International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 05 Issue: 10 | Oct - 2021 ISSN: 2582-3930

# Importance of Cryptography in Digital World

Anshika Tripathi

*Student, Dept. of M.Sc I.T, Model College, Dombivli, Mumbai, Maharashtra, India.*

**Abstract--** *In recent years, cloud computing may be a fast growing technology. Cloud is a group of data centers and servers that are placed at a different location and this application is used by a user as pay on service with the help of the internet. The main reason for using the cloud is that the user can store and access the stored data within the cloud from anywhere anytime. The cloud user needn't worry about the upkeep of software, hardware and space for storing . The main advantage of cloud computing is that these services are provided at low cost for the user. For that reason, all users transfer their data on the cloud. The major issues in cloud computing are security because the knowledge stored within the cloud isn't directly maintained by the customer. While sending the info through the web any unauthorized user can modify the info or access it. To overcome the safety issues various cryptography and steganography algorithms are proposed. In this paper, focused on the basics of cloud computing and discussed various cryptography algorithms present in the existing work.*

***Keywords*-- *Introduction, Types of Cloud, Cryptocurrency Attacks, Safeguard from Attackers, Non-Custodial Vs. Custodial, Conclusion.***

## 1.1 Introduction

Cloud computing is the trending technology that uses the network to provide service to the user. Cloud acts as a software virtualized. Large scale and small scale businesses are spending a large amount of money to store and maintain their data. Cloud computing provides the service to the business people by storing, computation and maintaining the data at low cost. Cloud computing allows the business user or individual user to use the application through the internet without installing in their system. For example: Gmail, facebook, YouTube, drop box. The user will pay the amount as per the data usage. The main advantage of cloud computing is low cost, increased storage and flexibility. The major risk in cloud computing is security and privacy (i.e. by putting the valuable data on someone else's server in an unknown location).

### 1.2. TYPES OF CLOUD

Depending on the user or business need the different types of cloud are available. There are four types of clouds available, Private Cloud – A private cloud can be accessed by a single group or single organization. It is managed by a third party or organization. Private cloud is highly secure and flexible so private cloud is often used by larger organizations or government sectors.

- **Public Cloud** – A public cloud can be accessed by any user with the internet connection and want to pay as per their usage. The files are hosted by a third party. Example: Amazon, Windows Azure Service Platform and salesforce.
- **Community Cloud** – A community cloud will be accessed by two or more organizations that have similar cloud requirements.

- **Hybrid Cloud** – A hybrid is the combination of two or more clouds (public, private, and community).

## 2. Cryptocurrency Attacks

With the growing fashionability of cryptocurrency, cybercriminals are taking advantage of the openings this creates to trick implicit victims and increase the gains they will make from their attacks, according to cybersecurity establishment Barracuda. Experimenters at Barracuda lately analysed phishing impersonations and business dispatch concession attacks transferred between October 2020 and 2021. They linked that the growing price of bitcoin has led to a rise within the volume of cryptocurrency- related attacks.

As certain organisations began to advertise that they are going to accept payments in bitcoin, interest in cryptocurrency increased. " Fueled by the chaos around bitcoin," cryptocurrency's price increased by nearly 400 per cent between October 2020 and April 2021. With this, cyberattacks snappily followed impersonation attacks, which led to its growth by 192 per cent, the report said.

Murali Urs, Country Manager, Barracuda Networks-India said, " The digital format of Cryptocurrencies make them decentralized in nature and with no regulations, they need to become the currency of choice for cybercriminals. It fueled and enabled a multibillion frugality of ransomware,cyber-extortion, and impersonation."

" These attacks are targeting not just private businesses, but also critical structures, in order that they increasingly pose a public security threat. The recent high- profile attacks on organisations like Colonial Pipeline and JOBS in the US are likely to bring lesser interest in the Government's intervention and regulation of bitcoin," added Urs.

