

Cryptography and Its Parameters

Authors: Mitanshu Holkar¹; Tushar Chiplunkar²; Palash Mehta³; Rohit Singh⁴; Yuvraj Bapna⁵

B.Tech 7th Sem SVKM's NMIMS Indore^{1,2,3,4,5}

Abstract—By using encryption, messages and other data are transmitted in a way that only their intended recipients can decode them. This process is known as cryptography. It was initially used for written communications. Modern computers made cryptography an essential tool for protecting various kinds of digital data. In this research paper, a brief of Cryptographic algorithms, theories, and various applications of Cryptography has been discussed. The applications which are discussed in this research paper are Cryptography in Cloud Computing, D2D Communication, Security key authentication techniques, Intrusion Detection Systems and Blockchain.

Keywords—Cloud Cryptography, D2D Communication, Key Authentication Technique, Intrusion Detection System, Blockchain

I. INTRODUCTION

In a world full of the Internet, Information, and data, security becomes a crucial aspect of protecting such data from breach, mishandling, and unauthorized usage. With the increase in data transferring and Information sharing, cybercrimes, Hacking, and Misuse of data has increased drastically. To protect the information/data from being compromised while communicating between two entities, Cryptography plays an important role. Cryptography refers to the Encryption and Decryption of data being transferred in a communication activity between two entities. Cryptography works on various algorithms and methods defined by various experts and practitioners. Various theories have been defined for cryptography, which helps us understand the algorithms and implementation.

II. CLOUD CRYPTOGRAPHY

In the world of digital media all over, cloud computing plays an important role in providing on-demand access to data whenever the user needs it. It provides a virtual space for the user for storing their data and using the applications. Since most Cloud Computing works on public cloud resources, the security of the data becomes a major concern.

To prevent user data from being hacked or misused by a third party, cloud cryptography is used. In Cloud cryptography, the encryption of user data is done using cryptographic algorithms to generate cipher data so

that even if the data is breached by a third party, it will be in encrypted form, and a key is used for the algorithm to decrypt the data again to its original form. There are two main types of cryptography algorithms are used, symmetric key cryptography, where a single key is used to encrypt and decrypt the data, and Asymmetric key cryptography, where a dual key is used, one for encryption and one for decryption.

The algorithms used in cloud cryptography are:

1. Advance Encryption: AES takes 128 bits of the input message, which is passed into a number of rounds. The number of rounds is variable and depends on the key length. For example – 128 bits keys require 10 rounds, and 192 bits require 12 rounds. The Rounds contain Shift rows operations, Mix Columns, and add round key functions.
2. Data Encryption Standard – It uses 64-bit input and 64-bit output. A single key is used for both encryption and decryption. Initial permutation happens to the input and passes to the round function. Here 16 round functions are used. The 64-bit key is permuted first and then sent to the left circular shift and then again sent to permuted choice and then to the round function. The same step is repeated for all 16 rounds. At last, 32-bit swapping is done and then after the initial permutation, we finally get the cipher text.
3. RSAAlgorithm- Two keys are used which are the public and private keys, messages which are encrypted using the private key, can get decrypted by the public key.
4. Hashing Key Cryptography – Methods like SHA-1, SHA-1, MD5, SHA-2, MD5, MD4, and SHA-3 are used.
5. Homographic Encryption – To preserve the integrity of data, this technique is used. It is used to compute the result of the cipher text by validating the results that should match the process of encrypting the plaintext. It has three classifications – partially homographic encryption, somewhat homographic encryption, and fully homographic encryption.

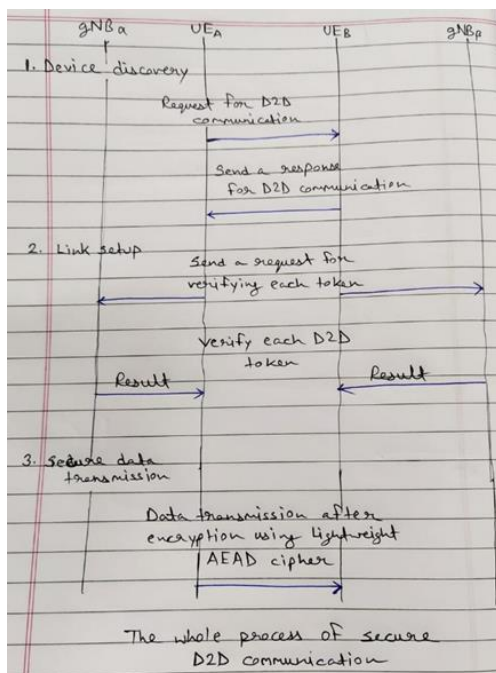
III. D2D COMMUNICATION

The Internet of Things (IoT) with the advancements of numerous technologies opens a decent variety of the

latest applications like smart appliances, smart cities, and smart grids. Despite its quality and worth, it creates a replacement attack surface for hackers notably on very unnatural devices that have restricted memory footprints and method power. These unnatural devices generally use documented cryptography with Associated info (AEAD) to secure info held on inside the devices and transmitted over the network. During this paper, they need to use a lightweight secret writing core in hardware with the support for AEAD to secure IoT applications on vulnerable devices.

