vital role in

securing communication and protecting sensitive data. This transformation is achieved through various mathematical algorithms and cryptographic techniques. ciphar is a secret message that sender encrypts data and receiver decrypts the data. Cryptography is mainly used for network security and its a methods to secure information and communication through use of codes .Encryption process translates information using algorithms that makes original content unreadable, to protect data in digital world where messaging applications are used rapidly for communication the messages we sent on air is always prone to getting hacked by hackers to overcome this we use cryptography techniques .Encryption and decryption falls under blanket of cryptography, cryptography keys are categorised into 2 different ways 1)Symmetric key and 2)Asymmetric key. Symmetric key refers as 1 key that is being used by sender as well as receiver whereas Asymmetric key refers as different keys such as private key and public key, private key is used for decryption and it is known to a particular person and public key is used for encryption and it is known for everyone. The most popular symmetric key cryptography system is known as DES(data encryption system) and popular asymmetric key algorithms such as RSA,DSA,Elliptic curve etc and there are some security goals for safeguarding data such as confidentiality, integrity, availability and security services such as data confidentiality, data integrity, authentication, non-repudiation, access control.taliking about security attacks these are of two types 1)passive attack 2)active attack , passive attacks are difficult to detect

and further dived into 2 types 1)release of message content 2)traffic analysis, active attack is further dived into subtypes named:1)masquerade 2)modification of messages 3)replay 4)denial of

services, we can prevent these types of attacks by using better encryption techniques.

II.LITERATURE REVIEW:

Historical Development of Cryptography

The term "cryptography" has its origin from Greek words "Krypto" meaning hidden and "graphien" meaning to write, can be defined as the process of converting a plain text information into a coded information (ciphertext) . The one who does this encoding and decoding is known as cryptosystem and the main motive is to exclude any unauthorized person from the information. A formal definition can be "Cryptography is the mathematical science of transformation of clear data into the certain form that could be an automatic deciphering of the transformation is virtually impossible by other than intended recipient.

Technological advancements have not only benefited the honest user leading to the secure and faster way of communication over the network but also a dishonest user in cracking the information. Image data with medical records, online purchases using credit cards, cellular phone conversations and secure line of VPN are few such examples that demand the security of the data being transmitted over the network.

Source: Mandrita Mondal, Kumar S. Ray - 2019 - arxiv.org. Review on DNA Cryptography. [PDF]
Maria Velema - 2013 - arxiv.org. Classical Encryption and Authentication under Quantum Attacks. [PDF]
Anderson Gonçalves Marco, Alexandre Souto Martinez, Odemir Martinez Bruno - 2012 - arxiv.org. Fast, parallel and secure cryptography algorithm using Lorenz's attractor. [PDF]
Owen Lo, William J. Buchanan, Sarwar Sayeed, Pavlos Papadopoulos, Nikolaos Pitropakis, Christos Chrysoulas - 2022 - arxiv.org. GLASS: A Citizen-Centric Distributed Data-Sharing Model within an e-Governance Architecture. [PDF]
Philip Chan, Itzel Lucio-Martínez, Xiaofan Mo, Wolfgang Tittel - 2011 - arxiv.org. Quantum Key Distribution. [PDF]
Christiana Chamon - 2021 - arxiv.org. Random Number Generator, Zero-Crossing, and Nonlinearity Attacks against the Kirchhoff-Law-Johnson-Noise (KLJN) Secure Key Exchange Protocol. [PDF]

Principles of Cryptography

Symmetric and asymmetric algorithms are the backbone of encryption and are the de facto tool for protecting information. Symmetric key ciphers are very fast and do not add a lot of overhead to the data being protected. Asymmetric key ciphers are relatively new compared to symmetric key ciphers but provide a great service in key management. They add more security to the data they are protecting because of the infeasibility of deriving the decryption key from the encryption key. They also do not require secure channels to exchange keys. This will be explained more thoroughly throughout the essay but is important to understanding why key management for asymmetric algorithms can be quite different from that of symmetric.

