QRYPTIC

TEAM NAME AND TEAM MEMBERS:

QuantData

Member 1: Khushee Kapoor

Member 2: Shreya Akurathi

Member 3: Supriti Rosita

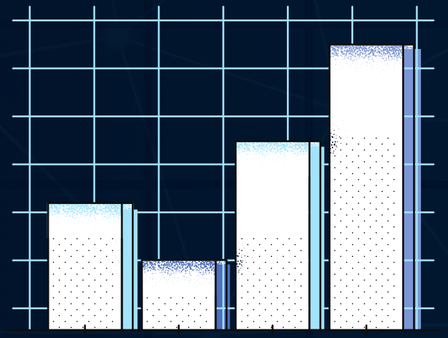
Member 4: Shreeyanka Das

THEME

Build a quantum-safe crypto-algorithm for future-proofing Amex’s sensitive data

PROBLEM STATEMENT

As a global financial services company, Amex provides a range of payment products and personal finance management tools to millions of customers worldwide. However, the increasing frequency of cyberattacks targeting financial institutions poses a significant threat to the security of sensitive customer data held by Amex. Moreover, the emergence of quantum computers presents an additional vulnerability to traditional encryption algorithms like RSA and ECC. Shor's Algorithm, and Grover's Algorithm among others can be used to bypass these techniques. Given these challenges, there is a critical need for innovative solutions that can enhance the protection of customer data within Amex's personal finance management tools and online account management features.