D2D communication could be a mechanism between devices to transfer data securely. D2D communication helps cut back the bottom station's energy consumption by transmitting information directly between devices.

Firstly, the token is generated and then the next step is the link setup for a communication session. Before the communication session, it checks for the D2D token through the history of the device. And lastly, the transmission of data takes place. In D2D communication, the gap between devices is sort of shorter than the gap between a tool and a base station. This implies the interference of frequency decreases in a D2D communication situation, and it helps to transmit multiple pieces of information.



The whole process of secure D2D communication

Lightweight cryptography could be a reasonably secret writing methodology that chooses a touch footprint and/or low method quality. The aim is toward increasing the applications of cryptography to affected devices and its connected international standardization and tips compilation square measure presently afoot. A block cipher is often used in a mode of operation. Notably, authenticated secret writing with associated info (AEAD) that provides confidentiality and credibility is widely used.

IV. INTRUSION DETECTION SYSTEM

Internet & online procedures are increasing day by day which requires some secure channel, and every person needs some network security practices. There are some threats and sources which got attacked by some bugs and harmed the operating system and softwares that are used to become more functional and larger in size. Users' data & files which got attacked by some intruders have the right to access these data and store some valuable and private information that is provided by the user unknowingly. Firewall are hardware or software systems which are placed along two or more computer networks to stop the attacks which occur on any user's system. It is also true that Firewalls are not only sufficient for the network security as it protects from external attacks but not from internal attacks. Here, The Intrusion Detection System plays an important role which tries to stop the attacks.

IDSs collect the information from a computer or other computer networks in order to detect the attack and misuses of the system. IDSs analyze the attacks and some of them try to stop these attacks at the time of intrusion. Intrusion Detection System (IDS) monitors the system which detects some malicious activities and gives the alerts about the attacks which are detected by the system. It monitors, scans, looks for malicious activities, analyzes some patterns in the network, gives alerts upon detecting the unwanted intrusion activity that comes in contact with the user.

Intrusion Detection Network developed by ISS. There are 4 types of Intrusion Detection System which are as follows:

- a) **Network Intrusion Detection System:** A Network Intrusion Detection System is installed at a strategic location throughout the network. All devices on the network are monitored by NIDS. It looks at the data

traveling across the whole subnet and compares it to the information included in the packets' metadata and payloads.

- b) **Host Intrusion Detection System:** HIDS only looks at the device's incoming and outgoing data. It monitors the device for any abnormal behavior and notifies the administrator of any findings. HIDS also compares a snapshot of the current file system with a snapshot of the previous file system to determine whether any system files have been moved. This data structure is used to hold information analyzed from network traffic.
- c) **Protocol-Based System:** To safeguard their servers, businesses install intrusion detection systems based on protocol at the server's front end. Protocols between the server and the user are interpreted by it. For the HTTP server, this is a necessary part of the protocol.
- d) **Application-Based System:** It is common practice to deploy Application Protocol Based IDS inside a cluster of servers. It analyzes the server's internal communications with its apps to spot the intruder.

Intrusion Detection System has many functions that are very useful for the user's perspective. Some of the functions that are very useful are as follows:

- a) **Data Collection:** The intrusion detection system's efficacy relies heavily on its data collecting technique (IDS). Upon completion of this section, the Data is sent on to the IDS as an input. Information is logged and processed later.
- b) **Feature Selection:** Keys for infiltration might be extracted from the source and destination IP addresses, the kind of protocol used, the length and size of the header, and so on. Data with irrelevant characteristics reduces model accuracy and lengthens the time required to train the model. There is no way to construct an IDS without first selecting its features (IDS).
- c) **Analysis:** There is a search for truth in the data.
- d) **Action:** There is a clear explanation of the assault and the system's response.

V. BLOCKCHAIN

In cryptography, data is made impenetrable to outsiders and accessible only to the intended audience by using the technique of encryption. Later, as technology advanced, a number of advanced safeguards were used to protect the message so that the data could not be compromised. Numerous technically difficult techniques, including AES and RSA, are used to encrypt and decrypt the data. Computer science advancements have led to the application of cryptography in the development of cryptographic money and cryptocurrencies. The blockchain distributed ledger technology, which uses top-notch encryption techniques, is the foundation upon which the Bitcoin cryptocurrency is created. In numerous phases, blockchain uses cryptography, and some of the techniques it uses are state-of-the-art. The numerous cryptographic attacks are reviewed in this article.