Source: Peter P. Rohde, Vijay Mohan, Sinclair Davidson, Chris Berg, Darcy Allen, Gavin K. Brennen, Jason Potts - 2021 - arxiv.org. Quantum crypto-economics: Blockchain prediction markets for the evolution of quantum technology. [PDF]
Horace Yuen - 2016 - arxiv.org. Security of Quantum Key Distribution. [PDF]
Nicolas Gisin, Grégoire Ribordy, Wolfgang Tittel, Hugo Zbinden - 2001 - arxiv.org. Quantum Cryptography. [PDF]

Applications of Cryptography in Data Security

Data can be encrypted at several different points in the cloud – at the server, during transfer to and from the server, and on the endpoints of the cloud service. When protection of data throughout its entire lifecycle is necessary, a consistent encryption method whereby the data is only in an unencrypted state when it is being accessed is most effective. A powerful method to achieving automatic and consistent data protection is to have the data and the encryption keys stored on the customer's premises, with the actual encryption and decryption occurring at a separate data centre. This method allows the customer to implement and manage their own encryption method with minimal impact on the way data is accessed and used. In the case where a business simply wants to have all data that is transferred to and stored in the cloud always encrypted, a simple yet effective method is to use the public cloud server as a remote location to archive the data stored in a private cloud. Both encryption methods and deployed applications must ensure the scalability and seamless integration of encryption methods that are vital to success in the cloud.

Encryption of sensitive information is the principal method to achieving data security. To translate information into a secure format, companies typically use products such as encryption appliances or VPN for data while it is being transmitted, and use storage encryption technology or software applications to translate data into an encrypted form. Encrypted data, also known as ciphertext, must be translated back into its original form (plaintext) in order to be understood. In order to ensure the security of transmitted information, encryption/decryption and the keys that are used must be secure. High-speed decryption can subject encrypted data stored on portable media to a brute force attack, so the method of encryption and strength of the algorithm are vital. Keys used to encrypt and decrypt data should be transmitted in an encrypted format for heightened security.

Source: Lynda kacha, Abdelhafid Zitouni - 2018 - arxiv.org. An Overview on Data Security in Cloud Computing. [PDF]
Mazharul Islam - 2023 - arxiv.org. A Practical Framework for Storing and Searching Encrypted Data on Cloud Storage. [PDF]
Mazharul Islam - 2023 - arxiv.org. A Practical Framework for Storing and Searching Encrypted Data on Cloud Storage. [PDF]
Ryan Amiri, Erika Andersson - 2015 - arxiv.org. Unconditionally Secure Quantum Signatures. [PDF]
Pablo Daniel Marcillo Lara, Daniel Alejandro Maldonado-Ruiz, Santiago Daniel Arrais Díaz, Lorena Isabel Barona López, Ángel Leonardo Valdivieso Caraguay - 2019 - arxiv.org. Trends on Computer Security: Cryptography, User Authentication, Denial of Service and Intrusion Detection. [PDF]
Adedayo M. Balogun, Shao Ying Zhu - 2013 - arxiv.org. Privacy Impacts of Data Encryption on the Efficiency of Digital Forensics Technology. [PDF]

Challenges and Limitations

Two major types of cryptanalytic attack exist: known plaintext and chosen plaintext. Known plaintext attacks are less common, as they involve a cryptanalyst who has a set of plaintext and ciphertext and is looking for the key used to encrypt the text. In chosen plaintext attacks, a cryptanalyst either knows how to encrypt using the cryptosystem or has a device that can do so. The attacker then has one of these devices encrypt specific plaintext and tries to derive the corresponding ciphertext. This is more dangerous than a known plaintext attack and usually means the cryptanalyst is close to breaking the cryptosystem. In both types of attacks, the cryptanalyst tries to deduce the key used in the cryptosystem and then use it to decrypt ciphertext other than the text used to find the key. The vulnerability of a cryptosystem to these types of attacks depends solely on the strength of the key. If the strength of the key is equivalent to the strength of the ciphertext in the sense that there is only one possible key, then the cryptosystem is immune to known plaintext and chosen plaintext attacks. This condition is difficult to achieve in theory and practice with modern computers since even a simple algorithm can generate many possible keys, and the task of the cryptanalyst can become key exhaustion rather than a direct attack. However, given a set of n keys, the cryptosystem is effectively n times stronger than it would be with a single key.