### 2.1 How Cryptocurrency Affects the Security of Your Business

**So what does this mean in terms of your business?**

Since cryptocurrencies are completely decentralized, there's no central authority to cover the deals and overall crypto exertion. Likewise, cryptocurrencies involve low situations of regulations. This makes cryptocurrencies a miscreant's haven. Every business that uses cryptocurrencies may be a target unless they increase its cybersecurity measures. Cybercriminals can buy or sell virtual currencies without ever being discovered.

That down, all businesses that make exchanges using cryptocurrencies are exposed to numerous pitfalls. Exchange addicts and cryptocurrency dealers risk making bad trades that can result in significant losses. Also are some of the most common cybersecurity risks:

- **Phishing:** A phishing crusade targets trading platforms with the primary thing aimed at stealing stoner's credentials that scammers can use to ask for profit or deliverance.
- **Hacked trading platforms**: Cybercriminals concession trading platforms by stealing finances from the addicts.

- **Compromised Registration forms** : Cybercriminals steal addicts' information. They also sell it in the black request for profit.
- **Third- party operations** : This is an excellent way for cybercriminals to steal your stoner data and use it to target further attacks.
- **Malware:** Cryptocurrency- related malware enters the mining machines and steals the mining coffers of the infected computer. It also can be wont to steal cryptocurrencies from online holdalls.

The voguish thanks to cover your business from these cyber- attacks is by administering proper crypto cybersecurity protocols and practices also as being spare conservative with the operations and spots you use.

### 3. Guard of Cryptocurrency from Attackers

The trouble with your digital currencies is substantially through cryptocurrency wallets (digital wallets) or exchange providers. A crypto wallet doesn't store your digital coins, but it holds a private key, which allows you to trade cryptocurrency online. This private key is your digital identity to the cryptocurrency request and anyone who gets hold of this can perform fraudulent deals or steal your crypto coins. Cybercriminals use sophisticated ways to compromise digital wallets and steal/ transfer crypto means without the user's knowledge. Securing your wallet is essential when it comes to securing your digital currency against cyberattacks.

**Presently are some of the ways to secure your cryptocurrency**:

- **Use a Cold Wallet:** Unlike hot wallets, cold wallets don't connect to the internet hence, they aren't prone to cyberattacks. Storing your private keys in a cold wallet, also known as a hardware wallet, is the most feasible option as these come encoded, keeping your keys secure.

In 2019, the Japanese exchange BITpoint discovered an unauthorized withdrawal of$ 32 million from its hot wallet in different cryptocurrencies targeting other than users. The exchange held five cryptocurrencies in its hot wallet Bitcoin, Bitcoin Cash, Ethereum, Litecoin, and Ripple. though, BITpoint clarified that its cold wallet and cash effects weren't affected in the incident.

- **Use Secure Internet:** While trading or making crypto deals, use only a secure internet connection and avoid public Wi-Fi networks. Indeed when penetrating your home network, use a VPN for more security. A VPN changes your IP address and position, keeping your browsing activity safe and private from trouble actors.
- **Maintain Multiple Wallets:** Since there's no limitation for wallet creation, you can diversify your cryptocurrency investments in multiple wallets. Use one wallet for your day-to-day deals and keep the rest in a separate wallet. This will cover your portfolio and mitigate the loss of any breach to your crypto account.

- **Secure Your Particular Device:** Make sure your particular device is over to date with the latest virus descriptions to defend against recently discovered vulnerabilities. Use a strong antivirus and firewall to better your device's security to avoid hackers from taking advantage of the weakness by writing code to target the vulnerability.
- **Change Your Password Regularly:** We can not underestimate the significance of a strong password while talking about security. According to a study, three- quarters of millennials in theU.S. use the same password on further than 10 devices, apps, and other social media accounts. It also stated that maximum of them were using the same password in over 50 different places. Make sure you have a strong and complex password, which is tough to guess, and change it on a regular basis. Use separate passwords if you have multiple wallets. Conclusion for two- factor authentication (2FA) multi-factor authentication (MFA) for more security.
- **Don't Get Phished:** Phishing scams via malicious advertisements and emails are rampant in the cryptocurrency world. Be careful while making crypto deals and avoid any suspicious and unknown links.