Blockchain is a decentralized public ledger that is spread throughout the network and records network transactions. Every node in the network is equipped with a copy of the distributed ledger, which is accessible to everyone. The network's transactions are organized into blocks, and each block is related to the one before it using hashing techniques. The network nodes broadcast the information to the network while tightly encrypting the data into blocks. By using the hash code to connect each block to the next, hashing aids in maintaining the integrity of the data. Blockchain refers to a chain of blocks connected by a hash. Due to its distinctive qualities like immutability, integrity, security, and reliability, blockchain is currently one of the technologies with the greatest growth rates. Blockchain is a distributed, public ledger that records network transactions and is not centralized. Every node in the network has a copy of the distributed ledger, which is available to the whole public. The network combines transactions into blocks, and hashing methods link each block to the one before it. The network nodes tightly encrypt the data into blocks before broadcasting it to the entire network. By connecting each block with the other using the hash code, hashing aids in assuring the integrity of the data. Blockchain is the term used to describe a chain of blocks connected by a hash. Due to its distinctive qualities including immutability, integrity, security, and reliability.

Blockchain technology is currently one of the fastest-growing technologies. A miner is the person who

creates and validates the block, and every node in the blockchain network keeps a copy of the Blockchain. A peer-to-peer network known as a blockchain does its own self-verification, doing away with the need for a third party. The network nodes that carry out the validation process honestly receive rewards. Mining refers to the process of validating transactional data. The Proof-of-Work idea is used in the Blockchain. A network must solve a cryptographic puzzle before broadcasting the answers for verification and timestamping to the network. The proof-of-work principle maintains the network's integrity.

The SHA-256 algorithm is employed in Pow because, despite being very difficult to solve, it can be easily validated. Due to its decentralized nature, immutability, and security services feature, blockchain technology can be used in most fields ranging widely. A lot of businesses are currently concentrating on finding a suitable use case for blockchain to fit in. Other than financial services, some of the key industries where blockchain is being used are education, healthcare, supply chains, IoT, data management and security services, the energy industry, and so on.

VI. Key Authentication Technique

Authentication is identification of end users. There are different ways for authentication techniques are like:

- a) Something they know – Pin, Passwords, etc.
- b) Something they have – Mobile, Device, etc.
- c) Something they are – Biometrics, etc.

Key based authentication (also called as cryptographic authentication). It is used to prove one's identity. It is deployed over every enterprise environment.

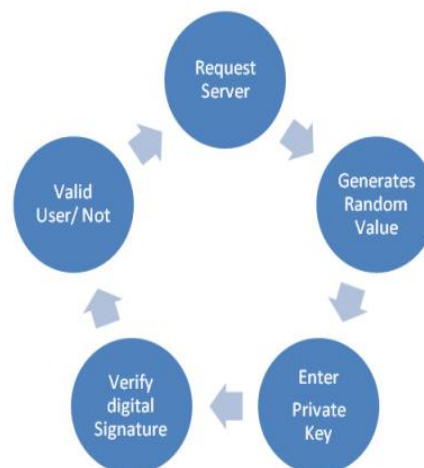
Private keys provide strong authentication but fail if the keys are misplaced or taken by someone which is very vulnerable to cause the offline brute force attack even if it is encrypted with a password.

The key authentication works on the two main keys: -

- a) Public Keys – It is provided to all users.

- b) Private Keys – It involves the public key and always remains private.

The Process of Key Authentication: -



TLS is also used in authentication techniques to provide security over a network. To prevent the hackers attack we use: M-RSA (Mediator RSA) key based authentication security is used for establishing private keys. If a hacker wishes to guess a password after stealing the encrypted private keys then it sends or records every event as logs to the mediator for each event.

By which the user gets time to revoke the key for the lost device. This method can be used with the user's existing device as there are no new systems needed and the server only needs to verify the digital signature.

VII. REFERENCES

- <https://www.canva.com/design/DAFNaxIoWQo/pjBIi3vWExdOVkq31Yh-8w/edit#>
- <https://www.geeksforgeeks.org/intrusion-detection-system-ids/>
- <https://www.techtarget.com/searchsecurity/definition/intrusion-detection-system>
- <https://www.checkpoint.com/cyber-hub/network-security/what-is-an-intrusion-detection-system-ids/>
- https://www.researchgate.net/publication/45902386_Intrusion_Detection_System_Overview
- <https://ijcsmc.com/docs/papers/March2020/V9I3202050.pdf>
- <https://www.mdpi.com/2076-3417/10/1/217/htm>
- <https://thesai.org/Publications/ViewPaper?Volume=11&Issue=10&Code=IJACSA&SerialNo=37>