Source: Horace P. Yuen, Ranjith Nair, Eric Corndorf, Gregory S. Kanter, Prem Kumar - 2005 - arxiv.org. On the security of AlphaEta: Response to `Some attacks on quantum-based cryptographic protocols'. [PDF]
Hasindu Gamaarachchi, Harsha Ganegoda - 2018 - arxiv.org. Power Analysis Based Side Channel Attack. [PDF]
Chengqing Li, Yuansheng Liu, Leo Yu Zhang, Michael Z. Q. Chen - 2012 - arxiv.org. Breaking a chaotic image encryption algorithm based on modulo addition and XOR operation. [PDF]

Recent Advances in Cryptographic Research
Homomorphic encryption is a form of encryption that allows computation on ciphertexts, generating an encrypted result which when decrypted, matches the result of the operations as if they had been performed on the plaintext. The homomorphism property is valuable because it allows computation to be carried out on encrypted data without access to a private key. The first fully homomorphic encryption scheme was presented by Craig Gentry in 2009. In the last few years, the speed of homomorphic encryption has seen great improvements. These improvements began in 2010 when Marten van Dijk, Craig Gentry, Shai Halevi, and Vinod Vaikuntanathan showed that somewhat

homomorphic encryption could be achieved using ideal lattice-based encryption. Later that year, Chris Peikert and Vaikuntanathan showed that the learning with errors (LWE) problem is a good candidate for a basis of cryptosystems, and in 2011 they and several others demonstrated fully homomorphic encryption. Full implementation of homomorphic encryption by companies such as Microsoft Research and IBM has allowed for practical use with the encryption technique.

Source: Tanvi S. Patel, Srinivasakranthikiran Kolachina, Daxesh P. Patel, Pranav S. Shrivastav - 2022 - arxiv.org. Comparative evaluation of different methods of "Homomorphic Encryption" and "Traditional Encryption" on a dataset with current problems and developments. [PDF]
Louis J. M. Aslett, Pedro M. Esperança, Chris C. Holmes - 2015 - arxiv.org. A review of homomorphic encryption and software tools for encrypted statistical machine learning. [PDF]
Zhiyong Zheng, Fengxia Liu, Kun Tian - 2023 - arxiv.org. An Unbounded Fully Homomorphic Encryption Scheme Based on Ideal Lattices and Chinese Remainder Theorem. [PDF]

III. Methodology

Research Design

Literature review of existing cryptographic methods and protocols
The primary goal of a cryptographic method or protocol is to provide the users of the method with some desirable security guarantees, the strongest of which is usually considered to be that of "semantic security crystal 2003", which loosely states that an adversary even with substantial computational power cannot learn anything about the private messages being sent. Other security guarantees are usually specific to the type of protocol being used and are often subjective to the implemented method. A protocol often begins with some party of users wishing to perform a function on some data, while other parties interact with them trying to obtain or subvert that data. A cryptographic protocol for this function is the composition of one or more methods of encryption and decryption of the data, and methods of authentication of the identities of the users, all carried out in accordance with the desired security guarantees. Step by step analysis of the composition will have one or more users be in some state of knowledge at a point in the protocol, and an eventual desired state can be defined as completion of the function with the same private data. A security breach in this type of protocol is usually defined as revelation or alteration of the data by a user who is not legitimate in the context of the function.

Cryptographic methods have increased in public awareness in recent years, with the internet and electronic commerce providing the need for secure communication and transactions. The field of cryptography is concerned with the construction and analysis of protocols that prevent third parties or the public from reading private messages, and the subsequent protocols in various subfields of information security that provide access to a message that is kept secret. In today's global networks, and the generally increasing size of the electronic world, the problems that people are concerned with are gradually coming to resemble the security issues that governments, companies, and individuals have attempted to address with continued varying success. This continues to provide motivation for new work on cryptographic protocols and methods, the results of which will span the duration of the information age into the unforeseeable future.