In 2021, there were over 623 million cyberattacks recorded globally

Average cost of a data breach is estimated to be $3.86 million

73 days - for conntainment efforts

206 days - to identifying a data breach

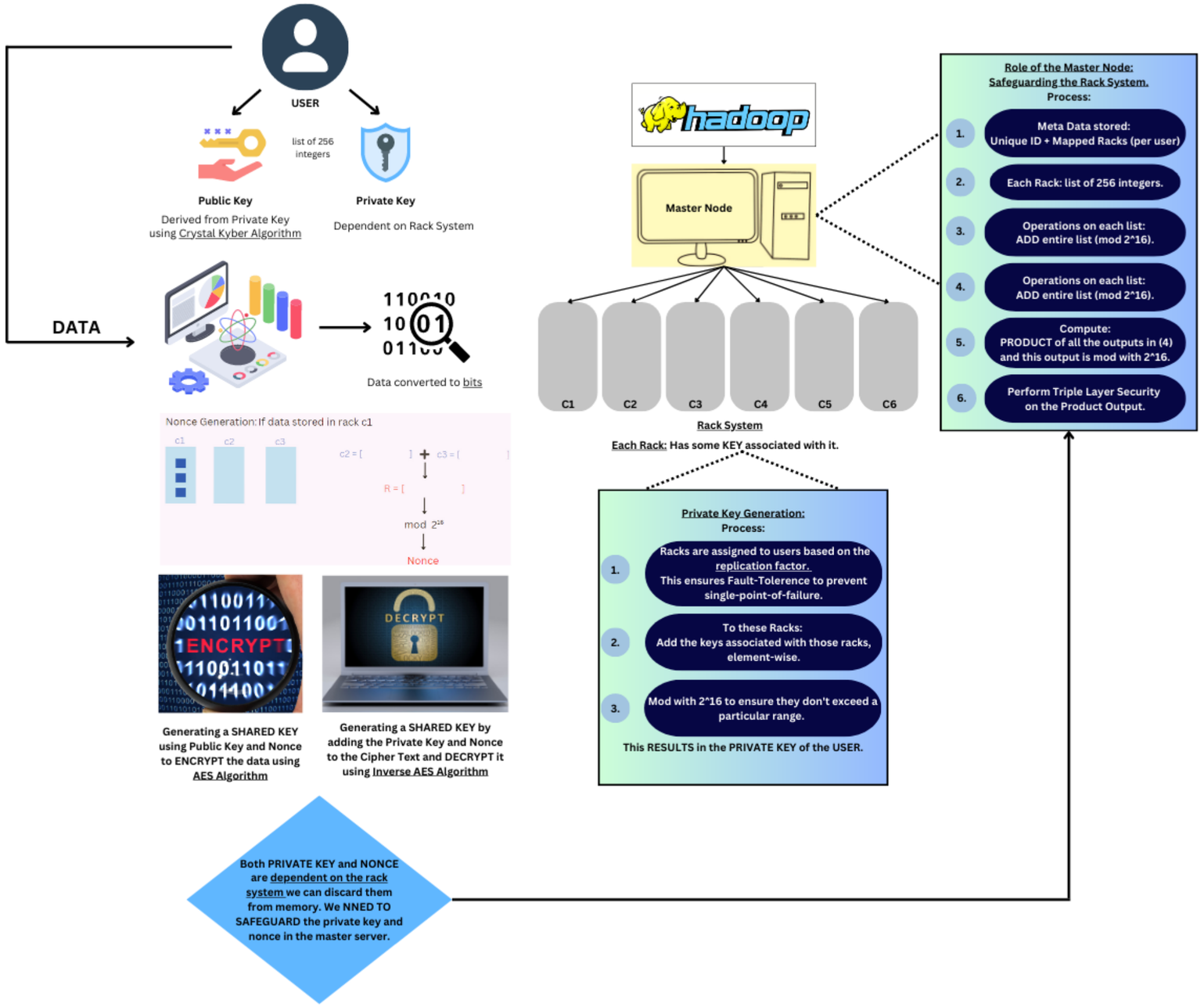
SOLUTION

We propose a novel algorithm that combines big data analytics tools with quantum-safe methodologies to provide a comprehensive, highly secure, and future-proof approach for safeguarding the confidentiality and integrity of sensitive data.

Designed to be impervious to attacks from quantum computers, the algorithm offers resistance from vulnerabilities, ensuring protection against cryptographic attacks employing quantum algorithms as well.

By seamlessly integrating these techniques, our algorithm provides a holistic solution at the forefront of modern cryptography.

METHODOLOGY


USER
list of 256 integers
Public Key
Derived from Private Key using Crystal Kyber Algorithm
Private Key
Dependent on Rack System
DATA
Data converted to bits
Nonce Generation: If data stored in rack c1
c1
c2
c3
c2 = [ ] + c3 = [ ]
R = [ ]
mod 2^16
Nonce
ENCRYPT
DECRYPT
Generating a SHARED KEY using Public Key and Nonce to ENCRYPT the data using AES Algorithm
Generating a SHARED KEY by adding the Private Key and Nonce to the Cipher Text and DECRYPT it using Inverse AES Algorithm
hadoop
Master Node
C1
C2
C3
C4
C5
C6
Rack System
Each Rack: Has some KEY associated with it.
Private Key Generation:
Process:
1. Racks are assigned to users based on the replication factor. This ensures Fault-Tolerence to prevent single-point-of-failure.
2. To these Racks: Add the keys associated with those racks, element-wise.
3. Mod with 2^16 to ensure they don't exceed a particular range.
This RESULTS in the PRIVATE KEY of the USER.
Role of the Master Node: Safeguarding the Rack System.
Process:
1. Meta Data stored: Unique ID + Mapped Racks (per user)
2. Each Rack: list of 256 integers.
3. Operations on each list: ADD entire list (mod 2^16).
4. Operations on each list: ADD entire list (mod 2^16).
5. Compute: PRODUCT of all the outputs in (4) and this output is mod with 2^16.
6. Perform Triple Layer Security on the Product Output.
Both PRIVATE KEY and NONCE are dependent on the rack system we can discard them from memory. We NNED TO SAFEGUARD the private key and nonce in the master server.

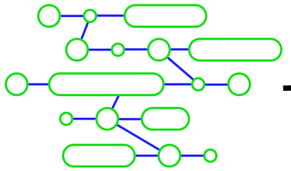
MODEL ARCHITECTURE

User

Private Key

Public Key

Nonce



Data

Bytes of data

Cipher Text

mod 2^{16}

R = [ ]

Element wise addition of 256 integers across 3 vectors

c1 = [ ]
c2 = [ ]
c3 = [ ]

Rack System(Hadoop)

Master Node

Rack System

c1 = [ ]
c2 = [ ]
c3 = [ ]

Addition of all 256 integers in a vector

mod 2^{16}
mod 2^{16}
mod 2^{16}

mod 2^{16}

Multiply integers to get 1 integer

SHA 3

hash

SHA 3

hash

hash

CRYSTAL Kyber Encryption + AES

LINKS TO PROTOTYPE

LINK TO VIDEO DEMOS AND EXPLAINATION

LINK TO GOOGLE COLAB NOTEBOOK

FUTURE SCOPE

- Our modular solution allows for easy replacement of SHA-3 with more advanced algorithms like Blake in the future, ensuring optimal performance and adaptability.

TECH STACK

- We have successfully implemented a prototype of our algorithm using Python and Google Colab.

- In future, we aim to seamlessly integrate our algorithm into existing functional pipelines using big data frameworks like Hadoop. This will enhance scalability and enable efficient processing and analysis of large-scale data.

SALIENT FEATURES

01 3 Level security

We propose a robust data encryption scheme implemented at the master node, employing the SHA-3 algorithm for hashing, and fortified with quantum-resistant encryption powered by CRYSTALS Kyber.

02 Double Hashing

The data is enhanced with an additional layer of protection through the utilization of the SHA-3 algorithm, wherein the bytes are intricately enveloped between two hashes.