In a recent cryptocurrency heist, a hacking group " CryptoCore" targeted cryptocurrency exchanges via spear-phishing campaigns. Attackers stole cryptocurrency worth$ 200 million in two years, targeting companies in theU.S. and Japan since 2018. ClearSky stated that CryptoCore initiated a surveillance phase to identify the mail accounts of the cryptocurrency exchange's workers and security directors before conducting a spear-phishing attack. These attacks were performed using fake disciplines impersonating affiliated associations and workers, and by embedding malicious links in documents via emails.

## 4. Non-Custodial Vs. Custodial holdalls

First, it's important to understand the different types of holdalls out there. However, you can use bothNon-Custodial holdalls or Custodial holdalls to store your finances, If you decide to buy Cryptocurrency. It; s depend on the person's particular decision.

- **Non-Custodial Wallet:** With a Non-Custodial, or self- custody, wallet, you're in control of your private keys and you hold your own cryptocurrency goods.

  When using aNon-Custodial wallet service, you are completely responsible for remembering your private keys and maintaining security measures to cover your funds. However, which is common, you won't be capable of accessing your own cryptocurrency-- no exceptions, If you forget your private keys.

  " You have the responsibility to make sure you do n't lose your keys, and you 're really the only person with that responsibility," says Nick Neuman, CEO of bitcoin security and self- custody

company Casa. That means you 're responsible for making sure you employ back- over mechanisms like cold holdalls, including tackle holdalls, which are physical devices that store your keys offline, Neuman says. Numerous hardware wallets look correspondent to a USB stick.

Though hardware wallets are extensively considered to be the safest option to store private keys, there are still threats. It's important to use a trusted hardware provider and secure your hardware wallet in a safe place, since a physical device can still be stolen or destroyed. To physically secure their keys, some investors use a hardware wallet, while others write their private keys on paper and lock it in a vault. Some also prefer non-custodial wallets that offer multisig, or multi-signature, protection.

★ **Custodial wallets:** With a custodial wallet service, a third party, similar to exchanges like Coinbase, Kraken or Gemini, is in control of your private keys. This means that if you buy cryptocurrency through an exchange, you're given a kind of " IOU" for the cryptocurrency, while the exchange owns the private keys and holds the cryptocurrency in their wallet.

You should also understand the implicit threats. With a custodial wallet, a hacker would n't need your private keys to move funds from your account, since the exchange owns the keys, not you. That eliminates one wall of protection to your finances, Neumann Says. However, numerous exchanges invest heavily in security, and there are other ways to prevent your account from being addressed collectively, similar to two- factor authentication.

## Conclusion

The cryptocurrency industry is constantly evolving, and it is your sole responsibility to protect your digital funds by securing your wallet with essential safety precautions. Update yourself with the latest security news, attack techniques, and prevention strategies. It is our Responsibility to save our data from attackers. If we do not upgrade our details then it will be easy for an attacker to steal your credentials which may cause harm for victim and loss of currency.

It has become a severe problem in this digital world so take proper step and save your data from unethical use.

## Acknowledgement

It gives me great pleasure to present my Research paper on "Importance of Cryptocurrency in the Digital World". I would like to express my sincere thanks to all the teachers who helped us throughout. I would like to

acknowledge the help and guidance provided by our professors in all places during the presentation of this research paper.

We are also grateful to, Head of Department. This acknowledgement will remain incomplete if we do not mention a sense of gratitude towards our esteemed Principal who provided us with the necessary guidance, encouragement and all the facilities available to work on this project.

**Reference**

- https://cisomag.eccouncil.org/cryptocurrency-wallet-security/
- https://www.cnbc.com/2021/06/11/tips-to-help-keep-your-crypto-wallet-secure.html
- https://fultonmay.com/what-is-cryptocurrency-and-how-does-it-affect-cyber-security/
- https://www.thehindubusinessline.com/info-tech/cryptocurrency-related-cyberattacks-are-on-the-rise-report/article35048000.ece
- https://www.kaspersky.com/resource-center/definitions/what-is-cryptocurrency
- https://www.investopedia.com/terms/c/cryptocurrency.asp