Source: Tommaso Gagliardoni, Andreas Hülsing, Christian Schaffner - 2015 - arxiv.org. Semantic Security and Indistinguishability in the Quantum World. [PDF]
Moritz Wiese, Holger Boche - 2021 - arxiv.org. Mosaics of combinatorial designs for information-theoretic security. [PDF]
Gorjan Alagic, Anne Broadbent, Bill Fefferman, Tommaso Gagliardoni, Christian Schaffner, Michael St. Jules - 2016 - arxiv.org. Computational Security of Quantum Encryption. [PDF]
Alexander Poremba - 2017 - arxiv.org. Quantum Learning Algorithms and Post-Quantum Cryptography. [PDF]
Phillip J. Brooke, Richard F. Paige - 2013 - arxiv.org. The Value of User-Visible Internet Cryptography. [PDF]
Philip Chan, Itzel Lucio-Martínez, Xiaofan Mo, Wolfgang Tittel - 2011 - arxiv.org. Quantum Key Distribution. [PDF]

Data Analysis

Qualitative Analysis of Cryptographic Approaches

The purpose of this research is to bring together and document some of the most dependable private key cryptosystems in use today. By describing an assortment of attacks on these cryptosystems (some of which are not widely known to the security community), we enlighten cryptanalysts on the efficiency of their attacks and also show system designers how to build safer cryptosystems. This work should dispel the general belief that the Feistel Structure suffices for the design of a secure cryptosystem and should persuade readers that constructing provably secure cryptosystems based on permutation or substitution functions is a complex task. To aid in the process, we introduce a methodology for classifying key-dependent functions at both the primitive and cryptosystem level. Finally, we make the distinction between Type I and Type II deterministic algorithms and show that it is possible to build public key cryptosystems that are as secure as their private key counterparts.

Source: L. Evain, "Knapsack cryptosystems built on NP-hard instance," 2008. [PDF]

P. Bergamo, P. D'Arco, A. De Santis, and L. Kocarev, "Security of public key cryptosystems based on Chebyshev Polynomials," 2004. [PDF]

M. Kaplan, G. Leurent, A. Leverrier, and M. Naya-Plasencia, "Quantum Differential and Linear Cryptanalysis," 2015. [PDF]

IV. Proposed Framework for Cryptography Integration

Secure Communication Protocols

The first goal is confidentiality. This is achieved using symmetric encryption to conceal the content of the message. The second goal is data integrity. This involves using a message authentication code to ensure the data has not been tampered with during its transfer. If the message is changed at any point, then the MAC will fail to authenticate the data, and the SSL/TLS session will be dropped. The third goal is authentication. This is done by either having the server authenticate itself to the client or by also having the client authenticate itself to the server. When the server authenticates itself to the client, the client will use the public key infrastructure to verify the server's public key and to check that the server possesses the correct private key. This method is used by most SSL/TLS sessions and is sufficient if the client is reluctant to reveal its identity. If the client needs to also authenticate itself to the server, a separate key pair will need to be stored by the client, and a certificate for this key pair will be required. This method is usually reserved for situations such as online banking where both parties want assurance of each other's identity.

Transport Layer Security (TLS) and its predecessor, Secure Sockets Layer (SSL), are protocols that provide secure communication across a network between two computers. Their goals are data privacy and data integrity between the two communicating applications. TLS and SSL are widely used in secure internet (web) transactions or secure transmission of e-mail. An implicit and essential aspect of the protocols is that of server authentication. This is accomplished by the server sending its certificate to the client. The client, using the relevant methods, checks the validity of the server certificate. If the certificate is authenticated, the client will generate a pre-master secret and will encrypt it with the server's public key. The server can then decrypt the pre-master secret using its private key. This is how confidentiality is provided for the rest of the session. SSL and TLS have three goals when encrypting data.