03 Private Key generation for data encryption

We introduce a novel and distinctive element-wise approach for incorporating the user's private key and nonce, providing an innovative method for enhancing security in cryptographic protocols.

IMPACT METRICS

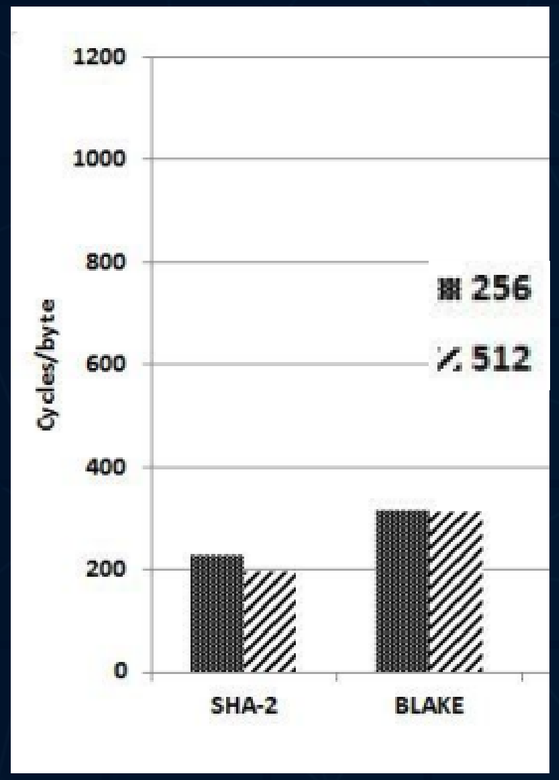
- **Key Size:** Our algorithm boasts a large key size of 256 integers, making it exceedingly difficult to breach and ensuring enhanced security against unauthorized access.
- **Key Generation:** The intricate key generation method employed in our algorithm ensures that the private key remains impervious to cracking attempts, bolstering the overall resilience of the cryptographic system.
- **Computations:** Significantly reducing the number of computations required, our algorithm offers improved efficiency without compromising security, enabling faster cryptographic operations.

IMPACT METRICS

Our proposed quantum-safe crypto-algorithm effectively mitigates the risks associated with various theoretical security metrics, including:

- Our algorithm safeguards against replay attacks by preventing malicious interception and replaying of recorded messages, ensuring communication integrity and thwarting unauthorized access.
- Our algorithm employs advanced cryptographic techniques to defend against eavesdropping attacks, ensuring the confidentiality and privacy of transmitted data and protecting sensitive information from unauthorized interception.
- Our algorithm provides robust protection against chosen cipher text attacks by utilizing advanced encryption schemes, preventing unauthorized access and information disclosure by thwarting attackers from selecting specific cipher texts and obtaining decrypted plaintext.

COMPARISON OF HASHING ALGORITHMS



Graph Source 1
Graph Source 2

ASSUMPTIONS,REASONING CONSTRAINTS

- **The user's private key will be stored safely and its integrity will be maintained. To ensure the security of the cryptographic system, it is crucial to handle and store private keys securely, protecting them from unauthorized access or tampering.**

- **Crystals-Kyber is a NIST-certified quantum-proof algorithm. The NIST certification validates the quantum-resistant properties of the Crystals-Kyber algorithm, providing assurance that it can withstand attacks from quantum computers.**

- **SHA-3 is relatively quantum-proof for large outputs and is more secure than its predecessors, making it more resistant to attacks, including those leveraging quantum computing capabilities.**

- **The replication factor assigned in the rack system ensures fault tolerance. By replicating data across multiple racks, any failures in individual racks can be mitigated, ensuring continuous availability and reliability of the system.**

POTENTIAL USE CASES

These use cases highlight the versatility and applicability of our algorithm in securing various aspects of Amex's operations, from payment processing to personal finance management and data storage. By adopting our solution, Amex can proactively address the evolving threat landscape and maintain a robust security posture, instilling trust and confidence in their customers' financial transactions and data privacy.

- **Personal Finance Management**: By integrating our algorithm into Amex's personal finance management tools, sensitive customer data, including account balances, transaction histories, and budgeting information, can be encrypted using quantum-safe methodologies. This use case safeguards the confidentiality and integrity of personal financial data, preventing unauthorized access and ensuring privacy.

- **Data Storage and Backup**: Implementing our algorithm within Amex's data storage and backup infrastructure enhances the security of critical financial data. By utilizing the SHA-3 algorithm for hashing and quantum-resistant encryption, the algorithm protects sensitive information stored in databases or cloud storage from potential breaches, ensuring data integrity and mitigating the risk of unauthorized access.

- **Secure Online Payments**: Our algorithm can be implemented within Amex's payment processing systems to ensure secure and quantum-resistant encryption of transaction data. This use case protects customers' financial information from potential attacks, offering enhanced security and peace of mind during online transactions.

thank you!