Source: Rainer Falk, Steffen Fries, Hans-Joachim Hof - 2015 - arxiv.org. Secure Communication Using Electronic Identity Cards for Voice over IP Communication, Home Energy Management, and eMobility. [PDF]

Mahdi Nikooghadam, Hamid Reza Shahriari - 2022 - arxiv.org. Comment on "Provably secure biometric-based client-server secure communication over unreliable networks". [PDF]

Jesus Diaz, David Arroyo, Francisco B. Rodriguez - 2012 - arxiv.org. Formal security analysis of registration protocols for interactive systems: a methodology and a case of study. [PDF]

End-to-End Encryption Solutions

The Signal Protocol is a cryptographic protocol that provides end-to-end encryption for privacy-focused secure messaging. The protocol defines a double ratchet algorithm which operates on a pair of ephemeral keys used to provide forward secrecy, future secrecy, and post-compromise security for the session. The algorithm combines the cryptographic ratchet with a ratchet based on the key hierarchy. A triple Diffie-Hellman (3-DH) handshake is used to provide the additional security with identity hiding forward secure property. The

first 2 DH exchanges are used to mutually authenticate the two parties. The 3rd DH is used to provide the root key which is used to initialize the double ratchet algorithm. This structure is used to provide an alternative to the STS (station-to-station) protocol in a way that is specifically designed to protect metadata. In order to defend against man-in-the-middle attacks, the session keys are tied to the intended communicants' long-term identity keys, and the Double Ratchet uses public-key cryptography with these identity keys to provide encryption. In the case that a communicant's identity key is changed, the Double Ratchet will provide a way to securely transition to a new identity key pair. This is done by including an identity key pairing in the ratcheting data and creating a new ratcheting data structure for the new pair. The new structure will be used after both parties have sent a message with the new keys and will not be used prior to that time. This will ensure that the compromise of an identity key will only affect the security of messages whose keys were exposed. Ephemeral keys are periodically rotated to provide future secrecy for older messages, and lost messages or state compromise can be recovered from if a new session is initialized with a new ratcheting key, provided that the previous state was securely deleted. Finally, the protocol is designed to be robust against all known passive and active attacks on encrypted data and to hide metadata.

Source: Dennis Heinze, Jiska Classen, Felix Rohrbach - 2020 - arxiv.org. MagicPairing: Apple's Take on Securing Bluetooth Peripherals. [PDF]
Christian Johansen, Aulon Mujaj, Hamed Arshad, Josef Noll - 2018 - arxiv.org. The Snowden Phone: A Comparative Survey of Secure Instant Messaging Mobile Applications. [PDF]
Boel Nelson, Elena Pagnin, Aslan Askarov - 2022 - arxiv.org. Metadata Privacy Beyond Tunneling for Instant Messaging. [PDF]

Cryptographic Tools for Data Protection
The victor proclamation was made on November 26, 2001, and the FIPS Publication 197 determined the AES. Runtime execution has remained an essential thought for some genuine clients of encryption, so we were satisfied that effective and exceedingly refined execution strategies provided details regarding the Rijndael calculation are workable and entirely secure. Be that as it may, the course taken has reasonably realized to a substantially more prominent accentuation on other security qualities: an extensive variety of potential applications with to some degree unique prerequisites, the basic significance of institutionalization and interoperability, and a longing for clear and general scientific confirmation of security attributes. Thus, the NIST esteem of having an open calculation to be considered by experts from numerous groups has been recognized, and we anticipate an extensive variety of both examination and useful applications of the AES.

The motivation for the Advanced Encryption Standard (AES) was to set up a Federal Information Processing Standard (FIPS) distributing that would indicate an unclassified, open calculation equipped for encoding touchy government data and that may be utilized by offices and temporary workers for securing data. This objective was refined by the National Institute of Standards and Technology (NIST) in a straightforward way so as to unquestionably decide a victor in a challenge between contrasting calculation entries. The challenge procedure required execution of an extensive variety of possibility calculations in a few programming dialects and stages, the accommodation of execution measurements and test vectors and rounds of assessment and dialog of the outcomes. An essential part of the general methodology—and one that was not at first expected—was that exact documentation of the calculations themselves would be required to agree to the assessment criteria and to encourage the examination of their execution comes about.

Source: Sumith Yesudasan - 2021 - arxiv.org. Generating and Managing Strong Passwords using Hotel Mnemonic. [PDF]
Hyunwook Lee, Seungmin Jin, Hyeshin Chu, Hongkyu Lim, Sungahn Ko - 2021 - arxiv.org. Learning to Remember Patterns: Pattern Matching Memory Networks for Traffic Forecasting. [PDF]
Mansoor Ebrahim, Shujaat Khan, Umer Bin Khalid - 2014 - arxiv.org. Symmetric Algorithm Survey: A Comparative Analysis. [PDF]

Source: Jaydip Sen, Javier Franco-Contreras, Gouenou Coatrieux, Nilay K Sangani, Haroot Zarger, Faouzi Jaidi, Bob Duncan, Alfred Bratterud, Andreas Happe, Chin-Feng Lin, Che-Wei Liu, Walid Elgeanidi, Muftah Fraifer, Thomas Newe, Eoin OConnell, Avijit Mathur, Ruolin Zhang, Eric Filiol - 2017 - arxiv.org. Advances in Security in Computing and Communications. [PDF]

Jahnavi Reddy, Nelly Elsayed, Zag ElSayed, Murat Ozer - 2021 - arxiv.org. Data Breaches in Healthcare Security Systems. [PDF]
Paul Lesov - 2010 - arxiv.org. Database Security: A Historical Perspective. [PDF]

Policy and Regulatory Considerations

Compliance with data protection regulations As the concept of electronic health records (EHRs) evolves, it is important to ensure that health data is protected against breaches of confidentiality and improper uses of data. There are many instances where health data is not protected. For example, in a recent study in New Zealand, it was found that 16% of the websites of the top primary care organizations provided ways for patients to communicate personal health information that was not secure. This lack of security in protecting patient health information could lead to a breach of the Health Information Privacy Code, of which the health entities may be in breach. EHRs have huge potential to improve healthcare delivery, but with the potential for good also comes the potential for harm if the data is not kept safe. In order to mitigate these potential harms to patients, it is important for all health entities to become familiar with data protection issues related to EHRs. And given the international nature of EHRs, it is also worth considering the implications of storing and transmitting data offshore, as different legislation in other countries may affect the level of protection given to patient health information.

Conclusion

In conclusion, the rapid demand for secure communication and data security has impressive improvements in cryptography in recent years. The development of cryptography, homomorphic encryption, blockchain-based cryptography, and secure communication protocols has addressed the challenges posed by quantum computing. Through the use of various cryptographic techniques such as encryption, hashing etc data can be securely transmitted and stored, safeguarding it from unauthorized access, and interception. Furthermore, cryptography plays a crucial role in trusting online transactions and communication channels. It act as backbone of secure communication protocols, e-commerce platforms, and other applications where privacy and security are important factors, as we can see growth in technology nowadays, rate of cyber threats increasing rapidly this can be fixed or resolved by cryptography and its techniques, research and innovation in cryptographic techniques and protocols are essential to stay ahead of emerging threats and ensure the ongoing security of digital systems in digital world. Source: Alberto Sardi, Alessandro Rizzi, Enrico Sorano, Anna Guerrieri - 2021 - arxiv.org. Cyber Risk in Health Facilities: A Systematic Literature Review. [PDF]. Lawrence Nehemiah - 2014 - arxiv.org. Towards EHR interoperability in Tanzania hospitals: Issues, Challenges and Opportunities. [PDF]. Alberto Sardi, Alessandro Rizzi, Enrico Sorano, Anna Guerrieri - 2021 - arxiv.org. Cyber Risk in Health Facilities: A Systematic Literature Review. [PDF]